Universitat Autònoma de Barcelona

Analysis of background textures in banknotes and identity documents for counterfeit detection

Albert Berenguel Centeno

Universitat Autònoma
de Barcelona

Analysis of background textures in banknotes and identity documents for counterfeit detection

A dissertation submitted by **Albert Berenguel Centeno**
at Universitat Autònoma de Barcelona to fulfil the degree
of **Doctor of Philosophy**

Bellaterra, September 16, 2019

Co-Director	**Dr. Josep Lladós** Universitat Autònoma de Barcelona Centre de Visió per Computador
Co-Director	**Dr. Oriol Ramos Terrades** Universitat Autònoma de Barcelona Centre de Visió per Computador
Co-Director	**Dra. Cristina Cañero** Research Group Mitek Systems Ltd.
Thesis committee	**Dr. Jean-Marc Ogier** Computer Vision Laboratory Université de La Rochelle Laboratoire L3i **Dr. Antoine Tabbone** Université de Lorraine Institut des Sciences du Digital, Management et Cognition **Dr. Marçal Rusiñol** Universitat Autònoma de Barcelona Centre de Visió per Computador

This document was typeset by the author using LaTeX 2$_\varepsilon$.

The research described in this book was carried out at the Centre de Visió per Computador, Universitat Autònoma de Barcelona.

ISBN: XXX-XX-XXXXXX-X-X

Printed by Ediciones Gráficas XXXXX, S.L.

There are no secrets to success. It
is the result of preparation, hard
work, and learning from failure.
— Colin Powell

Part of the inhumanity of the computer is that,
once it is competently programmed and
working smoothly, it is completely honest.
— Isaac Asimov

To my family and friends

Acknowledgements

This stage as a PhD student has been one of the most rewarding, complete and challenging periods of my life. This thesis has produced a profound impact on how a perceive research. Before starting this thesis collaborating with the research community seemed a difficult goal due to the fast pace the computer vision field is moving. Closing my epoch as PhD student, I dare to say the initial fears were not founded. Entering to this field is rewarding when enough effort, good and positive attitude are set in your mindset. Helping you to see and recognize opportunities to improve not only the research community but also as an individual. The continue interactions with other researchers, reading daily their works, collaborating with them and living the life of a PhD student has made me appreciate even more the research fellows. Shall this serve as a humble recognition of all those who contributed to this work.

Let me start with those academically close, *i.e.*, my supervisors, without their support this thesis would have never seen the light. Oriol and Josep thanks for your unconditional support, discussions and the ideas you provide me. You have been there anytime I could need you and we have nice talks, being research or any non-related topic with the PhD. Both, outside the academia framework have prove I could count with you for any problems I could have. I hope after this thesis, the relation that we have can continue as always has been. Last, but not least, I want to thank Cristina, for her support and laughs at any time of the day. You have helped me with your opinions and support during this thesis. We have known each other for so long, seeing each other near every day, and we still have funny moments in multiple situations in our daily life. I hope these thing will not change in the future.

I also want to thank all the people from the CVC who made the three years of my stay in the building really smooth and welcoming. Specially to Pau Riba, Pau Rodriguez, Arnau and Edgar Riba, they have been there from begin to end. We have done many activities inside and outside research. Playing padel, going to the gym, barbecues and other outdoor activities had helped me in clear my mind when I really needed. Other colleagues from CVC has also helped me to stop staring the screen in the everyday student life, and concentrate in what really matters that is knowing amazing people along the way. So thanks to Jordi Gonzalez, Carola, Xavier, Claire, Ana, Mari, Montse, Alexandra, Meritxell, Pep Gonfaus, Felipe, Yaxing, Dena, Gemma, Arash, Onur, Bojana...I would keep on naming fantastic persons from CVC, in general thanks to all of you. Thanks for being there with me, sharing breakfast, talking about stupid things and above all your friendship.

My deepest gratitude to my friends outside CVC. They have suffered all my

absences due the many extra hours due this thesis. They always have understood that this period of my life was important for me, giving me support and welcoming me any time I wanted to relief some stress. Especially thanks to Serafin, Miriam and Carlos. I would not being able to do it without you all.

I leave my most inner circle to the end. Thanks to all my family for all the strength and courage you gave me. Your unconditional support and love made me able to finish this stage of my life.

Abstract

Counterfeiting and piracy are a form of theft that has been steadily growing in recent years. A counterfeit is an unauthorized reproduction of an authentic/genuine object. Banknotes and identity documents are two common objects of counterfeiting. The former is used by organized criminal groups to finance a variety of illegal activities or even to destabilize entire countries due the inflation effect. Generally, in order to run their illicit businesses, counterfeiters establish companies and bank accounts using fraudulent identity documents. The illegal activities generated by counterfeit banknotes and identity documents has a damaging effect on business, the economy and the general population. To fight against counterfeiters, governments and authorities around the globe cooperate and develop security features to protect their security documents. Many of the security features in identity documents can also be found in banknotes. In this dissertation we focus our efforts in detecting the counterfeit banknotes and identity documents by analyzing the security features at the background printing. Background areas on secure documents contain fine-line patterns and designs that are difficult to reproduce without the manufacturers cutting-edge printing equipment. Our objective is to find the loose of resolution between the genuine security document and the printed counterfeit version with a publicly available commercial printer. We first present the most complete survey to date in identity and banknote security features. The compared algorithms and systems are based on computer vision and machine learning. Then we advance to present the banknote and identity counterfeit dataset we have built and use along all this thesis. Afterwards, we evaluate and adapt algorithms in the literature for the security background texture analysis. We study this problem from the point of view of robustness, computational efficiency and applicability into a real and non-controlled industrial scenario, proposing key insights to use these algorithms. Next, within the industrial environment of this thesis, we build a complete service oriented architecture to detect counterfeit documents. The mobile application and the server framework intends to be used even by non-expert document examiners to spot counterfeits. Later, we re-frame the problem of background texture counterfeit detection as a full-reference game of spotting the differences, by alternating glimpses between a counterfeit and a genuine background using recurrent neural networks. Finally, we deal with the lack of counterfeit samples, presenting a novel approach based on anomaly detection.

Key words: *counterfeit, background texture, computer vision, machine learning, banknotes, identity documents*

Resumen

Las falsificaciones y copias pirata son formas de robo que no han parado de crecer en los últimos años. Una falsificación es una reproducción no autorizada de un objecto autentico/genuino. Billetes y documentos de identidad son dos objetos comunes de falsificación. El primero es usado por grupos criminales organizados para financiar una gran variedad de actividades ilegales o incluso para desestabilizar países debido al efecto de la inflación. Generalmente, para poder operar un negocio ilícito, los falsificadores crean compañías y cuentas bancarias usando documentos de identidad fraudulentos. Las actividades ilegales generadas por billetes y documentos de identidad falsificados provocan daños a negocios, la economía y a la población en general. Para luchar contra falsificadores, gobiernos y autoridades en el mundo cooperan y desarrollan medidas de seguridad para proteger sus documentos de seguridad. Muchas de las medidas de seguridad en documentos de identidad también se encuentran en billetes. En esta disertación centramos nuestro esfuerzo en detectar las falsificaciones de billetes y documentos de identidad analizando las medidas de seguridad del fondo de impresión. El fondo de documentos de seguridad contiene patrones de finas líneas y diseños que son difíciles de reproducir sin los modernos equipos de impresión de los fabricantes. Primero presentamos el estudio más completo hasta la fecha de medidas de seguridad en billetes y documentos de identidad. Los algoritmos y sistemas comparados están basados en visión por computador y aprendizaje automático. Posteriormente presentamos el dataset de falsificaciones de billetes y documentos de identidad que hemos construido y se usa durante toda tesis. A continuación, evaluamos y adaptamos algoritmos en la literatura para el análisis de fondos de seguridad. Estudiamos el problema desde el punto de vista de robustez, eficiencia computacional y aplicabilidad en un entorno industrial real, proponiendo ideas clave para utilizar estos algoritmos. Posteriormente, dentro del entorno industrial de esta tesis, desarrollamos una arquitectura orientada al servicio para detectar documentos falsificados. La arquitectura de la aplicación móvil y servidor está pensada para ser usada incluso por examinadores de documentos falsificados inexpertos. Más tarde, reformulamos el problema de detección de texturas del fondo de seguridad como un juego de buscar diferencias, alternado vistazos entre el fondo falsificado y el auténtico usando redes neuronales recurrentes. Finalmente, tratamos la falta de ejemplos falsificados, presentando un nuevo algoritmo basado en detección de anomalías.

Palabras clave: *falsificación, texturas fondo, vision computador, visión artificial, aprendizaje automático, billetes, documentos identidad*

Resum

Les falsificacions i copies pirata son formes de rob que no han parat de créixer en el darrers anys. Una falsificació es una reproducció no autoritzada d'un objecte autèntic/genuí. Bitllets i documents d'identitat son dos objectes comuns de falsificació. El primer es usat per grups criminals organitzats per finançar una gran varietat d'activitats il·legals o inclús per desestabilitzar països degut a l'efecte de la inflació. Generalment, per poder operar un negoci il·lícit, els falsificadors creen companyies i comptes bancaris usant documents d'identitat fraudulents. Les activitats il·legals generades per bitllets i documents d'identitat falsificats provoquen danys a negocis, l'economia i a la població en general. Per lluitar contra falsificadors, governs i autoritats en el mon cooperen i desenvolupen mesures de seguretat per protegir els seus documents de seguretat. Moltes de les mesures de seguretat en documents d'identitat també es poden trobar en bitllets. En aquesta dissertació centrem el nostre esforç en detectar les falsificacions de bitllets i documents d'identitat analitzant les mesures de seguretat del fons d'impressió. El fons de documents de seguretat conté patrons de fines línies i dissenys que son difícils de reproduir sense els moderns equips d'impressió dels fabricants. Primer presentem l'estudi més complet fins avui de mesures de seguretat en bitllets i documents d'identitat. Els algorismes i sistemes comparats estan basats en visió per computador i aprenentatge automàtic. Posteriorment presentem el dataset de falsificacions de bitllets i documents d'identitat que hem construït i que s'utilitza durant tota la tesis. A continuació, avaluem i adaptem algorismes en la literatura per l'anàlisi de fons de seguretat. Estudiem el problema des de el punt de vista de robustesa, eficiència computacional i aplicabilitat en un entorn industrial real, proposant idees clau per utilitzar aquests algorismes. Posteriorment, dintre de l'entorn industrial d'aquesta tesis, desenvolupem una completa arquitectura orientada al servei per detectar documents falsificats. L'arquitectura de l'aplicació mòbil i servidor està pensada per ser utilitzada inclús per examinadors de documents falsificats inexperts. Més tard, reformulem el problema de detecció de textures del fons de seguretat com un joc de buscar diferencies, alternant mirades entre el fons falsificat i l'autèntic utilitzant xarxes neuronals recurrents. Finalment, tractem la falta d'exemples falsificats, presentant un nou algorisme basat en detecció d'anomalies.

Paraules clau: *falsificació, textures de fons, visió per computador, aprenentatge automàtic, bitllets, documents d'identitat*

Contents

List of Figures

List of Tables

1 Introduction

Documents with security features are a key element of authentication in the current world. Security features objective is to avoid the alteration of the original document. This chapter identifies the current problems of security documents and explains the main motivation of this industrial thesis. Along with a brief explanation of anti-counterfeit measures, we explain why we center our effort in background security printing. Finally, we introduce the objectives and scope of this thesis.

1.1 Motivation

Counterfeit is the action of make an exact imitation of something valuable with the intention to deceive or defraud. Usually counterfeit products are produced for dishonest or illegal purposes, with the intent to take advantage of the superior value of the imitated product. Counterfeit objects produced for criminal activity not only causes potential harm to the health and safety of the citizens, it also affects legitimate economies, contributing to reduced revenues for the affected businesses, decreases sales volume and job losses. According to a 2013 report, the OECD estimated counterfeit goods accounted for 2.5% of global trade [160]. Currently, trade of counterfeit and pirated goods represents $1.7 trillion per year and is expected to grow to $2.8 trillion and cost 5.4 million jobs by 2022 [88]. In 2018, counterfeit was the largest criminal enterprise in the world, more than drugs and human trafficking [88].

From the different types of counterfeit document fraud continues to play a key enabling role in trafficking of counterfeit goods. Counterfeiting goods is an important source of income for organized criminal groups. At the stage of distribution of counterfeit goods, fraudulent retail licences enable the infiltration of the legitimate supply chain. Generally, in order to run their illicit businesses, counterfeiters establish companies and bank accounts using fraudulent identity documents (ID)

or under the name of a front person, and regularly make use of bogus invoices. Counterfeiters purchase or rent vehicles using fake documents. Number plates of cars belonging to criminal groups are registered abroad or under a fake identity. Fraudulent documents are widely used to facilitate the transportation, distribution and sale of counterfeit goods. For the purpose of importation, counterfeiters provide false shipping documents, such as bills of lading, to conceal the content of containers of packages and the origin of shipments. They often use false invoices issued for imported goods in declarations to customs. This practice is also used to undervalue their imported products.

Banknote counterfeiting is another illegal lucrative business for the counterfeiters. Through recorded history currency has been used as a medium of exchange for goods and services. Paper notes, coins and electronic currency are the general accepted form of trade. Governments of each country using central banks are the responsible to issue money and circulate it within an economy. Currency only holds its value as long as users have confidence in its authenticity to represent goods. A common threat for any economy is the quantity of counterfeit money which is being used in the actual market. Higher than previous years, in the first half year of 2015, $454K$ counterfeit Euro banknotes were withdrawn from circulation, being 86% of the counterfeits from €20 and €50 banknotes,[21].

The modus operandi in counterfeiting and piracy have partially changed over the past few years and are expected to evolve further in the future. To be able to carry out such a variety of activities, criminal groups need stable access to resources. However, this does not seem to pose any major difficulty for criminals. Widely available and affordable information and communication tools increasingly facilitate their activities.

Counterfeit detection has traditionally been a task for law enforcement agencies. EUROPOL and INTERPOL central offices are combating document and banknote counterfeiting [81, 116]. They have destined millions of euros in funds to provides technical databases, forensic support, training and operational assistance to its member countries. It makes no difference how many security barriers the experts place in their way, the criminal competitors are never far behind. As a consequence, the production of counterfeit money and IDs is on the rise. It is important to note that most of the anti-counterfeits measures present in security identity documents, were first created and used to detect counterfeit money banknotes.

There are many different strategies used to fake an ID like the alteration of a real passport, impersonation of the legitimate owner or printing false information on a stolen blank real paper, to cite some. Making a fake passport is easy, making a good fake passport is very, very hard. Probably there are few criminal organizations in the world which can produce a counterfeit visa or passport good enough to fool professional passport control. Same reasoning applies to banknotes counterfeit

production.

There is also a considerable amount of scientific and technological work underway in university and government research laboratories relevant for future counterfeit deterrence [219]. However, nowadays it does not exist a single visible deterrent feature that is readily recognizable, highly durable, impractical to counterfeit or simulate, available at low cost, and easy to produce. Hence the solution to detect counterfeits is to add a combination of security measures to each document. The key idea, is not matter how good the counterfeiter is, he just has to make a single mistake at one of the deterrent security features to capture them. A drawback of this approach is that you need algorithms and solutions able to detect each one of this individual security measures. These solutions usually exists in specialized document examination laboratories where examination specialists in security documents check for all the security measures. The examination cost of security documents to determine its authenticity is high in terms of time and money, due most of this anti-counterfeits measures are checked manually by these experts [200].

There is a need for automatic solutions to detect and assess security documents for faster, cheaper and less prone to human errors evaluation. Computer vision techniques have been useful to help or replace human analysis of some of the counterfeit features. Researchers have presented different algorithms to determine document authenticity [48]. Despite all these efforts counterfeit detection remains an open research problem. Most of this solutions still requires the usage of specialized equipment to produce the images which would be analyzed by these algorithms.

This dissertation corresponds to an industrial thesis to solve the problem of counterfeit detection in banknote and identity documents. We propose to use computer vision algorithms to detect the authenticity of security features. Our objective is to produce a low cost solution which does not require specialized equipment and does not need expert document reviewers.

1.2 Anti-counterfeit measures

Adding multiple anti-counterfeit measures to a security document will add complexity to the counterfeiter's task and increase the number of steps that has to follow to replicate a security document. The combination and duplication difficulty of this deterrents would cause the casual counterfeiter to "give up" on its task. There exists several deterrents depending on the substrate, ink and printing of each document. Computer vision algorithms can check security measures on the substrate of the document such as watermark, security fibres, planchetes, see through windows,

etc. Other features are related to the ink used, for instance pearl ink, color shifting inks, UV glowing ink or infrared ink. Security features like Guilloches, Intaglio printing, serial number and microprinting corresponds to some of the printing security features. All these features classified in four security levels:

- First security level corresponds to the features that can be inspected with humans senses typically: sight, touch and sound. Most of the anti-counterfeiting measures fall into this category such as holograms, color fidelity, etc. Touching the security document allows to have a precise idea of the paper or material used and therefore its texture. On banknotes it must be firm and should produce a specific sound, almost like a crackling sound. Polycarbonte ID cards are rigid and sound like a compact disc when dropped. Even the stitching and sewing of the passport pages are protected by sewing threads to secure the booklet pages to the end pages and covers. Any attempt at dismantling a passport would be quickly identifiable. Sound and touching deterrents unfortunately are out of scope for computer vision algorithms. Other deterrents from this category needs a video of the security document to be able to analyze it with a computer vision algorithm. Holograms or latent images are an example of security measure, which requires several image frames to distinguish the characteristic substrate visual properties.

- Second level of security features are hidden from human sense and can only be checked with specialized equipment like UV lamp or magnified glass, such as microtext or luminescence ink features. Once acquired the image through the specialized equipment, looking for the security features can be done by a computer vision algorithms or even by giving a quick glimpse by an human. Usually checking the hidden ink patterns like the glowing UV ink, once discovered by the especial equipment, are less complex than visible ones. Unfortunately, common users does not have available specialized equipment.

- Third level of security features corresponds to the security characteristics that are only known by expert forensics examiners. These last level of features are the result from the printing process and raw materials used during banknote fabrication, such as complicated patterns, texture analysis, etc. We want to focus on this level of security features because we want to replace the knowledge of an expert forensic examiner of complicated patterns and texture analysis for a machine learning model using computer vision algorithms.

- Fourth security level is secret and includes safety measures known only to a narrow range of experts. An example of these type is biometric ink. Biometric inks contains DNA taggants (uniquely encoded materials, like a fingerprint's

signature of identity) which are virtually impossible to duplicate. The knowledge of this DNA taggants in many cases is only available to the manufacturer only, hence it is outside the scope of this thesis.

1.3 Counterfeit generation procedure

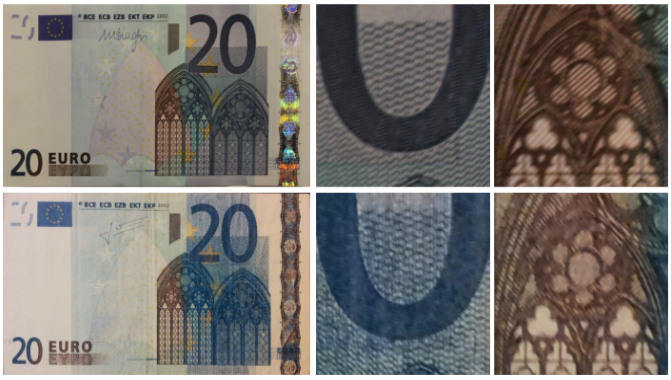


Figure 1.1 – Example of resolution loose in fine-line patterns. First row €20 genuine banknote and ROIs extracted, second row scanned and printed €20 counterfeit banknote. Acquired with BQ Aquaris M5 smartphone at 600 dpi.

Today, technology makes possible for anyone with a simple scanner, a high-end printer and some basic knowledge in image edition software to jump into the world of counterfeit document production. With a quick search in any web search engine, it is possible to find multiple tutorials of how to make a fake ID [4], or to find news where a non-experienced user produced between $10,000 and $20,000 of fake bills over two years, with a commercial inkjet printer before being caught [1]. These are clearly low-tech counterfeiting, but still an open problem for business owners and government agencies.

An important security feature that serves against counterfeiting and manipulation of documents is the background/security printing, present at the third level of security features. The counterfeiter requires high technical specialized printing equipment to reproduce this background printing techniques. Having this equipment is not feasible for the majority of the counterfeiters due economic and restricted availability issues. Thanks to this, a large part of counterfeits just follows the procedure of scan a real document, alter the data and then print the document with a common commercial printer.

The quality of the counterfeit will depend on the printer, materials and security features used in the production of the document. Following this procedure, we expect that the texture background print design such as *guilloché* or fine-line patterns will loose detail, hence it will be possible to classify it as counterfeit, see Figure 1.1.

1.4 Industrial thesis

This dissertation belongs to an industrial thesis proposed by Icar Vision Systems S.L. . The company main focus is in identity fraud prevention and document management solutions. Its products, systems identification based on digital images, allow structured and authentication of official identity documents reading using computer vision techniques. Recently, Mitek Systems Inc. acquired ICAR, creating a much more powerful solution, one that combines computer vision, artificial intelligence and machine learning.

Many users were sending counterfeit documents to the OCR system and those were following the normal pipeline without a robust counterfeit authenticity checking. We center our efforts in detecting low level counterfeiting. Most of this type of counterfeit just follows the *scan-printing* procedure. Following this procedure, we expect that the texture background print design will loose detail, and hence it will be possible to classify it as counterfeit. This industrial thesis proposition is to check the security measures visible to the naked eye like guilloche or fine-line patterns, intaglio, etc. present at the background of these documents. Focusing only in visible measures allows to generate anti-counterfeiting tools for non-experienced users which could be used with common smartphones.

1.5 Objectives and Scope

We target the third level of security features because want to focus on the complicated patterns and texture analysis. These will allow us to train a machine learning model which will act as an expert forensic examiner. The application scenarios are the services or products that require a genuine identification of highly secured documents where a smartphone is available, in a non-controlled environment for document acquisition and without the need of specialized equipment like UV or IR lamps. In addition, no video processing is used, being this a requirement of this thesis. The fact that we only process single images coming from the smartphone, discards the first security level of anti-counterfeit measures which are highly dependent of the availability of different frames, such as the color reflection of the holograms or the color fidelity of the Optical Variable Ink (OVI).

The benefits of this approach are: a low cost solution without the need of specialized equipment like UV or IR lamps, broadly available because it can be implemented as an application for common smartphones and the fast automatic detection of counterfeit textures patterns of security documents, which makes it more reliable and less prone to human errors. The application scenarios are the services or products that require a genuine identification of highly secured documents where a smartphone is available, such as renting a car, applying for a loan, pay with a banknote for a product, among others.

Summarizing, the aim of this PhD dissertation is to develop new approaches for document detection authenticity using the anti-counterfeit background textures features present at security documents. Our objective is to analyze its authenticity from a single image using a mobile phone camera within a non-controlled environment.

With this objectives in mind, we split this thesis into three parts, chapter three to eight are contained inside this three contextual blocks. The part I of this thesis presents first the created dataset which will be used across all the dissertation. Afterwards we study which algorithms could produce a better representation of the different types of genuine textures, to be able to discern the counterfeit cases. We also present a Service-Oriented Architecture (SoA) for counterfeit detection. To this end, we ask the following questions:

- How do we represent the textures for the type of counterfeit we want to solve?
- Is it possible to use existing hand-crafted texture algorithms for detecting the counterfeits?
- How can we translate the study of this algorithms to a proof of concept in a real industrial scenario?
- Are the selected algorithms feasible for an industrial application?

The part II of this thesis studies existing methods to produce more reliable counterfeit detection approaches to operate in real environments. This second part transitions from hand-crafted textures to learn textures introduced by convolutional neural networks. We also propose to use an end-to-end algorithm to which proposes where to look at each texture patch. In this part we deal with the following questions:

- Which texture features are better suited for the presented approach?
- Are the texture descriptors performance statically relevant?
- How the trained models generalize to new background textures of unseen documents?

- How to find where to look at each patch?

Last questions leads to the part III of this dissertation, in which we pose the problem as an anomaly detection. The lack of counterfeit samples in this domain made us move towards the creation of a robust manifold which could represent most of the non-anomalous data. Finally, we pose the questions:

- How to apply anomaly detection for the current problem?
- Can we improve counterfeit detection using a robust manifold optimization?
- Can we extend this approach from one-vs-all approach to multi-class?
- Is it possible to convert the problem to unsupervised?

The answers to these questions across this thesis, from the point of view of computer vision and machine learning, will help future researchers an industry to continue improving counterfeit detection setting our approaches to the problem as a baseline. We expect the proposed solutions used at this dissertation will produce mature counterfeit detection systems which can bring benefits for the society.

1.6 Outline

Chapter 2 corresponds to the related work in counterfeit detection. Here we divide the state of the art work in this fields by topics. From the hand-crafted features to more recent learned-based features with the introduction of the convolutional neural networks.

Chapter 3, inside Part I, refers to the creation of the dataset and how are we going to treat the documents for counterfeit detection. Chapter 4 studies the viability to approach the problem of background texture as a sparse coding dictionary representation. This corresponds to a first attempt to solve the problem at hand with already existing approaches. Also contained in part I, chapter 5 develops a service-oriented architecture for counterfeit detection. It is presented the server and client side of the full system, thought to be deployed at an industrial scenario.

Part II corresponds to the concept of the transition between hand-crafted features to end-to-end learned-based descriptors. The second part of this document, extends in chapter 6 the idea of using already existing texture descriptors doing a more complete and comprehensive evaluation in terms of computational time efficiency and accuracy performance. At this chapter we introduce already some of the most relevant convolutional neural networks and apply transfer learning to counterfeit detection. An statistical evaluation is performed to be able to compare

the large list of evaluated algorithms. Chapter 7 focuses in learning an end-to-end system which learns a metric to compare between patches of background textures. In addition, it presents a way to center the attention of the system to the most relevant regions of the compared textures.

Part III is centered into the anomaly detection concept and how can this be applied to the counterfeit detection. Chapter 8 deals with the scarcity of counterfeit examples in the dataset and focuses in the need to detect the outliers. Within this chapter, we want to create a manifold where most of the genuine sample can fall into.

Finally, chapter 9, last chapter of this thesis presents the general conclusions and future perspectives of this PhD thesis along with a summary of scientific contributions and related deliveries of this thesis.

2 Related work

One of the contributions of this thesis is the creation of a survey in identity documents and banknote security forensics. To the best of our knowledge this is the most complete analysis and comparison of the literature in anti-counterfeiting security features. From the non-experienced to professionals in security documents, can be introduced or deepen its knowledge in this topic respectively. From history of counterfeiting, effects on society, security features, counterfeiters types of attacks, trends among others can be found in this chapter.

2.1 Why another survey?

Different surveys about counterfeit has been presented over the years, most of them related with banknotes. The sparsity of the presented topics in the previous surveys created a need for a complete survey. To our point of view all of them lack completeness to present a general idea of all the broad subjects that involve counterfeit in security documents. Next we compare in Table 2.2 different surveys for counterfeit security feature detection. The work presented in [218] A survey of security features containing optically invariable devices and optically variable devices to measure its practical value for document security. It does not compare algorithms or approaches and it is for both banknote and identity documents. The main feature of this work is that it orders the security features by degrees of order and degrees of security. Being the degrees of order the size in mm need to inspect each one of the security features. More than 20 years has past since this survey was done, so it is not up to date with the new security features. In [204] an overview and comparison of digital watermarking techniques is presented. Although this survey does not fit entirely to the study of anti-counterfeits features in security documents, it does introduce the concept of securing documents by introducing unique watermarking codes. The survey in [151] centers in counterfeit paper currency recognition and detection. They detect fake banknotes, but some of the

approaches presented, centers the counterfeit detection in the recognition of the banknotes instead of the anti-counterfeit security features. If the banknote is not recognized by the classifier then it may be considered as a fake banknote. The work in [153] does a comparative study on security features of banknotes. It does not compare approaches, but show graphically different examples of banknotes what are the security features and where are located. The thesis in digital currency forensics in [47], contains a review for the security anti-counterfeit measures in banknotes, it contains some of the sections presented at the present survey. The fact that is a thesis and not a survery, explains why it needs a better comparison of the approaches presented and a clearer structure of the security features works explained. The survey in [43] for currency note authentication techniques lacks of a better comparison between the different approaches and expand the literature compared. In [134] a complete and easy to read survey on banknote recognition methods is presented. They focus in the recognition and counterfeit detection, with a large literature. They also include many comparisons and even does an study of the datasets available in recognition and counterfeit banknote detection. The inclusion of the recognition process of the banknotes makes that the counterfeit part is not as complete as it should. Our work also has a better explanation of each of the security measure present in security documents. In a more recent survey for conterfeit currency detection techniques in [216] explains what are most of the anti-counterfeiting techniques and which Rupee banknote denominations includes them. Most of the works compared are centered on the Rupee. This work lacks of a comparison between approaches presented. Finally, the only survey in identity documents is presented in [107]. Different approaches are presented and explained what could be the improvements and weaknesses of each method, but needs a better comparison between those methods and also to explain the dataset context to understand the experimental results.

2.2 A brief history of counterfeit detection

Counterfeit is as old as the alphabet or the money itself, sometimes referred too as the "2nd oldest profession" in the world [231]. In the ancient world, it was not unusual for the workers at the forge to duplicate coins by using gold plated bronze and not pure gold. Augustus Caesar and other rulers of the day were quick to see the implications and imposed heavy penalties, often death. Shaving the coin edges was a common practice to produce counterfeit coinage. Laws against counterfeit can be traced to the years 80BC when the Romans established a permanent court to try cases involving forgeries of all sorts, including currency counterfeit [23] or falsification of documents that transferred land to heirs [5].

Table 2.1 – Survery comparison. Identity/Banknote docs: survey done for IDs or banknotes. Counterfeit history: history of counterfeit. Effects Society: causality between the counterfeit and the effects in society. Document experts: figure of a document expert. Security Substrate/Ink/Printing: what are the anti-counterfeit features for these categories. Type of attacks: types of attacks done by the counterfeiters. Digital Tampering: digital watermarking approaches. Datasets: datasets of the presented approaches. Approaches: state-of-art works in counterfeit. Systems and apps.: state-of-art works contain systems and applications for mobile devices. Trends: general direction guidelines. *: Present work.

Features	[218]	[204]	[151]	[153]	[47]	[43]	[134]	[107]	[216]	*
Year	1995	2013	2014	2015	2015	2016	2017	2017	2018	2019
Identity docs	✓							✓		✓
Banknote docs	✓		✓	✓	✓	✓	✓		✓	✓
Counterfeit History					✓					✓
Effects Society										✓
Document Experts										✓
Security Substrate				✓	✓				✓	✓
Security Ink	✓			✓	✓				✓	✓
Security Printing	✓			✓	✓		✓		✓	✓
Types of attacks										✓
Digital tampering		✓			✓			✓		✓
Datasets							✓			✓
Approaches		✓	✓		✓	✓	✓	✓	✓	✓
Systems and apps.			✓		✓	✓	✓	✓	✓	✓
Trends										✓

Chinese started carrying folding money during the Tang Dynasty (A.D. 618-907), mostly in the form of privately issued bills of credit or exchange notes [171]. Wood from mulberry trees was used to make the money. To control access to the paper, guards were stationed around mulberry forests, punishing thieves entering the forests to death. Since then, the crime of counterfeit money has been practiced in every country where writing existed and paper was used for financial transactions. Europe took around 500 years more to start using paper bills, where the practice began to catch in the 17th century. English couple Thomas and Anne Rogers were convicted for counterfeiting 40 pieces of silver. Thomas was hanged, drawn and quartered while Anne was burnt alive. Forms of punishment were considered acts of treason against state or Crown, rather than simple crime. In 1739, similarly in America, Benjamin Franklin intentionally misspelled the word 'Pennsylvania' on his bills to catch forgers who corrected the error [30]. In the late 18th and early 19th centuries, Irish immigrants to London were associated with the spending of

counterfeit money [64].

Particularly the production of counterfeit money has been used by nations as a means of warfare, to overflow the enemy's economy with useless fake banknotes, so that the real value of the money plummets. Great Britain use this strategy during the American Revolutionary War to reduce the value of the Continental Dollar. During the American Civil War, counterfeited Confederate States dollar was mass produce by private interests on the Union side. Thanks to the access to modern printing technology, the imitations were often equal of even superior quality compared with the Confederate money. In the 1920s Hungary was engaged in a plot to purchase 10 million fake Francs as a move to avenge their territorial losses in World War I. Unsuccessfully during World War II, the Nazis attempted to collapse the Allies economy (Operation Bernhard) [32]. Jewish artists in the Sachsenhausen concentration camp were forced to forge British pounds and American dollars. The outstanding quality of the counterfeit money made almost impossible to distinguish between the real and fake bills. However the Nazis could not carry out the planned aerial drops with the counterfeit money over Britain and America.

Today the most sophisticated counterfeit bill ever produced and undetectable even to currency experts are the "Superdollars", because of their high quality, and likeness to the real US dollar. The origin of this banknotes is unclear, where North Korea, Russia or even the CIA has been accused [10, 100].

Not as well documented as the history of counterfeit money, notorious forgers of identity documents have also existed since the old days. After the end of the World War II, many officials and high-ranking Nazis forged identity documents to flee from Germany. Like Adolf Eichmann, referred as the "architect of the Holocaust", escaped to Argentina using a "laissez-passer" issued by the International Red Cross under a fraudulently identity [101]. Alexander Viktorovich Solonik, a hitman and a Russian gangster in the early 1990s, lived in Greece using a fake passport issued in the consulate in Moscow [103]. Also famous was the arrest of Kim Jong-nam, the son of North Korean dictator Kim Jong-il, who was detained by Japanese immigration official travelling with a forged Dominican Republic passport [104]. One of the greatest counterfeiters of the 20th century was Adolfo Kaminsky [102]. A former member of the French Resistance during the World War II, forged papers to save the lifes of 14.000 Jews. Afterwards he continued forging papers for various groups during 30 years trough different wars [120].

Last decades the control of identity documents and banknotes were exclusively controlled by document experts. Usually country border controls or banks did not had at their disposal automatic software to validate security document, which made the authentication prone to human errors. The apparition of computer vision and machine learning in the 50s-60s decades, has helped to develop new algorithms to automatically detect counterfeits documents. With machine learning it is even

possible to render new text in someone's handwriting, producing novel images of handwriting that look hand-made to casual observers, even when printed on paper [99]. Nowadays counterfeiters are using AI and machine learning to make better fakes [6]. At the same time researchers and authorities are developing new methods using AI to spot them.

Government authorities and counterfeiters have been playing a game of cat-and-mouse, as soon as new security features are added to the security documents, criminals try to copy them. Today, unlike a millennium ago under the rule of Emperor Augustus, fraudsters don't need to fight lions in the Roman stadium if they are caught, however severe forms of punishment exists differentiated by country [8]. Banks and government authorities need to have strong lines of defense against fraudsters of security documents. If they find themselves the weakest link, they can guarantee fraudsters will attack.

2.3 Effects of forgery in society

Counterfeit objects produced for criminal activity not only causes potential harm to the health and safety of the citizens, it also affects legitimate economies, contributing to reduced revenues for the affected businesses, decreases sales volume and job losses. According to a 2013 report, the OECD estimated counterfeit goods accounted for 2.5% of global trade [160]. Currently, trade of counterfeit and pirated goods represents $1.7 trillion per year and is expected to grow to $2.8 trillion and cost 5.4 million jobs by 2022 [88]. In 2018, counterfeit was the largest criminal enterprise in the world, more than drugs and human trafficking [88].

From the different types of counterfeit document fraud continues to play a key enabling role in trafficking of counterfeit goods. Counterfeiting goods is an important source of income for organized criminal groups. At the stage of distribution of counterfeit goods, fraudulent retail licences enable the infiltration of the legitimate supply chain. Generally, in order to run their illicit businesses, counterfeiters establish companies and bank accounts using fraudulent identity documents (ID) or under the name of a front person, and regularly make use of bogus invoices. Counterfeiters purchase or rent vehicles using fake documents. Number plates of cars belonging to criminal groups are registered abroad or under a fake identity. Fraudulent documents are widely used to facilitate the transportation, distribution and sale of counterfeit goods. For the purpose of importation, counterfeiters provide false shipping documents, such as bills of lading, to conceal the content of containers of packages and the origin of shipments. They often use false invoices issued for imported goods in declarations to customs. This practice is also used to undervalue their imported products.

Banknote counterfeiting is another illegal lucrative business for the counterfeiters. Through recorded history currency has been used as a medium of exchange for goods and services. Paper notes, coins and electronic currency are the general accepted form of trade. Governments of each country using central banks are the responsible to issue money and circulate it within an economy. Currency only holds its value as long as users have confidence in its authenticity to represent goods. A common threat for any economy is the quantity of counterfeit money which is being used in the actual market. Higher than previous years, in the first half year of 2015, 454K counterfeit Euro banknotes were withdrawn from circulation, being 86% of the counterfeits from €20 and €50 banknotes,[21].

The *modus operandi* in counterfeiting and piracy have partially changed over the past few years and are expected to evolve further in the future. To be able to carry out such a variety of activities, criminal groups need stable access to resources. However, this does not seem to pose any major difficulty for criminals. Widely available and affordable information and communication tools increasingly facilitate their activities.

2.4 Document Experts

The nature of document counterfeits is such that the initial encounter with a document requiring authentication is rarely within a specialized document forensics laboratory [200]. A passport may first be viewed by immigration or customs officers, currency by a shop assistant or a bank clerk, identity documents by a transport authority officer, etc. At this first step is where most of the counterfeits go unnoticed, just a small percentage are detected if the inspection is done by an a person without the proper training. After some assessment, if a security feature integrated in the document seems altered, the document is given to a specialist examiner.

The examiner looks for combinations of significant similarities and combinations of significant differences between the questioned document and an exemplar document. If the examiner finds combinations of significant similarities between the questioned and the exemplar, the examiner may conclude it is dealing with a genuine document. Otherwise, if significant differences exist between the compared documents he may determine is a case of counterfeit. Although this principle of comparison seems simple and sound, the reality is far from simple. The terms "significant similarities" and "significant differences" are subjective [76]. The examiner must ultimately decide what is significant and what is not. These decisions come from the examiner's knowledge and understanding of class characteristics, individual characteristics, and all the environmental facts that can affect the security document, such as the wear and tear, dirt, lightning conditions on how the

document is checked, etc. The authenticity response is highly dependent with the document examiner knowledge. The knowledge is acquired through intensive supervised training and much practical experience. The economic effort to train a document expert is high and usually there is a shortage of people who can effectively do this task.

The research of new algorithms to automatize this chain of processing of inspection is to make the authentication less prone to human errors. Nowadays, algorithms to detect counterfeit documents are still far from the accuracy of document experts and their examination laboratories. 60% of fake documents can be detected through detection machines or algorithms for counterfeit detection while 80% can be detected by document experts [152]. These data shows that most of the fraudulent documents have not yet been detected. Most researchers focus nowadays into the first level of the chain, where counterfeit detection is done by untrained personnel, and is possible to catch a bigger percentage of fraudulent documents.

2.5 Anti-counterfeit measures

Banknotes and identity documents contain specific security features for protection against counterfeit and fraud. Each year more and more security features are included in their designs in order to ward off potential counterfeiter, fraudsters and impostors. A single feature can never provide the level of security needed for this type of documents. The key for a robust and secure document document is the combination and connection of different anti-counterfeit measures.

Security patterns are specially designed with distinctive characteristics in the hope that people can easily recognize them. Three easy-to-follow methods can distinguish genuine banknotes or documents from counterfeit ones: feel, look and tilt. The first method correspond to touch the material of the document and check the surface does not present anomalies. The second method is to observe the document when hold against the light and compare it with a known genuine document. Last method, tilting indicates the security measures printed with special ink, optically variable when viewed at different angles. Moreover it is possible to check for more advances security features with specialized equipment.

The security features are designed to resist deterioration for reasonable wear and tear and robust to forgery. Security features against forgery can be categorize in three types: Substrate materials used for the fabrication of the document, the type of ink and the printing design, see Table 2.2.

Table 2.2 – Security features types classified by fabrication materials, ink used and printing process or design. Not all existing security types are included.

Substrate	Ink	Printing
Complex substrate recipe	Complex ink recipe	Offset Lithographic
Windowed security thread	Colour-shifting ink	Intaglio printing
Security fibres	Ultra violet ink	Personalization
Watermark	Infrared ink	
See through windows		

2.5.1 Security Substrate

Paper results from compression of different plant fibres. The substrate of security paper is manufactured for one particular application and for one particular contractor only; hence, it is not commercially available for the general public. Generally, the substrate is made of paper, almost always from cotton fibres for strength and durability. The security paper is usually provided with chemical reactants, watermarks, fibers, planchettes, and threads to add individuality and protect against counterfeiting. In later stages various types of mechanical perforation and laser perforation may be put to use to further enhance the security level. The majority of security paper manufacturers prefer the production of security documents with paper due its lower cost. Gaining popularity is the use polymer security documents made from BOPP, which stands for Biaxially-oriented Polypropylene [174]. The polymer fabricated documents are longer lasting, harder to destroy, waterproof, have better dirt resistance, and can be recycled when taken out of circulation decreasing the environmental impact. However, polymer documents can not be easily folded and can be permanently damaged if exposed to a heat of around 100° C. All security features from paper can be incorporated in polymer documents and allows to include new security features which can not be applied to paper. For instance, the inclusion of a small transparent windows (few milimeters in size) as a security feature, also name see through windows, is difficult to reproduce using common counterfeiting techniques [117]. Polymer documents usually incorporate *Optically Variable Device* (OVD) as a security feature and are very hard to counterfeit simply because many of its unique security features cannot be reproduced by scanning and photocopying them. Brightness reflected by the substrate composition can be also used as a security feature [28, 68, 243]. However, brightness will also be affected by the inks and printing.

Substrate embedded security features

Opacity is an intrinsic property to the paper substrate. It describes the amount of light which is transmitted through the paper. A complete opaque object is one which allow no light to pass through it. Cellulose fibers, the primary component of paper, are transparent, but stacking them and creating a web structure with them diffuses the light through the sheet and increases the paper opacity. Paper opacity determines the extent to which printing on a particular side of paper will be visible from the reverse side, named *show-through*. Manufacturers exploit this property to embed latent security components between the layers of the substrate. This also applies to polymer substrate where latent images or security components are hidden from normal view. Opacity also affects to the printed inks on the substrate, determining the level of transparency of the security document. Opaque pigments will block light to pass through and transparent pigments will allow varying amounts of light to pass trough the substrate, revealing the reverse side background printing of a sheet of paper.

Watermarks is a very well-known and reliable security feature for protecting documents against counterfeiting. Cylinder mould process is the preferred way to embed a watermark for banknotes and IDs. A cylinder covered by a wire mesh embossed with the watermark design rotates in a vat containing cotton pulp. The suspension of cotton fibres is agitated in the vat and the wire mesh retains the fibrous material in the hollow areas. The variations of fibre density forms the image of the watermark. The variation of fibre density produces areas with different paper thickness. Varying thickness of paper produces different shades of lightness/darkness when holding the document up to the light, or shining one through the paper. When a genuinely watermarked paper is held to the light, the thicker areas of the paper appear dark, and when placed beneath a light the dark areas appear lighter. The watermarks are used for displaying portraits and motifs. Given the high level of recognition of watermarks around the world, even tiny defects in the portrait or the motif are detected instantly. While the new polymer banknotes produced do not have watermarks, a very similar security features is produced by setting an image into one of the polymer substrata during manufacture. In the $5 note it is Australia's coat of arms in the top left of the note. Different works include the watermark analysis [50, 173].

Woven into the layers of the substrate, *coloured and fluorescent fibres* are embedded within the paper during its manufacturing. They appear as thin elements scattered all through the paper. These fibres are not visible under normal light, but under ultraviolet light the threads glow. They represent an effective feature to protect any document at a cost-effective price and are present in most banknotes and passports. Authors in [50] uses spectral analysis to the reflected signal of fluorescent

fibres.

Security threads are threads of natural or synthetic material placed in the paper during manufacture. Incorporated at the beginning of the paper production process, similarly to the security fibre, is embedded between the layers of the substrate, except it is placed in a regular position. Different variations of security threads has been developed. "Morse code" thread has solid and translucent sections. It is possible to read Morse code characters at the broken line created by the solid region when held to the light. Similarly "Microprinted" thread, shows microprinted writing on the translucent section. Usually, in banknotes the writing correspond to the initials of the issuing authority. The "contoured" thread is a wide thread that has one straight side and one wavy side, with the wavy side pointing either to the left or right on the document. "Windowed" threads, is the latest development in the use of security threads, more difficult to forge as threads are woven in and out of the note surface. Viewed normally it looks like it is appearing and disappearing at regular intervals at the surface of the paper. When held up to a light source it appears as a continuous line, although slightly broader. These variations can be combined to add further complexity to the security thread. Security threads are widely used in banknote and ID papers to deter counterfeiting, being reliable features as they are impossible to photocopy.

Likewise security fibres or threads, it is possible to implant small printed pieces of metal in the substrate, also named *planchettes*. They held the same properties as when held up to a light source or exposed to UV light only. Planchettess are minute disks, metallic or transparent, ranging from about 1 mm to 5 mm in diameter. Microprinted text or symbols can be added to the planchettes.

Usually counterfeiters include imitation security fibres in their document replicas, being this one a low security measure, however it is not obvious to the general public. The same applies to the security thread or planchettes, depending on their complexity.

Spectrography

Some of the previous substrate security features can only be inspected with specialized devices capable of producing different light waves to the security document, like ultraviolet light. These devices are based on *Spectroscopy*. Spectroscopy is the science related with the measuring and investigation of spectra produced when matter interacts with or emits electromagnetic radiation. For the analysis, a device separates separates incoming light waves reflected from the document substrate into a frequency spectrum for its analysis. Using a spectrography microscope it is possible to analyze different security components hidden to the naked eye, like the security fibers or embedded motifs made with security inks, go to 2.5.2 for

more details. Most of this forensic analysis can be done using infrared and UV spectrum. A procedure based on the analysis of several areas of euro banknotes using microscope ATR-infrared spectroscopy is proposed in [223].

Mössbauer spectroscopy is a non-destructive chemical analysis which probes very small changes in the energy levels of an atomic nucleus in response to its environment. Using this technique it is possible to determine the atomic composition of the pigments used in the substrate. The concentration of pigments in the printer ink used and the specificity of their Mössbauer spectra can be used to identify fakes and forgeries [184]. Same authors showed that Mössbauerr and X-ray fluorescence studies revealed that a significant number of banknotes are printed using pigments which contain considerable amounts of iron [185].

Similarly to Mössbauer, *Raman spectroscopy* is a powerful method for material identification, capable of recognize different substances and their structural modifications. Any differences in the composition of the inks or in the paper should appear in their Raman spectra as a presence or an absence of particular peaks and their distribution in spectrum. An important drawback of this method is that Raman spectra has a weak effect in comparison with luminiscence security features. The stronger quantum effect of the luminiscence intensity can overlap the Raman spectra and mask spectral information.

Fingerprinting paper surface

Low-cost physically unclonable functions (PUFs) as been receiving increasing attention in both research community and industry for counterfeit detection. Paper surface formed by overlapped and inter-twisted wood fiber forms an inherent unique 3D structure. The imperfections of a surface paper sheet caused by the manufacturing process can be used to uniquely identify the paper [38]. It is extremely unlikely that two document surfaces created with the same raw materials will be identical, although they will present similarities. Paper texture lead to unique maps of surface norm which can be transformed to a unique digital representation of the paper, named *paper fingerprint*.

Paper fingerprints can be effectively extracted with commodity scanners, scanning the paper surface from four different angles and then construct a 3D model, which later can be condensed into a feature vector [57]. Paperspeckle is another approach to extract the paper speckle patterns at microscopic level [196]. The authors use a microscope (with a 10-200X zoom) joined with an inbuilt LED source as the light which falls on a paper sheet. They microscope is then connected to a mobile device. A binary fingerprint is built with the randomly mixed dark and bright regions formed by the scattered light. They also demonstrate how this method produces a repeatable fingerprint even if the paper surface is damaged due to

crumpling, printing or scribbling, soaking in water or aging with time. Following the same line of work, other works carries out an study of how high resolution photos of paper surface acquired distantly using industrial acquisition devices have good authentication performance, whereas the extension into using built-in cameras of mobile phones has acceptable performance at a higher computational cost [70, 71, 225]. The industrial acquisition device (resolution of 5Mp) builds a micro-structure database of fingerprints under a controlled lighting environment. Later the verification can be done with a handheld camera (resolution of 2MP without optical magnification) in a different external environment. The drawback of this approach it critically depends on excellent lighting and acquisition conditions. Mobile cameras have not a substantial success in obtaining consistent appearance images due to the uncontrolled nature of the ambient light. To solve this drawback, it is possible to use multiple camera-captured images at different viewpoints to estimate the paper surface [235]. Exploiting the camera flashlight the authors create a semi-controlled lighting conditions. Although authors use different smartphones to acquire a square-shaped paper dataset, needs further study on how it could performs with ID documents or banknotes exposed to day to day degradation caused by the normal used.

It is also possible to exploit for PUF authentication purposes the embedded paper features instead of just focus in the substrate texture. The generation of spontaneous bubbles in a polymer it is being used commercially for anti-counterfeiting purposes [9]. They use a transparent polymer material that generates bubbles at complete random when manufactured. The bubbles positions, sizes and shapes constitutes a unique fingerprint impossible to replicate which is sensible to small variations. The use of randomly distributed visible fibers or color dots on surfaces can be also used to provide uniqueness [7, 9]. A comparison study of some of the mentioned previous PUFs to gain a better understanding of the factors affecting the performance under mobile imaging [234]. They claim that due the uncontrollable light sources, and limits in camera resolution and focusing capability, the patch image intensity maps have a bad performance for pixel-domain correlation detector. They have also found that the density of foreground objects at the paper textures have a strong impact on the authentication performance.

A novel paper fingerprinting technique is proposed by the authors in [213]. They propose to fingerprint the paper sheet based on its texture patterns instead of features on the surface as performed in previous works. An analysis of the translucent patterns revealed when a light source shines through the paper. The fingerprinted patterns represent the random interleaved wooden particles inherent to the manufacturing process of the texture paper. They report zero error rates for the collected databases and to be robust against various distortions such as crumpling, scribbling, soaking and heating. The authors also demonstrate that the

embedded paper texture provides a more reliable source for fingerprinting that feature on the surface. A drawback to this method is that the light needs to go through the document to be able to analyze the translucent patterns. They also use a camera-based acquisition device able to acquire images at high resolution and able to capture photos in a macro mode from a short distance (minimum 1 cm focus). A study should be done with smartphone cameras in a similar settings.

Table 2.3 – Summary of research works of anti-counterfeiting substrate features for banknotes.

Type	Feature	Method	References
Substrate	Brightness information	luminance histogram	[28, 68, 243]
Spectrography	Iron concentration	X-rays and Mösbauer	[185]
Spectrography	IR patterns	Fourier transform infrared	[223]
Embedded	Watermarks, Security Threads	binary segmentation	[173]
Embedded	Watermarks, Security fibers	spectral analysis	[50]
PUFs	paper substrate texture	norm map	[57]
PUFs	paper substrate texture	texture microstructure	[70, 71, 196, 225, 235]
PUFs	embbeded paper features	2D/3D bubble shape and location	[9]
PUFs	embbeded paper features	fibers, coloured dots shape and location	[7, 9]
PUFs	embbeded paper features	translucent patterns	[213]

Authenticating security documents using PUFs seems extremely robust in theory, especially through values stored in a database. From the banknote and IDs authentication point of view, using PUFs requires further studies of its resilience against tampering of the surface paper, like scratching, folding, crumpling, and on the reliability of the physical structure over their lifespan. The fingerprint could change over time due the damage that naturally and inevitably occurs as a result of normal wear or aging. Making irrelevant the initial stored database hash fingerprint for the authentication.

2.5.2 Security Inks

Security features further into their level of user concealment, named *overt*, *semi-covert* and *covert*. Overt security features indicates is directly perceptible by one or more of the human senses without recourse to external devices. Oppositely, covert means not directly perceptible by the unaided human senses and detectable only through the use of purpose-built tools or professional laboratory equipment. On the other hand, semi-covert stands for not directly perceptible by the human senses but detectable by those senses through the use of non-professional external devices. Chemical and physical analysis of inks on questioned documents provides valuable information regarding their authenticity. Inks can by also categorized by

their concealment level, see Table 2.4.

Table 2.4 – Security ink types classified by levels of concealment. Covert means a hidden ink invisible to the naked eye. Overt has the opposite meaning of covert and allows an inspector to verify the ink with a glance.

Overt ink	References	Semi-Covert ink	References	Covert ink	References
Optical Variable		Reactive		Biometric	
Holographic		Thermochromic		Invisible UV	
Iridescent		Metameric		Invisible IR	
Watermark		Photochromic		Magnetic	
See through windows		Phosporescent		Machine-readable	
		Fugitive			

Many security printing inks rely upon the absorption of UV radiation and its re-emission as visible light. For that reason, to work correctly, some security printing ink designs needs to be printed on UV-dead or uncoated paper. If no UV brighteners are present in the substrate it will work at other documents [226]. Additionally the printer can overprint varnishes and laminates, jointly with the security printing inks, to increase the difficulty to the counterfeiter.

Optical Variable ink (OVI) are tiny flecks of metallic film which changes color when viewed from different angles. Colour-shifting inks reflect various wavelengths in white light differently, depending on the angle of incidence to the surface. OVI ink is extremely expensive and is generally used only in small areas. It needs to be printed in heavy weight and is sometimes printed using the silk screen process. Most common colour changes are brown to green (and viceversa) as well as red to purple. Ink feels almost embossed on the substrate which is due to the amount of ink required to get the required effect. Authors in [50] analyzes the reflected spectral signal to extract the OVI.

Holographic ink is used for one of the most known overt features, which is the *hologram* and its being used to protect a broad amount of documents like credit cards. An Hologram incorporates an image with some illusion of 3-dimensional construction, or of apparent depth and special separation. They can be incorporated into tear bands in overwrap films, or as threads embedded into paper substrates. However, some hologram labels have been easily and expertly copied or simulated, and may often rely on hidden covert elements for authentication. Recently researchers have created a way to not only print chromatic holograms on any surface but also to create high-quality organic piezoelectric structures [123, 188]. Holograms are a type of OVD. OVD, based on diffractive optical structures, often without any 3D component is an image composed by an *iridescent ink* which exhibits various optical effects such as movement or color changes. OVD can be

created through a combination of printing and embossing. They are generally made up of a transparent film which serves as the image carrier, plus a reflective backing layer which is normally a very thin layer of aluminium. Other metals such as copper may be used to give a characteristic hue for specialist security applications. Extra security may be added by the process of partial de-metallization, whereby some of the reflective layer is chemically removed to give an intricate outline to the image, as can be seen on many banknotes. Alternatively the reflective layer can be so thin as to be transparent, resulting in a clear film with more of a ghost reflective image visible under certain angles of viewing and illumination. Partial removal of the metallic layer is a more restricted process and thereby increases both the level of security and the cost.

Inside the semi-covert ink category, *Reactive ink* is also referred as solvent sensitive. This type of ink can detect when there is an attempt to alter the document by a solvent or chemicals, such as bleach, alcohol or acetone. Reactive ink is usually found where variable data is printed on, these inks will run, change color, or cause a stain if an attempt to remove or alter information has been made. Reactive ink is commonly found in cheques, and is used on a printed watermark or fine guilloche artwork design.

Thermochromic ink is designed to be sensitive to temperature. It will appear or disappear at different temperature ranges. If you were to apply a thumb to a 15°C dark blue printed thermochromic spot the ink would disappear to nothing and as soon as you removed the heat source the ink would re-appear again. While it comes in a variety of temperature sensitivities, common temperatures available are 15°C, 31°C and 45°C. Before using this industrial ink, it's vital to consider the temperature conditions to which it will be exposed from the time of imprinting through its lifecycle. In hotter climates might be needed higher temperature inks as the it could be invisible from the ambient temperature itself. Some are available as a permanent change. e.g. when it has reached a temperature the ink colour does not reverse.

Metameric inks corresponds to a pair of inks formulated to appear to be the same colour when viewed under specified conditions, normally daylight illumination, but which are a mismatch at other wavelengths. *Photochromic ink* darkens, as the light level increases. It contain special chemicals which when exposed to ultra violet light e.g. sunlight, change from almost colourless to intense coloration. When removed from the source of ultra violet light, these inks revert to their colourless state. The photo-induced coloration commonly found in sunglasses may be used as anti-counterfeit markers on banknotes and documents such as passports. [110].

Phosphorescent inks glow in the dark after having been exposed, for a variable period of time, to daylight. They are able to absorb the brightness and emit light even after the radiation, responsible for the fluorescence, is no longer present. The

length of glowing time of the inks depends on the pigment type, the time of light exposed and the quantity of ink.

Fugitive ink, also known as aqua fugitive inks, is designed to react similarly as reactive ink. Any form of alteration attempt (with water or an aqueous solution) on a security document with fugitive ink, the ink will run, causing it to smudge and become unreadable. Even wiping the finger with saliva on it across the printed background will make the printed pattern ink smudge. There exists combined *solvent sensitive aqua fugitive inks* which combines both functions of reactive and aqua inks.

Among the various types of biometric personal identification systems, DNA provides the most reliable personal identification. *Biometric inks* contain DNA taggants (uniquely encoded materials, like a fingerprint's signature of identity) which are virtually impossible to duplicate and represent the ultimate marker for security purposes [106]. Special machines are designed that can read the tags, or the tags can be manufactured to react when a particular solvent comes in contact with them. Each batch of printed documents can contain different biometric properties. These are completely covert but require specialist methods to validate the authenticity.

Predominantly used where numerical sequences or serial number security is important, *Magnetic ink* contains minute magnetic flakes designed to communicate with electronic readers for document verification. Most common example of these is bank checks that use MICR (Magnetic Ink character Recognition) technology for highly sensitive data like check number, account number, and sort code of the bank. Magnetic ink is a type of *Machine-readable inks* which at its name implies are the inks made to be only read by a determinate type of specialized equipment or solution. The main objective of these inks i to address the increased challenges of automated document security handling. Pulse eddy is an advanced electromagnetic inspection technology, that can be used to test magnetic inks or security threads [175].

Invisible or fluorescence ink is the most commonly used security ink. Designs printed with fluorescence ink, invisible in daylight or artificial light, becomes visible when exposed to a black lamp (or UV light source) and does not produce, as it is the case with phosphorescence, any after-glow (persistence of fluorescence after switching off the Ultra Violet light). Invisible inks can be alcohol based or acetone based and either have white pigments or are without pigments. The composition of the ink can be controlled with additives to impact the response of the ink to a particular wavelength of ultra-violate or Infrared light. The ink must be applied to a UV dull substrate otherwise it will not be visible. As invisible ink is carried by the solvent it is relatively cheap and is available in many colours. UV inks are used in conjunction with a security background design to provide a higher level of document protection. *Secondary Fluorescing ink* works in the same way as

fluorescing ink however it will not glow or show under a black lamp unless an alteration or tampering on the material has occurred. For example, the secondary fluorescing ink will look green under UV light, but changes to red (secondary color) if an alteration has occurred. It is also possible to determine the fluorescence lifetime to discern the differences between genuine and counterfeit currency, using a two-photon microscope [54].

At infrared spectrum it is also possible to search for local defect due deterioration (like tears, stains or holes) along with the anti-counterfeit features [119]. Other works prefer to binarize and segment the image searching for IR patterns [37, 41, 135].

Table 2.5 – Summary of research works of anti-counterfeiting ink features for banknotes.

Type	Feature	Method	References
OVI	OVI digits	spectral analysis	[50]
Fluorescence	fluorescence lifetime	fluorescence spectra	[54]
Magnetic ink	magnetic inks, Security threads	pulse eddy	[175]
UV	paper substrate texture	norm map	[57]
IR	paper substrate texture	texture microstructure	[70, 71, 196, 225, 235]
IR	Patterns	binary segmentation	[37, 41, 135]
IR	Patterns and defects	mesh of control points	[119]

2.5.3 Security Printing

Printing, the application of colour, consists of two main components: pigments, solvent. In addition modifiers and additives, like driers, waxes or anti-skinning agents are added to the ink to change its properties. Pigments are the ingredients that comprise the color of the ink. The ingredients are formulated from substances, found in nature or produced synthetically, which create the desired color when blended together in specific proportions. The solvent combines the pigment with the drying agent, responsible of speeding up the ink drying process and bind the pigment to the substrate. Wax additive improves the slip and scuff resistance of the ink, it also reduces the possibility of the ink to be transferred from one sheet to the back of another sheet. Anti-skinning agent adds the property of keeping the ink from drying too rapidly and skinning over in the ink fountains of the printing press. Offset Lithography and Intaglio press are two primary security document printing methods, differing between them by the solvents chemical composition used.

Printing processes

Although not a secure printing process in its own right, *Offset Lithographic printing* is the most common commercial printing process used in secure documents. Often used as a security feature, background printing represents a great portion of the overprinting of any security document. The image on the printing plates is defined by raised areas. The raised areas are inked up and instead of being transferred straight to the paper the design is transferred or offset to a rubber blanket. The print is then transferred from the blanket to the paper. Lithography is used for most of the background printing and is the first to be printed. Lithography requires a different printing plates for each color of components present at the background design. The ink is oil based and the resulting print is flat crisp, sharper line on edges, and a brighter overall results than Intaglio press printing.

Intaglio printing plates have the image area etched into them. The plate is inked up and wiped, having only ink in the recessed areas. The ink from the plate is then directly transferred onto the paper substrate at a high temperature and pressure (with one metric ton per cm linear). The printing conditions are such that the paper is sucked into the recesses in the plates and deformed. The ink then sits on top of the paper deformations and hence a tactile effect results from a combination of paper deformation and ink thickness. Ink dries by evaporation, being the drying longer than Offset Lithography. This longer time of drying causes an ink feathering effect, where the edges appear to run. This printing technique and the capillary effect lead to embossing of the substrate and the tactile high amount of ink. Intaglio printers can produce non-uniform quality standards and regional production disparities of an Intaglio print appearance. This difference in the look of an intaglio zone, may confuse security document reviewers and help counterfeiters to produce an similar intaglio respect the genuine one. To reduce this variability and quality deviations, Intaglio quality analysis and measurement can be performed[92, 112]. To describe quality levels they use Intaglio line discontinuities, bleeding and inner holes in the lines as well as large areas without ink.

Intaglio printing has a distinctive feel to it and can also be checked easily, simply by running a finger over the printed page. Intaglio printing process can produce *latent images* as a counterfeit security measure. Latent images can be viewed when tilted and illuminated using side/oblique lighting. When viewed straight on, a latent image reveals nothing but lines. They are composed by patterns of raised lines at right angles. The fine raised ink pattern is rendered variable in contrast to the foreground. Counterfeits made using the intaglio process had been seen on rare occasions due intaglio presses are far more expensive than ordinary offset, typographic or lithographic presses, which yield inferior counterfeits. Moreover the tactile effects in particular are hard to reproduce. Intaglio offers a high level of

security compared to digital printing. Different works compares the characteristics of motifs printed with Intaglio and other printing processes, such as offset and use these differences for counterfeit detection [95, 143, 145, 180].

Other commercial printing processes such as letter-press, flexography, gravure, and screen printing are not specific to secure documents, however they are often used for document numbering, laminate printing, and security feature inclusion.

Personalized printing

Personalized printing corresponds to the printing of variable information between security documents of the same type, thereby allowing individualize the document. Banknotes are classified by their value, series and country. Usually, the only intra-variance between the same group of banknotes corresponds to the *serial number*. Serial numbers provides security and identity to the notes on which they are printed. In the case of identity documents all personal information requires personalized printing. High-volumes of unique information printing is required, hence printing methods that are readily available, versatile, and cost effective are mandatory. These requisites are accomplished by *desktop production* or commonly named as *desktop printing* and are available and affordable to the ordinary person. Depending on the document substrate type, various desktop printing processes may be employed.

Most documents are produced with inkjet, laser, thermal transfer, or dye diffusion thermal transfer. Laser engraving is used for synthetic documents. However is it possible to find traditional processes as typewriter and dot matrix machines at older issued IDs, which does not have expiry date or are still valid nowadays. Inkjet and toner printing processes, together with typewriters and dot matrix printers, are restricted to print directly on paper based documents. An exception to this direct transfer of the ink to the substrate is its printed onto the reverse of a laminate adhered to the substrate. If a photo needs to be added onto an ID, a physical patch should be added to the traditional printing processes, meanwhile with inkjet and toner it is possible to print text and images directly at the document. Referring polymer substrate printing, meanwhile dye diffusion thermal transfer combination only prints correctly on polymer substrates, more general thermal transfer printing can be used on both polymer and paper documents. Both of this processes, likewise inkjet and toner, allow to print either black and white or color photos directly onto the substrate.

A well-known technique to print personalization information is laser engraving. This technology does not involve the use of inks and can only be used on "laserable" materials like synthetic polymer documents. The carbon sensitized layer within the polymer substrate, into which data is engraved, is made with plastic containing particles that are laser sensitive. A laser beam burns the particles of this layer,

printing the personalized information. As a consequence of the carbon particles, printing can only create black and white images . This laser-based process creates flat and/or raining printing, into the thickness of the document, impossible to remove and adding further security to the document. In [69] variations of statistics along edges between a printing press, a laser and an inkjet can be differentiated with a mobile device.

Nowadays all major commercial manufacturers of color laser printers have entered a secret agreement with governments to ensure that the output of those printers is forensically traceable [89]. The U.S. Secret Service admitted that the tracking information objective of this measure to identify counterfeiters. Each printer may contain some kind of forensic tracking code, visible or not to the naked eye. The most famous subtle pattern are the yellow dots covering the document. Those dots are a microscopic code that allows government agencies to trace the documents back to the printer which create it. Researchers lead by the Electronic Frontier Foundation (EFF) cracked the code of dots on documents made by Xerox, company who pioneered this technology since 1984, to assuage fears that their color copiers could easily be used to counterfeit bills [90]. These anti-copy marks are known as *screen traps*, causing most of the scanners, copiers, and desktop publishing software, to fail to reproduce the document when detected. Found in most of the banknotes, an example of this yellow dots, is the EURion constellation found on Euro banknotes, consisting of a pattern of five small circles, in exact distance apart, size, proportion and colour, which is repeated across areas of the banknote at different orientations. The mere presence of five of these circles on a page is sufficient for some colour photocopiers to refuse processing. Constellation should be of exact measurements and colour properties, if the constellation is altered by even a small variation, copying is possible [222]. Similarly to yellow dots, authors in [125] present a method for data hiding in any bicolour printed documents, which can contain characters, drawings, schematics, diagrams, cartoons, but not halftones. They pseudo-randomly distributing tiny black dots to embed the message. When the security trap is produced with thermal ink jet, dry electrophotographic, and liquid electrophotographic digital printers, it is possible to calculate its security strength [202, 207]. Repeated line patterns, two-dimensional (2D) bar code reading, and authentication of a color deterrent (color tile), prove to be effective to measure colour fidelity. The optimum selection of printing strategy, print technology, substrate and printed pattern may reduce the options of a counterfeiter.

Multiple laser image (MLI) based on the laser engraving technology is widely used as a security feature on ID documents. MLI as a single/separate element and in a simple format is regarded as having lost its strength and security role. However, the combination of MLI with offset printing, visible and invisible UV and positive relief features, and utilizing the latest advances in lamination plate technologies,

MLI remains one of the most powerful visible document security features [2, 137].

Serial numbers serves to identify uniquely each banknote printed and in circulation. It is a simple, cheap and effective security measure designed to make life difficult for the counterfeiter. In IDs documents, identity numbers are the synonyms for the serial number and can vary for each country. Additionally a format and limit ranges are added to increase the level of security. These numbers are stored in databases, accessible through ATMs and government systems, which can quickly notice if there are duplicates simultaneously at different geographically locations. Several works include serial number authentication in their pipelines [84, 85, 230, 250]. Additionally the age of ink of the serial numbers can be determined and consequently compared with the date it was issued. A essential zone for some IDs, like passports, is the Machine Readable Zone (MRZ). Similarly to serial number, MRZ contains identity number or/and passport document number, which also follows some rules and limit ranges. Those can be stored in a database for authentication. Furthermore, it also contains cheksum digits along with other bio-data information which can be compared with the printed data at other zones of the ID for detecting counterfeits [130].

Microprinting is another personalized anti-counterfeiting technique used in both banknotes and ID which is difficult to reproduce by digital methods. The patterns or characters are printed at a scale that is only visible through magnification with a magnifying glass, or microscope. To the naked eye, microprinting may appear as a solid line. Counterfeiters who tries to replicate these patterns using a photocopy or image scanning usually translates as a dotted, solid line or very low quality text on the counterfeit item when it is printed. Usually microprinting personalizes personal information like dates, words, abbreviations or serial numbers.

The *Typography* used at each of the fields of banknotes and IDs are also a security feature. The font, style and size of characters is a very distinctive feature in security documents [27]. Most of the printable fonts in IDs use proprietary, custom-designed typefaces. The fact that these typefaces might look like some commercial or publicly available typefaces is coincidental. Intrinsic characters and fields features, which we name *Intrinsic*, for the bio-data printed characters like the layout, alignment, skew and shapes, among others are also used as security measures to catch inexperienced counterfeiters [26, 190, 217].

Complex printing designs

Complex printing designs are printed on the security documents to prevent the rendering of these intricate patterns. Even if high quality desktop equipment may be capable of render them, when magnified the area of the patterns the edges begin to blur. The intricate level of detail of the complex geometrical designs achieved

by Intaglio and Offset Lithography remains as a secure anti-counterfeit measure against counterfeiters.

An example of geometrical complex printing designs are the *Guilloches*. Guilloches are patterns of subtle thin lines interwoven according to the rules of geometry. The wavy decorative lines and graphic patterns which composes them are primarily used on banknotes and ID documents. It works using a mathematical shape known as a hypotrochoid, which is the equation for the fixed point of a circle rolling around inside a larger circle (same concept as a spirograph works).

Moiré effect is an optical phenomenon generated by the interference between two different superimposed periodic structures, like line gratings or dot screens. A new visible observable pattern, named *Moiré patterns* , is created when the individual structures are superimposed, being the new pattern different from the original structures. The new observed image is extremely sensitive to small variations in the original layers, hence can be used as a anti-counterfeit feature. Moiré patterns are designed to interfere with halftone screens used in the printing industry, also known as screen traps (a moiré version similar of the yellow dots screen traps from 2.5.3). The screen traps are produce strong artifacts when a document is counterfeited using any standard halftone-based colour reproduction system such as offset printing. When moiré patterns are applied for digital photocopying or digital scanning prevention of security documents, the popular name scan traps is used.

Three general different types of moiré patterns are commonly found named 2D, 1D and pseudo-random, based on their moiré intensity. 2D moiré patterns are generated with between two specially designed periodic dot screens characterized by three parameters: its repetition frequency, its orientation, and its dots shapes. 2D repetitive pattern array, sampled with a 2D array of microlenses, produces a moiré image consisting of the enlarged and rotated array of repetitive patterns, also called 'moiré magnifiers'. The encoding desired information resides in the shape of the individual dots of the periodic dot screen. This repetitive pattern is often used to generate predefined letters, digits, country emblems, or other symbols, either in color or in black and white. These 2D moiré patterns can be used in the security threads of banknotes, passports and identification cards as another authentication measure. 2D moiré designs must reside within a single period of the 2D pattern array, when bigger sized patterns are created they need larger array periods. However as it grows the array period it greatly reduces the possibility of generating sophisticated designs at high frequencies.

To overcome these design limitations instead of 2-fold periodic dot screens, 1-fold periodic line grids can be used as in 1D moiré patterns. For 1D, the information is encoded withing lines of a periodic line grid and the revealing layer consists of a 1-fold periodic grid made of linear cuts rather than a 2-fold periodic pattern array. This configuration of moiré bands allows to include information of practically any

desired length. Also it is more easily visible in difficult light conditions due the amount of light passing through the grid made of line cuts is larger compared with the 2D pattern array. A drawback in comparison with 2D, is that they are more sensitive to layer rotations, since it causes a shearing effect which may alter the carried information. Color motifs, graphics or text can be designed along the length of the base band of a 1D moiré pattern. The larger the band, more elements can be included without modifying the moiré period. Usually the band width ranges between 10 and 20 μm, yielding an effective offset printed resolution between 1270 and 2540 dpi. However, this resolution is not enough to prevent counterfeiting using desktop scanners and printers.

The last type, is the pseudo-random variants of both 1D and 2D techniques previously mentioned. These variants corresponds to pseudo-random line cuts (or dot screens) instead of periodic ones, causing that the moiré effect resulting from the the superposition to not be periodic. The pseudo-random moiré pattern consisting of a single moiré shape. The moiré effect only appears when the element locations of the revealing layers are correlated with the element locations in the base layer. This requires that both layers uses a built-in encryption using the same sequence of random numbers, which can be used for additional security checks.

Vignettes are decorative and intricate designs which resembles to pieces of art, used to to increase the security of the documents. Nowadays is not a high security feature due the advances of scanning and printing technology. Banknotes have started to combine vignettes with other security features, like Australian polymer banknotes, which embeds a vignette inside of a clear window, creating a robust anti-counterfeit feature.

Some works uses the whole security document to find differences at different regions after applying a single feature extraction. These regions usually correspond with a security feature, like the vignette, microtext, watermark or security thread, to cite some. The feature extraction can be just binarize the whole document and then try to find discrepancies respect a reference genuine document [17, 173].

2.5.4 Security Levels

All the security features can be further classified in three security levels, see Table 2.7. The first level, correspond to the overt security features, or Level 1 features, which corresponds to the features that can be inspected with humans senses typically: sight, touch and sound. Most of the anti-counterfeiting measures fall into this category such as holograms, color fidelity, etc. Level 2 features, correspond to the features hidden from human sense and can only be checked with specialized equipment like UV lamp or magnified glass, such as microtext or luminescence ink features. The third level corresponds to the security characteristics that can

Table 2.6 – Summary of security printing techniques studies of anti-counterfeiting features for banknotes.

Type	Method	References
Offset Litographic	edge variations, respect inkjet and laser	[69]
Intaglio design	texture quality	[95, 143, 145]
Serial Number	binarization	[84, 230, 250]
MRZ	binarization, template matching	[130]
Typography, Intrinsic	hu moments, character size/alignment/axis inertia	[26]
Typography	conditional random field model	[27, 190]
Layout	text-line skew and alignment	[217]
Microtext, Background patterns	binary segmentation	[173]
Background patterns	slicing, edge detection, binary segmentation	[17]

Table 2.7 – Security features types classified by levels.

Level 1		Level 2	Level 3
Substrate fidelity	Security fiber	Microtext	Magnetic ink
Print fidelity	Planchets	Luminescence ink	Screen traps
Colour fidelity	Tactile fidelity		Manufacture anomalies
Acoustic fidelity	Color-shifting		Materials interaction
Serial number	Clear window		Complicated patterns
Issuing authority	Matching sides		Complicated designs
Hologram	Latent images		Fluorescence eminence
Watermark	Security thread		Texture analysis

only be visualized/authenticated by a forensic specialist using dedicated laboratory equipment. This last level of features are the result from the printing process and raw materials used during banknote fabrication, such as complicated patterns, texture analysis, manufacture known anomalies, etc.

2.5.5 Types of attacks and vulnerabilities

Duplication, imitation and mutilation are the most common types of attacks to forge a document or banknote, see Table 2.8. The three types of attacks are detailed next.

- Mutilation. The most aggressive technique of modifying a genuine document or banknote, in which the original parts are removed or replaced. Usually banks exchange full value for mutilated banknotes which a portion is missing or which is composed of more than two pieces. This fact is used for the coun-

Table 2.8 – Security features attack types classified by mutilation, imitation and duplication.

Mutilation	Imitation	Duplication
Ink removal	Desktop production	Photographing
Precision cutting	Commercial production	Photocopying
	Intaglio/Lithographic production	Scanning

terfeiters to disguise other types of forgeries in the banknotes. In documents is a rare attack because the official identity documents are more prone to be replaced when damaged.

  - *Ink removal.* Removing ink can be use to modify the value of a lower value banknote to a higher value preserving the original substrate of the banknotes or alter the information at some documents. From light amounts of chemicals such as bleach, Acetate or Acetone present in most nail polish removers, chlorofluorocarbon existing in hairspray and denatured alcohol or witch hazel present in after shave lotion to cite some is helpful to remove marks in any surface. Banknotes can also be ink-stained agains a stole attack. When criminals open a protected cash container, an ATM or a safe in a cash transportation vehicle, an anti-theft device known as intelligent banknote neutralization system (IBNS) can be activated and stain the whole banknote or some parts of it make in it unusable. When a banknote is stained by an IBNS, the security ink soaks into the banknote flowing from the edges to the center leaving a characteristic pattern. When the criminals tries to use chemicals to remove this security ink the original colours could be also altered, and some security features may be damaged, or may even disappear.
  - *Precision cutting.* ATMs can also protects itself against an attack, using glue to fuse all the banknotes into a solid brick and render the cash unusable. If the thieves try to peel off individual banknotes, they tear into pieces. Banknotes or documents can be cut into precise vertical strips and then joining with clear adhesive or glue to produce forged new ones. In documents the strips can be used to alter some biodata information. Although difficult to detect, under close inspection, image edges tend to slightly deviate from the original image.

- Imitation. This term correspond to the ability to fabricate new documents or banknotes with the available technology to common consumers. The

equipment that can be obtained without the supervision of the government or special authorities.

  - *Desktop production.* Common office printers can produce resolutions of 300 dots per inch (dpi) or more. Nowadays the casual or low funded counterfeiter, can acquire the necessary equipment within a reasonable price which can already reproduce high quality documents and banknotes passable at the first glance. Most photo IDs are printed by digital thermal transfer, color is transferred from a single-use ribbon to various kinds of receptor materials by this process. Intaglio and Offset Lithographic methods can not be matched and under microscopic inspection, microtext and Guilloché patterns are not rendered with the required quality.
  - *Commercial production.* Digital printing business has last-generation commercial equipment at their disposal capable of reproduce microtext and Guilloché patterns with higher precision. Image fidelity and image quality are superior than desktop production due it uses better inks and higher resolutions. The substrate of the document or banknote imitates closer to the genuine one in weight, thickness, fiber texture and surface. Security components such as watermarks, security fibers and security threads within the substrate are not replicated because this knowledge is kept secret by the issuing authorities.
  - *Intaglio/Lithographic Production.* Usually both Intaglio and Lithography are printmaking processes only known by the legitimate issuing authorities, however criminal organizations with enough resources have available the necessary equipment and knowledge of the inks and printing design to reproduce the original document. Spotting the counterfeits is extremely difficult in these cases. Forensic document examiners can rely at observed uncharacteristic anomalies at known legitimate printers. Moreover, security fibres, threads and watermarks can provide some clue of forgery if they are misaligned or deviate from the original document.

- Duplication. The idea is to duplication is to fabricate an identical copy of the original security document in all of its aspects. Duplicate means to make a perfect copy and absolutely identical to the original document, which would be the ideal case for the counterfeiter. However, finding replicas of security documents is much more common. A replica means to get a copy that is almost the same as the original, but not quite the same, it is always slightly different from the genuine at least in terms of its identity.

- *Photographing.* Usually the forger starts a new counterfeit inside a dark room, where acquires the legitimate document with a high quality photograph. A separate photograph is taken of each shade used on the document, as well as the pattern on the back. Each photo is stored in film or photographic negative, where the pattern of the document is transparent. A machine prints the pattern on a thin plate using light. The light going through the transparent bits prints the pattern onto the plate. For each shade a separate plate is created. The negative fails to hold all the detail of the original, so it has to be touched up by hand. Finally each plate is inked and printed on paper or other material. The produced counterfeit has vivid colors which at first glance are identical to the genuine document. However by touching the substrate is it possible to appreciate different tactile qualities.

- *Photocopying.* This type of forgery is only performed by the casual counterfeiter and it is the easiest to spot. Usually the ink and paper quality correspond to standard office supplies, which makes the reproduction differs greatly from the genuine and easily to differentiate by the substrate and dull colors.

- *Scanning.* For an affordable price it is possible to buy scanners able to scan a document with resolution over 2400 dpi. These scanners are often referred to as copy-dot scanners because they attempt to copy all of the halftone dots in the original. The purpose of greater scanning resolution is to modify the images with editing software and achieve a greater precision of the modification. Spotting the tampered document will depend on the printing operation and the quality of the ink and substrate.

2.5.6 Security features not visible photocopying or scanning

In section 2.3 we have explained how the counterfeited banknotes or money is affecting the society. Also we have explain several cases, some of them surprising, of people photocopying banknotes or printing their own money. Authorities alert the public to remain vigilant for people attempting to pass off counterfeit banknotes, and to call police should they be presented with what they suspect may be fake currency. However, human inspection of this bogus banknotes is prone to errors. Also ID theft industry protection have boomed over the last years, offering services that can authenticate an ID received from a customer, who has digitally scanned the document. This companies has to implement algorithms to automatically check the sent document is a photocopy or not to provide a minimum level of security.

Along this section 2.5, we have introduce different anti-counterfeit security features that can be used to authenticate a security document. A color copier or scanner can copy a document only at one fixed angle relative to the document surface. In a banknote inspection is possible to search for most of this features as a mean to determine if a note is genuine. Most of the security features will not be present in a photocopy. On the other hand, when validating an ID document using a single camera-base acquisition that has been sent online, most of the security measures can not be inspected.

Some elements of minor importance, in terms of security feature level, are more or less visible on photocopies, and can be used for authentication such as stamps, holographic films, perforate numbering, the paper embossing, the typography. However the reliability of such methods will depend on the quality and resolution of the photocopy. The rest of the security features mentioned along this whole section can not be controlled or detected from a photocopy. The same applies behaviour applies to the scanned images, however if the resolution of the scanned image is sufficient, other security measures can be checked, as the motifs, perforated image, Intaglio or background complex printing or texture designs.

2.6 Digital Tampering

The previous section 2.5 corresponds to a summary of the most common used anti-counterfeiting techniques against the tampering of security documents. Typically fraudsters try to create a replica or duplication of security documents in a physical material format, to ultimately use these counterfeit for criminal deception purposes. Having the existing physical document is mandatory to show in person to the corresponding authority or seller in order to buy goods or contract services. Although the last statement is compulsory for banknotes, it does not always applies for identity authentication and verification. Nowadays most of the services or products required for the general population, such as opening a bank account, applying for a loan, renting a car, checking-in in a hotel, etc. are easily available to contract through Internet. The companies who offers this services, needs a genuine online identification of the interested client before formalizing the contract or provide the service. The process of on-boarding a new client needs to be fast and seamless to obtain as many clients as possible in the shorter amount of time. Generally the client is asked to acquire his identity document with a smartphone or digital camera and send it online. In this case if the client is an imposter who has created a tampered document by most of the attacks explained in 2.5.5, most of the anti-counterfeiting techniques from this section are rendered useless once the document is transformed digitally to a single image.

As technologies used to digitally authenticate people over the decades have advanced, so too have the techniques attackers find to trick or bypass digital authentication. Fraudsters may modify some parts of its own personal data or impersonate completely other citizen, previously stealing his ID to afterwards replace some parts such as the photo. Typically forgers find is an easier option to replace small portions of real existing personal data information printed on a document than preparing a fake ID document from scratch. Most common forgeries replace the photo or change the number or letters containing the bio-data information, like changing the expiry date in a residence permit card. Even common users can produce high skilled documents forgeries, due to the availability of low-cost, high-performance computers, and the emergence of powerful software for processing and editing images. It has become relatively easy to manipulate or edit digital images even for non-professional users. *Digital Tampering* definition is the procedure of replacing the content within a region of the original image by some new content using editing software.

2.6.1 Tampering types

Table 2.9 – Common tampering types categorized according the manipulation operations and image source.

Type	Actions	Single image source	Region duplication	Tampering Objective
Copy-move		✓	✓	Object removal
Splicing	Cut-paste	✗	✓	Object addition
Inpainting	Erase-fill	✓	✗	Object removal

The three most common tampering types are: *splicing*, *copy-move* and *inpainting*, see Table 2.9. *Splicing* is a technique of creating an image by combining two different images. In image splicing a majority part of one image is used. The objective is to achieve the impression the new foreground object is part of the background. In *Copy-Move* type of forgery, a part of the image is copied and pasted onto another part of the same image to hide some object or some detail. These type of forgery is used to hide so information or alter the bio-data with copying the letters and numbers from other text fields with the same typography. When the part duplicated, using a single image, is removed from the original location and filled, this technique is called *Inpainting*. The filling operation is usually performed with gradient techniques to achieve realistic backgrounds. Recent image editing software suggests, for the three tampering types, to use neighboring patches or pixels within the original image to replace the target region because using these

patches is easy and more likely to achieve smooth filling effect than using patches from another arbitrary image.

2.6.2 Tampering detection approaches

It has been demonstrated that humans are easily fooled by tampered images [122, 159, 191]. When no original images are given for comparison, people have an extremely limited ability to detect and localize image tampering. Research community has put a lot of effort into develop algorithm to automatically discover tampered images.

Different surveys has been published on image forgery detection [211, 246, 252]. The works cited in those surveys are mainly evaluated against very large collection of forgeries datasets collected from various Web and social media sources. Currently there is no publicly available tampered identification document dataset, read section 2.7 to understand the reasons it does not exist. However the techniques applied at some of these works can be transferred to the digital identity tampering discovery.

Identity documents are going to be acquired in a open-world scenario. We are interested in *passive detection* techniques aims at verifying the authenticity of digital images without any a prior knowledge, like the acquisition device or identity document layout. Passive detection algorithms exploit the artifacts and inconsistencies to distinguish between pristine and forged areas in the image [228]. Among these algorithms statistical methods, based on pixel-level analyses, are the most common. These statistical methods can follow a model-based or a data-driven approach. Model-based methods use features like lens aberration [244], color filter array (CFA) [86], JPEG artifacts [165] or camera response function [51] to build a mathematical model to detect the tampered areas.

Data-driven algorithms are evaluated on the noise residuals of the image. Noise residuals can be obtained applying high-pass filters in the spatial or transformed domain, as Fourier [221], DCT [108] or Wavelet [82]. Authentic scanned text documents may contain multiple, similar-looking glyphs (letters, numbers, and punctuation marks). In [11], the authors study the impact of copy-move existing algorithms to this scenario, showing that under specific threshold and parameters values, the block-based methods have a modest performance. They also propose an analysis framework for detecting copy-move tampering in text images, joining OCR character characteristics like weight, size, style and roughness with the copy-move algorithms focused on the background.

When a uniform source light falls on a camera sensor, each pixel should output exactly the same value. Small variations in cell size and substrate material result in slightly different output values. Photo response non uniformity noise (PRNU)

stands for the differences between the true response from a sensor and a uniform response [148]. PRNU is caused by the physical properties of the sensor, it is almost impossible to remove entirely and is usually considered to be a normal characteristic of the sensor. Different works demonstrate PRNU patterns are a good option for identifying and localizing forgeries [42, 55]. A drawback of this approach is that PRNU patterns must be estimated for each camera model, which uses a specific sensor type, requiring a large number of frames from the target camera model to obtain realiable results.

Authors in [176] use steganalysis to suppress the scene content and force the network to work with noise residuals using a deep learning model. In [253] a two-stream model network, where the first network learns the noise residuals and the second is a general purpose network. Authors in [22] propose a localization framework using an hybrid CNN-LSTM model to learn the boundary discrepancy between pristine and forged regions. In [31] identifies different camera models using a CNN that compares image patches, however it requires the camera models to be in the training set. A Siamese network can learn the EXIF metadata, to create model that distinguishes patches from different camera sources [114, 127]. Following this idea, Noiseprint exploits image content and camera model information [61]. It can detect most of the tampering types. Noiseprint has been successfully used in forgery localization under a supervised setting and in video forensics [60, 62]. ManTra-Net is a novel that exploits a long short-term memory model to asses local anomalies [238].

2.6.3 Digital Watermarking

The previous section establishes a principal constraint which is the unavailability of the original image. When IDs are manufactured it is possible to acquire a digital image of the original genuine document. If *digital watermarking* is applied to this image, it can be used for secure digital transactions. The digital watermaked image can also be reprinted embedding the code physically in the document. Digital Watermarking are the techniques that hide information, for example a number or text, in digital media, such as images. The content of the digital data is manipulated to embed the hidden secret digital information, called "watermark". The pixel values modified and quality degradation in the watermarked image must be unnoticeable by human eye. Moreover, the watermark should be robust to resist manipulations or possible attacks on the digital image, such as lossy compression, scaling, cropping, among others[129]. Furthermore, the hidden information should be possible to be detected or recovered, with the objective to verify the authenticity of the digital image.

At early stages of computer vision to prevent counterfeit digital tampering at-

tempts, the most notorious works were based in Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), [59, 140]. A watermark is embedded in host images at these approaches in spatial or frequency domain.

Authors in [167] inserts a unique personal code inside the photo to figure out fraud photocopy ID documents. The forgery is detected when the embedded data is compared with the ID information on the document. Also in in [212] a ID personal number watermark is embedded into owner picture, the difference is that they print the photo watermarked on the ID. Later, with a camera-based acquisition of the printed ID, the watermark can be extracted and checked if belong the ID personal number corresponds with the one at the document. Projective transformation registration technique is applied to minimize perspective, rotation, scaling and translation distortions.

Printing a digital watermark to a physical ID card and its posterior scanning for authentication may introduce random noises into the images, named printing and scanning distortion (PS). Distortion can appear at pixel values and the geometric boundaries of the scanned image. In [115] adaptative watermarking using matrix of regulation factors is proposed to remove the PS noise in the watermark before extract it. Another possibility is to combine different hiding technologies like digital watermarking, 2-D bar codes, copy detection patterns and biometric information to protect ID documents against several types of forgeries [170]. Recent surveys in digital watermarking can be found in[197, 203, 204]. The later presents the use of anti-forensics sections, where they explain how the forgers hide the tampering as a result of the fingerprints study that might be introduced due to their use.

In most cases digital watermarking techniques can only be applied by the manufacturers of the original ID document. Furthermore, digital watermarking is weak against three types of attacks: removal, cryptography and protocol attacks. The removal attacks try to remove all watermarking in the document. The Cryptography attacks aims to alter the watermarking and the protocol attacks objective is to attack the watermarking applications.

2.7 Datasets

The evaluation of counterfeit detection algorithms is a constant challenge for researchers. Building a counterfeit dataset *per se* represents a difficult task due the scarcity nature of counterfeit documents. Usually a counterfeit dataset contains a small percentage of counterfeits compared with their genuine counterpart. Counterfeit datasets are usually collected by documents experts, see section 2.4. Training a document expert is expensive, hence generating a dataset generated by them represents a big economical effort. Most private companies in document security

analysis can afford to invest in the generation of counterfeit dataset, however make these datasets public does not play in its own interests. On the other hand, even having the economical means and the predisposition of building a public dataset, is difficult to publish it as a benchmark for the research community. The copyright status of the security documents designs is carefully controlled by counterfeiting laws. In the case of the banknotes, this copyright status can vary from nation to nation [65]. Some of the restrictions imposed at the banknotes, for instance the Euro banknotes, are harmful for evaluating computer vision algorithms. Euro banknotes are copyright of the European Central Bank. There are rules such as the word SPECIMEN must be printed diagonally across the reproduction, in a non-transparent colour contrasting with the dominant colour of the note. Also width and height of the word must represent at least 75% and 15% respectively of the document. Moreover the resolutions of the shared image must not exceed 72 dots per inch (dpi). These restrictions, established to prevent counterfeiters to fabricate imitations, also harms the use of algorithms which requires higher image resolutions to look for authenticity details.

Despite all these obstacles, researchers have produced algorithms to solve the banknote counterfeit problem creating their own datasets. One work around to publish datasets of banknotes is to process the images with your algorithm and then share only the output feature data [142]. These features, extracted from genuine and forged banknote-like specimens, contains Wavelet Transformed image (variance, skewness, curtosis) information and entropy information. These features, corresponds to patches of 400x400 pixels of the banknote. The patches are digitized with an industrial camera, at close distance from the banknote to the lens. Due the close distance to the investigated banknote the resulting resolution is 600 dpi [143]. However this dataset does not allow to develop new computer vision algorithm development approaches.

Most of the researchers works directly with the banknote images and do not share their datasets due the commented previous limitations. A recente survery analyzes 45 datasets for banknote recognition methods and only one is publicly available [134]. The public available dataset corresponds to Jordan bills and coins acquired with a smartphone on different backgrounds [74]. In the survery they also explore 16 counterfeit banknote detection datasets, used in 31 research publications, where none of them are public. At Table 2.10 we present ID and banknote counterfeit datasets used at the current literature. We present the availability, the number of document samples, the number of classes and the percentage of counterfeits it contains.

The dataset collected in [50] is collected on the street including new and worn out banknotes. Local defects of tears, stains, graffiti or holes for fitness classification and counterfeit detection are manually labeled in [119]. In [180] the regions of the

Table 2.10 – Datasets on ID and banknote counterfeit detection (Ref.: References, N/I: Not Informed, N/A: Not Available).

Availability	B/ID	#Images	#Classes	μ	σ	%Counterfeit	References
N/A	B	60K	6	10K	0	-	[119]
N/A	B	99	1	99	0	29%	[243]
N/A	B	-	7	-	-	-	[28]
N/A	B	357	3	119	1	-	[41]
N/A	B	1K	1	1K	0	50%	[180]
N/A	B	900	6	-	-	-	[95]
N/A	B	264	-	-	-	-	[143]
N/A	B	66	1	66	0	50%	[145]
N/A	B	2.75K	7	-	-	-	[37]
N/A	B	82	2	-	-	48%	[69]
N/A	B	200	1	-	-	50%	[50]
N/A	ID	50	22	-	-	-	[130]

rupees banknotes are scanned using four different 4 different light sources, which are UV light, Co-axial light and Flood light with two different magnitude and gain configurations. Then the authors uses the source light that suits best the security feature they want to analyze. A dataset for intaglio textures authentication is build in [95]. The dataset is divided in textures printed with Intaglio printing process and by offset printing. The dataset is also classified into high-quality and medium-quality prints. They scan at 1200 dpi and convert to grayscale 6 different classes of textures. Both counterfeit and genuine banknotes have been acquired under several environmental lighting conditions, with different illuminants and brightness in [37]. The authors also introduces in the dataset misalignment with slightly translated and or rotated banknotes. In [69] the genuine banknotes are scanned at 1200 dpi, to print them later with an inkjet and laser printer. Genuine press printed banknotes, inkjet and laser ones are acquired in a later stage with a smarphone.

As in banknotes, identity document designs are copyrighted in most countries. Additionally, identity documents contains Personally identifiable information (PII). PII is any data that could potentially identify a specific individual. Information which, when disclosed, could result in harm to the individual whose privacy has been breached. PII can be exploited by criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts. Laws and regulations from each country ensures their citizens are protected against fraudulent use of the PII contained at their identification documents. Countries differs in the approach to

data protection. For instance, in Europe, privacy and data protection appear as fundamental freedoms, contained in the General Data Protection Regulation (GDPR). All these restrictions and protection laws makes impossible for the research community to share a public dataset to be used as a benchmark for counterfeit ID detection. In [130] they created a passport dataset for MRZ and bio-data comparison.

2.8 Approaches, methodologies, and techniques

In this section we summarize most of the algorithms presented at section 2.5. We have divided in three steps the presentation of these algorithms: preprocessing, feature extraction and classification. These are the usual steps followed to authenticate a banknote.

2.8.1 Preprocessing

Most of the presented works for counterfeit detection need as an initial stage to have the banknote correctly cropped. Removing the background from the object that needs to be inspected, will contribute to better accuracy results of authentication. A simple cropping of the document can use Hough Transform on a Canny edge detected image. Afterwards registration can be done with Template matching of relevant patterns at the document. These are simple algorithms, which can be certainly improved with better approaches. However the registration of the document is outside of the scope of this work and we presuppose the cropping is already done.

Preprocessing step is commonly used as a prior to descriptor calculation in order to normalize illumination differences from the acquisition devices such as scanners, cameras, smartphones, etc. It is important to improve the quality of the sourced image and at the same time do not remove important information printing information which could lead to the counterfeit identification [152]. Banknotes and IDs surface can also be soiled by dirt and sebum from users hands. Banknotes are more easily contaminated due to their wide circulation. The environmental acquisition conditions can also introduce variations in the aspect of the acquired image, such as the exposure, brightness, contrast, etc. To address this, noise removal prepossessing techniques are introduced as a first step in the processing pipeline. Histogram equalization or storing a brightness map to normalize with the test images, is used for brightness normalization and contrast enhancement [25, 28, 37, 243]. Authors in [152] presents a preliminary study on the difference between using gradient filter for illumination normalization for IDs background analysis. Author in [78] are interested in the noise produced by the laser and inkjet printing

techniques. They filter the printed area calculating the Otsu's threshold and getting the median gray-level for the background pixels from the original image.

Most of the works directly works with the RGB color space from the input image. If a cited work no color space is specified RGB is what they use. Other authors, to reduce the input dimension authors may adopt other colorspaces and only use one component. Only the Y component from the YIQ color space is used in [28, 243]. The b* component from L*a*b color space is used for analyze microletter in [180]. Single channels of RGB, HSI and L*a*b colour spaces are compared, for complexity reduction in [47]. They achieve higher accuracy if they use an average of RGB channels for their dataset.

Authors may partition the image into different patches, scattered at the image input. The objective is to reduce the dimension of the input image, preserving global information [28, 68, 243]. The features are then extracted at each patch and combined in a later stage. In [17] original grayscale images are decomposed into their equivalent 8 binary images, claiming is useful in analyzing the relative importance contributed by each bit of the original image.

Table 2.11 – Preprocessing techniques in the counterfeit flow.

Task	Method	References
Brightness normalization and contrast enhancement	Histogram Equalization	[17, 25, 28, 243]
Brightness normalization	brightness map	[37]
Brightness normalization	gradient filter	[152]
Colorspace	b* (L*a*b)	[180]
Colorspace	Y (YIQ)	[28, 243]
Colorspace	RGB average	[47]
Colorspace	Grayscale	[69, 78, 95, 173]
Colorspace	Grayscale Slicing	[17]
Image filtering	Otsu, median grey-level	[78]

2.8.2 Feature extraction

Once preprocessed the image, next step is to extract features of interest which could repeat a common pattern in the genuine security documents easily distinguishable against the counterfeit documents. Next we detail some common works center in

banknote counterfeit features extraction.

A Free From Deformation (FFD) model for banknote image registration is proposed in [119]. The authors propose to map a mesh of control points, and measure the deformed position of each pixel by a tensor product of cubic B-splines. Afterwards the map is compared against a reference image with a energy cost function to detect dissimilarities. The authors in [37] also use IR images for invisible ink inspection. They base their work in learning the patches, locations and thresholds from the most discriminant IR patterns such that the intra-class distance is minimized, whereas the inter-class distance is maximized. The work is [41] uses UV information. They calculate similarity with a UV reference image, using a simple pixel sum and remainder comparison. A similar approach is used with the grayscale image in [173], where the authors after binarize the test image, and they compared the thresholded pixels against a binarized reference image. Several cropped anti-counterfeit regions are check following this procedure, such as microprinting, watermark, security threads, etc.

The authors in [28, 243] discard the chrominance information and use only the Y component to build a 256 bin luminance histogram. GLCM features are additionally concatenated with the histogram in [28]. In [17] higher order bit levels are evaluated for grayscale banknote images with the application of Canny edge detection algorithm. They observed that the edges obtained using bit-plane sliced images are more accurate and can be detected faster than obtaining them from the original image without being sliced. A single threshold value-based pattern segmentation method may have difficulty segment the patterns of the UV image. A Gaussian mixture model (GMM) and Expectation maximization (EM) algorithm can be applied to consider the multi-modal characteristics of the UV histogram [135]. Feature vectors containing the cross-correlation with a synthetic template statistics, the cross-section along the edge and the projection across the edge can be use to distinguish counterfeits made with inkjet and laser printer from genuine bills [69]. Authors in [180] extracts 18 features to check for ink, security thread, Guilloches and Intaglio. They check the denomination region of the banknote which is printed using Intaglio. 9 features are used for this region, such as pixel dominant intensity, hole count, average hue, contrast, etc. For ink, they use colour composition and ink fluidity. Microletter is validated with the spread distribution of the b* component of the L*a*b* color space. The security thread, is composed of two binary features. The first is check for the registration, where the thread should always appear as a single line. The second is determine the presence of text in the thread by pattern matching. Dot distribution, along with cluster distribution and dot density for the strokes, is used as features for Guilloches. Also a latent image, printed with Intaglio is evaluated for inconsistency in the sharpness of the lines, by using a MLP-NN classifier.

Wavelets appear to be suitable for digital image texture analysis, because they allow analysis of images at various levels of resolution. Authors differentiate genuine and counterfeit Intaglio banknote features by first order statistical moments of wavelet coefficients, using 2D incomplete shift invariant wavelet packet transform (2D-SIWPT) [95]. Instead of decomposing the full wavelet packet tree (WPT), the authors also proposed a Best Branch Algorithm (BBA). This algorithm focuses in the branches with highest spatial frequency which contain significant texture characteristics and prunes the rest. Once the best nodes of each scale level are selected an histogram of wavelet coefficients is built. They only used the σ^2 and kurtosis of the histogram as features to detect counterfeits. Following the previous work, skewness and the local adaptive cumulative histogram (LACH) features of the histogram are added, [143, 145]. The LACH features divide the histogram into three areas: left, middle and right. Being the middle part centered at the zero value coefficient with a width of σ^2. Afterwards the coefficients in each area are accumulated forming three different score features. The most important lower-frequency DWT coefficients are used in [50] for spectral analysis of watermark, OVI and fluorescent fibres.

Most of the features used for different kinds of text related security documents can also be applied for ID security documents. Authors in [26] proposes a document forgery detection method based on document's intrinsic features at character level, such as font properties, character shapes, and character/word alignments. They aim to detect marks such as misalignment or skew found in Scan-Edit and Print (SEP) forged documents. They use a feature vector of Hu moments to detect character similarities, and character size, character horizontal alignment and character principal inertia axis as the feature vector for conception errors. Later, same authors propose to use a conditional random field model which first allows to recognize and classify typefaces, highlighting font forgeries [27]. The CRF model, describes the correlation between fonts, styles, and sizes of the characters. Measuring the probability that a character belongs to a specific font by comparing the font features with a knowledge database, to know whether the character is genuine or fake. Also using a CRF model, the authors in [190] focus in font recognition, predicting the typeface, weight, slope, and size of the fonts without knowing the content of the text.

It is possible to differentiate between laser and inkjet printing focusing on the edge areas of the printed letters. A feature vector is formed with line edge roughness, area difference, correlation coefficient and texture [131]. Sharper edges indicates laser printer, meanwhile the opposite correspond to a injket printout. Similarly, authors in [93] differentiate laser from inkjet printed pages looking at the edges of the characters for possible forgery attempts. It is possible to differentiate different types of inkjet and laser printers by just looking at the noise produced

Table 2.12 – Comparison of works based on substrate.

Type	Security Measure	Method	References
Printing	Printing process	Edges + Cross Correlation	[69]
Ink	IR Patterns, Defects	Free From Deformation (FFD)	[119]
Ink	IR Patterns	Pixel segmentation	[37]
Printing	MicroPrinting, Guillochés	Pixel segmentation	[37, 173]
Printing	MicroPrinting, Guillochés	Canny + Pixel segmentation	[17]
Ink	UV Patterns	Pixel sum and remainder	[41]
Ink	UV Patterns	GMM + EM	[135]
Substrate	Document Brightness	Luminance Histogram	[28, 68, 243]
Ink	UV Patterns	GMM + EM	[135]
Printing	Intaglio	2D-SIWPT + BBA	[95]
Printing	Intaglio	2D-SIWPT + LACH	[143, 145]
Printing	Typography, Intrinsic	CRF, Hu moments, ...	[26, 27, 190]
Printing	Printing process	edge roughness, area difference, ...	[131]
Printing	Printing process	character edges	[93]
Printing	Printing process	μ, σ, skewness, kurtosis	[78]
Printing	Guilloches, Printing process	2nd order statistics, spectral analysis	[152, 169]
Ink,Substrate,Printing	Intaglio, Color MicroLetter, Ink Fluidity Security Thread, Guilloches	Dominant intensity, textural similarity colour composition, pixel distribution dot distribution and density, Otsu, ...	[180]
Substrate, Ink	OVI, fluorescent fibres, watermark	DWT	[50]

by the printing technique [78]. This approach is independent of the document content or size. Authors in [152, 169] use a composite representation based on 27 different criteria (from basic local gradient magnitude to SURF on FFT, or wavelets) to identify the different printing process.

Text-line alignment and orientation measurement for forgery detection is analyzed in [217]. They detect implausible skew angles or alignment distances. A considerable area of IDs belongs to non-static data, usually corresponding to the actual content of the document. In [16] propose a framework to detect forgeries only focusing on the static part of non-IDs printed documents. Although the non-static part is also mandatory to check for the final authentication, their approach can be used to determine automatically the variable and non-variable regions of the documents.

2.8.3 Classification

The final step in the pipeline of counterfeit authentication is to produce a binary response if the document is either genuine or counterfeit. It is possible to compare feature vectors using Euclidean or Mahalanobis distances [26]. They compare test characters with a dataset of genuine character. Afterwards a threshold is applied

to decide if it is a genuine or fake character. This approach is fast an efficient if the feature vector are enough representative of their classes.

Most of the works presented use Support Vector Machine (SVM) as the preferred classifier[25, 28, 50, 78, 95, 131, 180]. Linear Discriminant analysis (LDA) is preferred if all elements of classes, follow a gaussian distribution, contribute to the solution uniformly and the possibility of the misclassifying unknown data is fairly low. A multi-stage LDA classifier is used for mobile device banknote counterfeit detection using adaptive wavelets for the analysis of different print patterns on a banknote [143, 145].

Choosing a kernel function or hyperparameters in advance for SVM may lead to bad performance. They focus on determine the best kernel function and the associated kernel hyperparameters. An specific kernel kernel for SVM is associated for each partition of the features in [243]. The combined matrix is calculated with a linear weighted combination of the multiple kernels. Semi-definite programming (SDP) learning is used to obtain optimal weights for the kernel matrices. In [180] they use a combination of two SVM, with Poly and RBF kernel, and an ANN. Then a majority vote approach is followed in integrating results from these classifiers.

Bayes theorem, describes the probability of an event, based on prior knowledge of conditions that might be related to the event. Bayes can be used for instance to model the conditional probability that two consecutive characters are written with different fonts [27]. In [93] they use k-NN for unsupervised anomaly detection to detect documents printed with a different printing technique than the majority of the documents. This yields the advantage that even unknown printing techniques can be detected.

Table 2.13 – Comparison of works based on classifiers.

Method	References
Homogeneity-based deterioration energy (BDE)	[119]
Artificial NN	[180, 250]
SVM	[28, 50, 78, 95, 131, 180]
LDA	[69, 143, 145]
Multiple kernel SVM	[68, 243]
Euclidean, Mahalanobis distance	[26]
Bayes probability	[27]
k-NN	[93]

2.8.4 Summary results discussion

Most of the papers cited in this work report accuracy as the results measure, which is defined as a ratio between the correctly classified samples to the total number of samples. However in counterfeit detection we deal with imbalance datasets, being the accuracy measure clearly misleading for reporting results when there exists a big difference between the positve and negative samples. The word *positive* is used in the sense of counterfeit, whereas the word negative is used in the sense of genuine. False positive rate (FPR), also called false alarm rate (FAR), represents the ratio between the incorrectly classified negative samples to the total number of negative samples. False negative rate (FNR) or miss rate is the proportion of positive samples that were incorrectly classified. Both FPR and FNR are not sensitive to changes in data distributions and hence both metrics can be used with imbalanced data. In Table 2.14 we present the results reported by their correspondent authors in the literature. This comparison only includes the works with an ID or banknote counterfeit dataset. We also have not included the works that did not report the results, or the one without enough information of the dataset use for the result. However in the comparison we also talk about non-ID works, which focus in text security documents. Some of this approaches could be transferred to ID security documents.

First we start with banknote related results. In [50] claims that lower-frequency DWT coefficients works very effectively and keeps important characteristics for OVI, watermark and fibres feature extraction. The extracted features from [95, 143, 145] allows to separate linearly without error all the elements in the dataset. The work in [41] is though for low quality, high-speed inputs for real-time counterfeit detection experiments. So the actual comparison should be improved with a more complex pattern recognition for more complex acquisition scenarios.

Discarding the deteriorated security document can be a good practice to not raise unnecessary false alarms, if the IR image is available [119]. It can also be used to check the anti-counterfeit IR patterns. Learning the most discriminatory IR patches could be an issue when a highest variability of banknotes is presented in the approach from [37]. Although authors in [243] reports perfect results, they have a small dataset and their method requires more than 13 seconds to compute. Authors in [28], do not provide enough information about the configuration of the dataset for the reported results. Moreover, luminance features are not robust under uncontrolled lighting conditions.

Laser and inktjet printers are unable to produce similar sharp edges due to the dithering and satellite droplets respectively. In [69] demonstrate how it is possible to differentiate genuine printed banknotes from inkjet and printed ones using the edge information from mobile phone acquire images. In their studies only the

projection along the edge has an acceptable performance in terms of low FPR. The multi-security feature authentication analysis from [180], can be useful to use some of the low complexity algorithms presented as complementary features for other approaches. The only two classes used for this work are not representative for generalization of the proposed methods to other security documents.

Focusing in text related document forgery, the method propose in [131] also proposes to differentiate laser and printer. However they present an error rate of 5.2%, which is too high for a fully automatic system. This is cause because a single forged letter makes the whole document a forgery in their method, which is much to sensitive. The approaches in [26] works with binarized low-resolution documents and do not specify if they included IDs in their datasets, which makes uncertain how it will work under the presence of, for instance kinegrams, occluding the characters. In their later work [27] the same problem of the dataset applies and the performance with banknotes or IDs needs to be tested. The algorithm for text-line alignment and orientation in [217] only works with pure text documents. This algorithm should be adapted for the presence of images and security features present at IDs and banknotes.

Table 2.14 – Comparison of works based on banknotes.

Method	μFPR	μFNR	μAcc	μAuc	μF1	References
IR Registration similarities	4.7%	7.7%	-	-	-	[119]
IR pixel segmentation	4.3%	0.0%	-	-	-	[37]
UV pixel comparison	-	-	100.0%	-	-	[41]
Luminance Histogram + GLCM + SVM	-	-	85.0%	-	-	[28]
Luminance Histogram + Multiple Kernel SVM	0.0%	0.0%	100.0%	-	-	[68, 243]
Multiple features + MLP-NN + SVM + ANN	-	-	100.0%	-	-	[180]
2D-SIWPT + BBA + SVM	0.0%	0.0%	-	-	-	[95]
2D-SIWPT + LACH + LDA	0.0%	0.0%	-	-	-	[143, 145]
DWT + SVM	-	-	99.0%	-	-	[50]

2.9 Systems and applications

The previous section 2.8 presents different approaches or methodologies to solve the problems of counterfeit detection in banknotes or IDs. At this section we focus in complete systems and applications integrated in smartphone for counterfeit detection. One of the main purposes as explained in section 2.4 is to provide tools to security document reviewers and citizens for accessible, affordable and

comprehensible counterfeit detection.

Targeting mobile-based solutions for banknote counterfeit detection, authors in [177] use statistical features, and surface roughness of a banknote to represent its properties such as paper material, printing ink, paper quality, and surface roughness, however their dataset is rather small. Researchers in [72] fuse shape context, SIFT, gradient location and orientation histogram (GLOH), and Histogram of Gradient (HOG) into an ensemble base classifier. They focus in banknote recognition, but their system can also detect obvious counterfeits. They achieve real-time on-device processing times, because they only use the quantity number region of the banknote. Authors in [180] propose a system checking multiple anti-counterfeit features, covering the substrate, ink and printing features to create a final decision of the authentication of the document. They also perform a comparison between forensics experts, bank employees and their systems to show its accuracy and time, to deploy their system for mass checking of currency notes in the real world. The authors claim to kept optimal the complexity of the overall system, to be able to run in a low cost hardware, however they are reporting processing times of 20 minutes.

Focusing on the Intaglio regions, the authors in [143, 145] propose a system of counterfeit detection able to run on smartphones. They propose to use Y-channel, from the preview image in YCrCb format due it seems to be uncompressed. This way they avoid the JPEG-artifacts distortions, which affects the high frequency components. Also this channel from the preview image has low resolution, therefore usable for image processing applications. The preview image with 1280×720 is used, and a pre-processing part of the camera module generates in one step a grey-scale image in the preferred size of 400×400 pixel for the top, middle and bottom region, with an approximate resolution of 620 dpi. The Intaglio zones have been also validated by the authors in [168], a two-dimensional discrete Fourier transform (2D DFT) is use to identify the periodical screens within the separated channels. Afterwards, unimportant frequencies are suppressed, transforming back the remaining ones. Finally, a model-based feature extraction determines the screen angles and the individual offset rosettes. They acquire their dataset with a minimum of 1100 dpi within a controlled environment.

The applications of fingerprints in ID documents is discussed in [240]. They propose a enrollment and verification system, that ultimately matches the collected fingerprints with the ones stored in a chip integrated on the ID. These system faces problems in case of wet, dry, or scratched fingerprint. Authors in [194] discusses the requirements, design and application scenario's of multi-modal biometrical systems. They study the privacy, security at biometric passports and the public perception and repudiation of these security measures. Other researchers have focused in a banknote validation method which uses radio frequency identification (RFID) and an NFC-enabled smartphone for real-time banknote validation [77].

Although this method is computationally less expensive than other methods not all the documents and banknotes have the RFID chips.

Table 2.15 – Comparison of systems and applications.

Year	Type	Security Measures	Processing time	References
2018	Smartphone App.	Quantity number	0.02ms	[72]
2017	Smartphone App.	Intaglio, Guilloches, Vignettes	9.2s	[194]
2017	Smartphone App.	Substrate quality/roughness, ink	-	[177]
2016	Smartphone App.	Intaglio	-	[168]
2015	System	substrate, ink, printing	20m	[180]
2015	Smartphone App.	Intaglio	1.2s	[143, 145]
2015	Smartphone App.	RFID chip, NFC-enabled	real-time	[77]
2014	System	Fingerprint	-	[240]
2009	System	multi-modal biometrics	-	[194]

2.10 Trends

In [233] the authors present from the invention of physical money to the evolution of paperless alternatives. They also present some insights of a "cash-less society" as either a big pro of a big con, doing an intriguing survey of what will happen to counterfeiters and others in the coming cashless society. Countries are eliminating cash at varying speeds. Reports shows that four out of five purchases in Sweden are paid for electronically or by card [83], there exists predictions which consider Sweden will be the first country in the world completely free of cash. Another contender for the first cashless country in the world is in China, embraced with the QR codes [157]. Other cases, like UK, does not fall behind the cash-less future, where credit/debit cards, contact-less and online payments have taken over cash payments. Smartphone applications transforms the device into a seamless wallet, remittance, and payments tool, granting financial inclusion and unprecedented convenience to billions of unbanked people around the world. Furthermore the rise of decentralised cryptocurrencies is starting to coexist legitimately alongside digital currencies. Removing physical cash, automatically will remove counterfeit banknotes, consequently large-scale criminal activity would be much easier to detect: transactions will have to bypass bank accounts, which are traceable.

Similarly, ID security documents are moving already to Electronic national ID cards (e-IDS). e-IDs include a microprocessor for stronger document verification but also on-line authentication and signature. These e-ID cards offers the best

identity theft protection and also enable governments to implement on-line applications such as eGovernment solutions, giving citizens access to public services with the reassurance of robust security. According to [12], the number of electronic National ID cards in circulation will reach 3.6 billion citizens by 2021. Furthermore, another strong and trusted method of identification, is the mobile ID (mID), which are mechanisms using an eID component for accessing online services via mobile devices [94]. Pioneers countries, like Austria, Estonia, Finland, Norway, and Turkey are moving towards mID. Moreover, several US states have launched pilots for digital driver licenses, also called mobile drivers license. It provides an on-screen mobile version of the traditional photo and driver information, being highly secure and with stronger counterfeiting characteristics. Being able to update instantly the driver data information and facilitates real-time communication.

Does this means researchers should stop improving anti-counterfeit features for the security documents? Quite the opposite. Physical IDs and banknotes are not going to disappear in a near future. Today, 85% of worldwide consumer spending is done in cash despite many forecasting the demise of this resilient product. The conclusion that the near and midterm future of cash is not a non-cash society, but the one with less cash [124]. Printing, circulation, and reprinting of banknotes and the growth in tourism is projected to increase the demand for passports and visas, which in turn, is driving the growth of the security paper market across the globe. The security paper market is projected to grow from USD 11.4 billion in 2018 to USD 14.8 billion by 2023 [232]. Hence counterfeit IDs and banknotes will continue circulating.

It has been observed that after the introduction of polymer substrate paper banknotes, the average quality of the polymer substrate counterfeits has also increased. Over the past two years, around 40 per cent of counterfeits detected in Australia have been considered high quality [19]. Authors in [123] created a way to print chromatic holograms on any surface and also create high-quality organic piezoelectric structures. Printing luminescent structures based on *nanoparticle ink* allows for the fabrication of custom holograms by means of a common inkjet printer, which can produce anti-counterfeiting objects with high stability and durability. Private companies are also developing new security features, like *Galaxy Threads* or *RollingStar Threads* [210]. The former produces three optically variable effects combined in this thread: 3D motifs, dynamic effects and color shift, are visible from any perspective. The later makes possible dynamic effects that immediately attracts attention, the thread links motion sequences and color shift. *Satellite holograms* and *Emerald number* have been recently introduced in the 100 € and 200 € banknotes [75]. The first makes and observable € symbols moving around the number when tilting the banknote and become clearer under direct light. The second is an OVI that changes the colour from emerald green to deep blue of the number, producing an effect of

light that moves up and down when tilting the banknote.

Most countries are constantly adding new security features or upgrading the existent ones at each of its banknotes and IDs. The aim is to make harder to counterfeit, but still easy to check. In this section we have just cited a few of the actual improvements and the current and future trends.

2.11 Conclusions and Future work

This related work of identity document and banknote security forensics is a contribution of this thesis. We focus in the anti-counterfeit security measures which can be solved automatically by computer vision algorithms. Initially we compare this work with multiple state-of-art surveys to show the completeness and the need of writing a new survey. We add sections which were not usually treated at other surveys, such as history, effects of forgery in society or document experts, with the objective that readers without the previous knowledge in counterfeit detection understand the basics and difficulties of this field. The sections anti-counterfeit measures explains how are designed the most known anti-counterfeit features based in three categories: The security substrates, the security inks and the security printings. With this categories we cover all the stages of production of a security document. We add also in these section what are the possible attacks a counterfeiter usually performs to forge an ID or a banknote.

We believe that in the other surveys created until now, not enough importance has been given to digital tampering. The availability of internet and the access to efficient and high quality image editing software for the majority of the population, creates a window for counterfeiters to be introduced in the forging world or to perfect their counterfeiting techniques. Nowadays the research of algorithms for detect tampering is more needed than ever. We divide this section in two depending on the availability of the original image and its access. If the original image has never been we propose several tampering detection algorithms, on the other hand if its possible to be in contact with the manufacturer which grants access to the original image, it is possible to use watermarking techniques.

Another section which is not frequently mentioned in the previous surveys is the dataset section. Here we found one of the main drawbacks for comparing anti-counterfeit algorithms. There is no public available datasets for counterfeit detection in IDs and banknotes. This leads to every researcher to build their own private datasets where it will extract some results that in most cases nobody would be able to reproduce. Also the difficulty of create these datasets to gather both genuine and counterfeit samples makes that each private dataset which generally contains few samples. Typically, this small subset of samples difficultly will represent the big

variety of cases in the open-world scenarios.

At the approaches section we present the state-of-art approaches for counterfeit detection on IDs and banknotes. We categorize this section into preprocessing, feature extraction and classification. Ultimately we discuss some of these works and the pros and cons of applying them for future research. Here we believe that future works on counterfeit detection, should be clear about the dataset information they used to generate the results. They should also use FPR and FNR metrics which are much more representative than accuracy metrics. Both FPR and FNR are not sensitive to changes in data distributions and hence both metrics can be used with imbalanced data.

Similarly to the approaches section, the section of systems and application suffers from the same problems. At these section we focus into the state-of-art of complete systems or smartphone application, because we believe one of the main purposes is to provide a wide range of population a set of tools to check for counterfeits in an accessible, affordable and comprehensible fashion.

We think that there no exists a single visible deterrent feature which is readily recognizable, highly durable, difficult to counterfeit or simulate, costly affordable, and easy to produce. A best strategy is to select a combination of features, which adds complexity to the counterfeiter's task and increase the number of counterfeiting steps to the point that the casual counterfeiter would eventually "give up". Discouraging the counterfeiter is harder and is best accomplished by having a larger number of anti-counterfeit features, each requiring a different means and material for simulation. The objective here is one of attrition, overwhelming the counterfeiter with so many tasks. Stopping dedicated professional counterfeiters is very difficult, the only thing it can be done is to periodically add new features designed to produce delays into the counterfeiter's production cycle.

To our knowledge we present in this work on of the most completes studies in anti-counterfeit features for security documents. One of the purposes of this work was to provide a reference for future researchers of the available datasets that they can work to continue developing new algorithms and techniques for counterfeit detection. Unfortunately the availability of ID and banknote datasets for this field continues to be an issue. Further study should be done in how it could be possible to create these datasets, without infrincting PII and copyright issues, to share for the research community and create a baseline of results.

In this work, we focus only in identity and banknotes. Both share similar anti-counterfeiting security features. A future line of work, would be doing the same analysis of tamper-evident labels, cheques, product authentication, stock certificates, postage stamps, etc. Then compare which of these objects has similar security features and which ones has easier available datasets. The objective would be two-fold. First study to possibility of using security detection algorithms of one object

to the other. Second study if its possible to transfer knowledge between models trained in one printing security object dataset to the other.

Part I

Counterfeit with classical approaches

3 Dataset

The second contribution of this thesis is the creation of a banknote counterfeit dataset. This is the first public dataset for researchers that has been shared until today. The purpose of making it public, it is that the research of counterfeit detection will continue progressing. This dataset could be use as a comparison baseline between present and future algorithms in banknote counterfeit detection. The dataset has been evolving during the completion of this thesis. Hence, three different configurations of the dataset exists. This chapter provides the details of the dataset and its configurations.

3.1 Scan-printing procedure

At the introduction section 1.4 of this thesis we mention the *scan-printing* procedure. There are security measures that are difficult to duplicate by printing without the specialized printers used by the manufacturers. The printers used by the legal manufacturers of security documents usually can not be obtained for regular citizens. A considerable amount of not highly skilled fraudsters produce replicas of the security document they want to counterfeit with publicly available commercial printers. Almost all of the security features present at the original document will be altered with commercial printing, fact that opens a door for document experts and computer vision algorithms to detect these counterfeits. Printing with commercial printers usually follows, what we refer as the *scan-printing* procedure.

A counterfeiter usually follows three steps to create a replica using the scan-printing procedure Figure 3.1. First they scan the security document at a high-resolution to loose the least possible amount of information. Afterwards, they may alter the original document with fraudulent data with an image editing software. Either free and proprietary image editing software has reached a level of quality that any person without a professional knowledge in these tools can create excellent forgeries. Finally they print the forged document with a commercial printer. Nowadays, commercial printers publicly available on the market are affordable for any wanna-be counterfeiter and produce high quality printings. During the whole

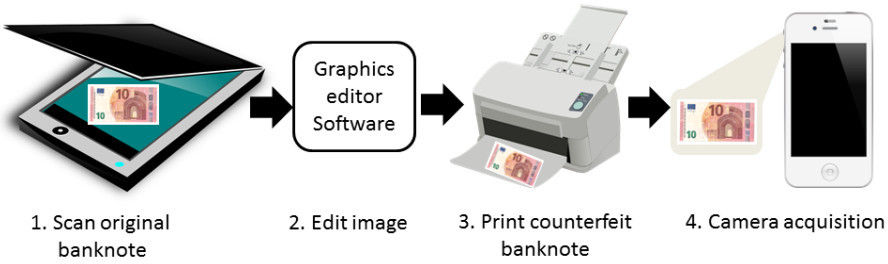


Figure 3.1 – Counterfeit generation images. The genuine scanned banknote is modified with a image software. Afterwards is printed with a high resolution printer to finally acquire the counterfeit printed banknote with a camera.

process, the final printed counterfeit document have lost details at each one of the steps. Hence the security features at the counterfeit does not resemble the ones present at the original document. In scan-printing, if the document is scanned at high resolution and the tampering with the image edition software is done with enough expertise, from the three steps the critical loose of details belongs to the printing stage. Guilloche, intaglio and vignettes contain fine-line patterns that are affected by scan-printing procedure and usually present a degradation visible by the naked eye.

A use case for the scan-printing procedure in banknotes would be scanning the banknotes and then, without tampering the document, printing many copies of it. These counterfeit banknotes can be later use by the counterfeiter to finance its illegal activities or to buy goods fooling the seller. Although not a common case it is surprising how many news are still appearing on the media occasionally.

In the case of an IDs, scan-printing procedure is much more frequent. The counterfeiter may be asked to acquire a photo of its ID with a smartphone. Many applications installed on mobile devices, such as for booking hotels, rental agencies, opening bank accounts, etc. force their user to do a first registration step to grant access to their services. This prior authentication step requires to acquire his physical ID with the smartphone camera. The counterfeiter in this case may create a new forged IDs from scratch using image editing software and a blank template of the document found online. Another case would be to do the three steps in the scan-printing operation for a stolen ID, or counterfeiter own ID altering some bio-data information.

3.2 Background textures for counterfeit detection

We could use most of the security features already presented in section 2.5 to authenticate a security document after the scanning-printing operation. However, initial conditions were posed for the execution of this thesis. First condition was to solve the problem of scan-printing of IDs. Second was that we should follow the restrictions of usage of the company pipeline. The pipeline of the industrial system to process the previous application ID scenarios is composed by 3 steps:

1. The user acquires the full security document through a smartphone with a single photo acquisition in a non-controlled environment. The application sends the complete image document to a cloud server.

2. The cloud server receives an image and processes the counterfeit validation. In case the sent document is an identity document, the personal information data is extracted to keep registry of the user of this service.

3. The response is sent back to the client of smartphone application if is a genuine document. Otherwise an alert is given to the corresponding authorities if the document is counterfeited.

The industrial system pipeline discards many of the anti-counterfeit measures because they need to use video instead of a single image. The security features that need high resolution should be discarded too because we need to capture the whole document. If this was not the case, it would be possible to capture just an area of the document at a close distance, hence augmenting the working resolution [145]. All security features related with source lights wavelengths different that the day light are discarded too. Hence, the main objective of this thesis is to check the security measures visible to the naked eye like Guilloche, intaglio, vignettes, etc. that contains fine-line patterns and security designs, which are affected by the scan-printing procedure.

It is worth saying that we do not expect to catch high-skilled counterfeits. The restriction of resolution acquiring the whole document hinders the detection of this types. We can only target subset of scan-printing counterfeits, if they use expensive printers in the market that can reproduce with high fidelity these fine-line patterns, they scan at high resolution and they were careful enough in their image software tampering operation. Just capturing as a first stage the more obvious ones it is already a success in terms of business operations.

3.3 Creating the dataset

The work of this thesis initially started as the identification of counterfeit identity document using the background security features. However, it does not exist public datasets corresponding to this task, see section 2.7. The copyrights laws and government data protection rules make counterfeit detection datasets very difficult to obtain.

Another contribution of this thesis is to present a new banknote dataset complementary to identity documents. The reason to create a banknote dataset, comes from the observation that most of the security features in the banknotes are also present in the identity documents. Another reason to create initially a dataset of banknotes and not start creating an ID dataset from the start, is the friction with the owner of the original ID. Usually people is not predisposed to lend its IDs to other persons due privacy reasons. Making a reliable dataset of IDs is much harder than banknotes.

We have created a camera-based Euro banknote dataset with genuine and counterfeit samples[1]. The images are acquired as a normal user could do. So we acquire the full banknote at close undetermined distance (allowing background) and also in a non-controlled environment. The counterfeit images are generated through the scanning-printing procedure, see Fig. 3.1. The genuine banknote is scanned at 1200 dpi resolution with the HP Deskjet F2280 scanner. Afterwards the counterfeit is printed with the banknote original size using HP Color LaserJet CP4520 printer.

We use six different acquisition devices: two digital cameras (Cannon PowerShot SX 200 and Cannon EOS 1200D), one tablet (Samsung Galaxy Tab 4) and three mobile cameras (Iphone 4S, Samsung Galaxy S2 and Bq Aquaris E5). Due to the characteristics of the cameras, see Table 3.1, and the non-controlled environment, under low luminance conditions the banknote image could present noise such as blurring or motion blur. Taking into account that the user will never fit perfectly the banknote on the camera margins, some background will certainly appear deducting resolution to the final image. Hence the banknote resolution will depend on the distance from the camera lens to the banknote and also from camera hardware. Also working with RAW images are still not common in mobile devices, so we set all the cameras to the minimum JPEG available compression.

Two different light conditions are considered to build the dataset: L_N means ambient light source which is the light that is available naturally, and L_A refers to the images taken under some artificial light source such as lamp or halogen. Different

[1] The Euro banknote datasets presented at this chapter are available upon request by contacting the authors of this work. IDs are not available due to PII law protection data.

Table 3.1 – Dataset cameras (from left to right): Galaxy S2, Iphone 4S, Aquaris E5, Galaxy Tab 4, Canon Powershot SX200 and Canon EOS 1200D. Large sensor size and less pixel density tend to provide better image quality despite the lower resolution. Smaller sensor size and/or aperture will cause noisier images in low light environments.

Camera	S2	4S	E5	Tab4	SX200	EOS1200D
Sensor size	1/3.2"	1/3.2"	1/3.2"	1/3.2"	1/2.3"	APS-C
Aperture	f/2.6	f/2.4	f/2.2	f/2.6	f/3.4-5.3	f/3.5-5.6

daytime hours and different locations have been used as acquisition scenarios. We acquire all the images without using camera flash, hence the images under L_A will be more subject to noise distortions.

The dataset comprises the Euro banknotes of 10€, 20€, 50€, see Table 3.2. We select texture patches focused on zones with Intaglio printing (ink that is below the surface used to engrave characters and structures) and background fine-line patterns, such as Guilloches and Vignettes. The Intaglio printing has been proved to be robust and one of the most reliable methods to defense against counterfeits [143].

The banknotes coordinates are established manually. Afterwards different patches within the cropped banknote are set. These patches are checked manually to be correctly centered. Although this revision, the patches are not perfectly registered at pixel precision.

3.4 Adding IDs to the dataset

As stated in the previous section, the initial requirement of this industrial thesis was to detect identity documents counterfeits based on the background textures. In a second stage of this thesis, we were able to get ID images, from the Spanish identity card. These images come from a real industrial scenario, subject to PII, with just a few images that were following the scan-printing procedure. We additionally created scan-printing counterfeits and we use the same acquisition and printing devices of the previous section. We also follow the same settings of environment acquisitions.

We combine the banknote dataset presented in Table 3.2 with the ID dataset and add two more €5 banknote classes. The €5 classes are clearly biased to contain counterfeit examples and it is the smallest set compared with other banknotes. The rest of the datasets are biased to contain more genuine samples which resembles the chance to find a counterfeit in reality. One of the tasks to perform with this

Table 3.2 – Created Euro dataset. Alias is the name as we will refer the set in the following sections. Side is the obverse (A) or reverse(R) of the banknote. Patches are the number of background textures validated at each banknote. Ok and False are the number of cropped genuine and counterfeit banknotes, respectively.

Alias	Banknote	Side	Light	Patches	Ok	False
$B1_{L_N}$	10€	A	L_N	6	277	188
$B2_{L_N}$	10€	R	L_N	6	279	182
$C1_{L_N}$	20€	A	L_N	8	290	153
$C2_{L_N}$	20€	R	L_N	5	272	150
$D1_{L_N}$	50€	A	L_N	8	270	211
$D2_{L_N}$	50€	R	L_N	5	275	225
$B1_{L_{NA}}$	10€	A	$L_N + L_A$	6	346	256
$B2_{L_{NA}}$	10€	R	$L_N + L_A$	6	348	242
$C1_{L_{NA}}$	20€	A	$L_N + L_A$	8	392	212
$C2_{L_{NA}}$	20€	R	$L_N + L_A$	5	373	216
$D1_{L_{NA}}$	50€	A	$L_N + L_A$	8	350	309
$D2_{L_{NA}}$	50€	R	$L_N + L_A$	5	351	321

dataset is to compare different state-of-art algorithms for texture feature extraction, see chapter 6. To reduce the computational time complexity of the comparison we decide to remove temporarily the €50 banknotes. We also remove the dataset split that was using only images acquired with an outdoor day light source. This configuration of the dataset and future configurations, use indoor and outdoor light sources combined.

The size of each ROI class ranges between 100×100 pixels from the smaller regions to 600×600 pixels for the bigger ROIs in the present datasets. As a second experimental case we have created an *ID* dataset, more challenging than the *Banknote* dataset because contains more images with noise distortions such as blurring, illumination changes, partial occlusions, etc. Also the *ID* dataset contains less security textures zones which are not altered by the printed personal data. The fact that the *ID* size is larger than the *Banknote* and the previous presented issues makes it closer to a realistic scenario.

3.5 Two dataset sets for generalization

One contribution of this work, is the creation of a new dataset adding 11 new country banknotes, following the same procedure of acquisition and counterfeit

Table 3.3 – Created datasets. Obverse (A) or reverse(R) of the document. nTextures is the number of background textures validated at each banknote/id. Train/Test is the number of documents used for train and test respectively. %Counterfeit is the percentage of counterfeit samples at train/test by this order.

Banknote	nImages	nTextures	Train/Test	%Counterfeit
€5 A	391	10	273/118	71.0/72.8
€5 B	331	10	231/100	66.6/72.0
€10 A	624	6	436/188	39.4/44.6
€10 B	614	6	429/185	40.0/37.8
€20 A	639	8	447/192	34.6/29.6
€20 B	622	5	435/187	34.0/37.9
ID	nImages	nTextures	Train/Test	%Counterfeit
ESPA	1865	10	1305/560	24.5/24.6
ESPB	1268	7	887/381	13.5/17.5

generation with the same acquisition and printing devices. We have created 2 datasets, called *SET1* and *SET2*, see Table 3.4–3.4. *SET1* contains the banknotes used in Table 3.3, but we move the €5 banknote to *SET2* and add the €50 which contains more samples and provides more variance to *SET1*. In *SET1* at test time, the network determines if a new banknote/ID is a counterfeit using background pattern textures which have been seen already during training. *SET2* on the other hand, contains very different textures backgrounds which had never seen by the training network. The purpose of *SET2* is to ensure the network does not overfits and memorizes the patterns of the documents, or learns the figures or text of the background. Both *SET1* and *SET2* are biased to contain more genuine samples than counterfeit samples, which resembles the chance to find a counterfeit document in reality.

Another important change introduced in the dataset is the use of the full banknote for feature extraction. In Table 3.2 and Table 3.3, we use previously cropped regions of interest in which we know it may be beneficial for counterfeit detection because contains highly textured zones. Using the full banknote we are learning an end-to-end model regardless of which region of the document is analyzing.

Table 3.4 – Created dataset SET1. A, B are the front and back respectively. Train/Test is the dataset size for train and test respectively. %Counterfeit is the percentage of counterfeit samples at train/test partitions by this order.

Banknote - ID	nImages	Train/Val/Test	%Counterfeit
€10 ESP A	624	371/65/188	41.0/40.0/40.9
€10 ESP B	614	365/64/185	38.3/48.4/38.3
€20 ESP A	639	380/67/192	34.7/34.3/29.6
€20 ESP B	622	370/65/187	35.9/32.3/34.7
€50 ESP A	486	414/72/209	45.6/44.4/44.4
€50 ESP B	497	423/74/214	45.8/43.2/46.2
ID ESP A	1865	1110/195/560	24.8/28.2/22.8
ID ESP B	1268	754/133/381	13.2/12.0/18.6

Table 3.5 – Created dataset *SET2*. Three letter codes represent ISO alpha-3, for each country. Front and back of the banknotes are included at each set. *SET2* is used for test only. Only ESP banknotes contains 53.9% of counterfeit samples. NClasses represents different countries banknotes designs.

	ESP	EGY	CHN	GBR	IND	KEN
nImages	2720	904	852	259	1229	130
nClasses	6	8	6	4	8	2
	NAM	ROU	SGP	TZA	USA	VNM
nImages	130	390	285	130	316	305
nClasses	2	6	2	2	4	4

3.6 Conclusions and Future work

The presented public dataset and its different configurations is one of the contributions of this thesis. Not previously public document counterfeit dataset was available until this one. We do not share the ID images of the dataset due it contains PII information. We work with highly secured textured documents datasets which are acquired as a normal user could do with a smartphone. The full document is acquired at close undetermined distance (allowing background) within a non-controlled environment. The counterfeits are generated through the *scan-printing* procedure.

As a future work we want to remove the limitation of using a single image and use videos to capture the full banknote at closer distance. This will provide high resolution patches of the document. Later, using image stitching computer vision algorithms a full document image could be sent to the server. The high resolution banknote image dataset and the videos used it to create it, could be shared with the research community to keep on advancing in counterfeit detection. This way not only background security printing can be checked, also many other security features would be available to authenticate.

4 Dictionaries for texture counterfeit

Our aim is to classify a genuine or counterfeit banknote from a single image acquired using a mobile phone camera within a non-controlled environment. The non-controlled environment raises problems such as sensor noise and luminance camera conditions that will affect the textures quality. The idea proposed in this chapter is to use three existing dictionary-based algorithms to represent in the dictionary background textures jointly with image quality degradations. The models also focus into finding a sparse representation of these dictionary coefficients. These approaches extract features that will allow a linear SVM discriminate between fake and genuine banknotes.

4.1 Sparse coding

Due to the camera-based non-controlled environment acquisition, the validated texture ROIs can contain sensor noise, shift translation, motion blur and other artifacts. The complexity of a model to deal with all these variations would be high and not suitable for this problem. A better idea is to generate a dictionary with the most representative texture ROIs which combined could represent most of the texture possible variations. In this section three different dictionary-based approaches are described: K-SVD, SIFT-BoW and SCSPM.

The dictionary can be optimized such as only a few combination of elements will represent a large amount of observed data, which is known as sparse representation. Sparse representation of images consist of finding a set of prototype signals $d_i \in \mathbb{R}^N$, also called atoms, that form a dictionary $D \in \mathbb{R}^{N \times K}$ which can be used to represent a set of given signals $y \in \mathbb{R}^N$ based on a sparse linear combination of dictionary atoms. Hence, for a given set of signals Y, we are looking for a candidate dictionary D such that $y_i \approx Dx_i$, being x_i a coefficient vector representing the linear combination and $y_i \in Y$. Typically D is a redundant dictionary with $N \ll K$. Mathematically, sparse representation can be posed as an optimization problem, where D and x_i are the variables to be found in

$$\min_{D,x_i} ||y_i - Dx_i||_2 \text{ , where } ||x_i||_0 < T \tag{4.1}$$

and $||x_i||_0$ represents the l_0 norm which counts the amount of non-zero elements of the coefficient vector and T is an established threshold controling the sparseness of the representation.

The objective problem is to find a dictionary and a sparse linear combination of the atoms in the dictionary that suits the desired signal. Given an over-complete dictionary D, the following methods try to learn a set of sparse coefficients x_i that feeds a linear SVM classifier. This classifier detects the counterfeits texture images by discriminating the atoms that represents them. As a preprocessing step the image source contrast is enhanced using histogram equalization on the grayscale image source, see Fig.4.1.

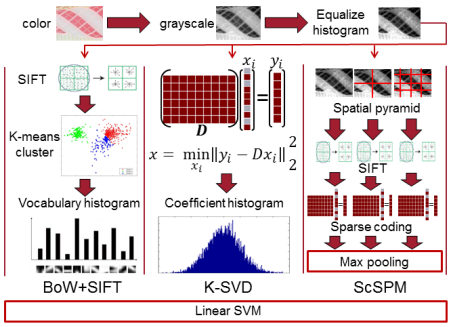


Figure 4.1 – Proposed methods scheme. A linear SVM classifier is applied for each method. The variables explanation in K-SVD can be found in subsection 4.1.1.

4.1.1 K-SVD algorithm

Finding an appropriate D is not a trivial matter, but even more difficult is the computation of the exact determination of the sparsest representation of coefficients x_i, which is a NP-hard problem. Although if T is small enough, is it possible to find approximations to the best solution with different algorithms. Orthogonal matching pursuit (OMP) algorithm addresses the problem of finding a sparse representation by finding the atoms iteratively. OMP adds maximum information and reduces the error reconstruction of the representation in each iteration. This method can be summarized in three steps:

1. Select atom from the dictionary with maximum projection on the residual.
2. Update $x^k = \text{argmin}_{x^k} ||y - Dx^k||_2$
3. Update residual $r^k = y - y^k$

Different approaches can be followed to construct D. If a fixed dictionary independent of y is used, for instance with a wavelet over-complete representation, this dictionary design may not be able to reconstruct all possible signals y. Thus it is possible to build a data dependent dictionary focusing in the application signals y. Such dictionary can be formed of unions of orthonormal bases and updated sequentially by the SVD calculation of its atoms. Aharon *et al.* presented the dictionary learning algorithm K-SVD, [15]. Let $Y = \{y_i | i \in [1,K], y_i \in \mathbb{R}^n\}$ be the complete set of observed signals and X as the matrix of all vectors x_i. (4.1) can be reformulated as,

$$\min_{D,X} ||Y - DX||_2^2 \text{ , where } ||x_i||_0 < T \tag{4.2}$$

K-SVD algorithm, from a initial estimation dictionary alternates iteratively between sparse coding the input data of the actual dictionary and update the atoms in the dictionary to better adapt the data.

Fixing D in (4.2) the problem now consists of finding the efficient code vectors x_i for each input signal y_i, which is done by the explained OMP algorithm. Once all x_i are found, then X is fixed, and SVD is used to tune the dictionary D from the previous estimation. Only a single atom d_k is updated at a time. Finally when all atoms in the dictionary are updated all the process starts all over until the algorithm converges.

Rubinstein *et al.* developed an efficient K-SVD algorithm and we use this implementation, [181]. The initial dictionary can be chosen between using a random initialization strategy or using an initial 2D-DCT basis. We use the random configuration because although the 2D-DCT basis D initialization is well-suited for natural image patches, it does not provide a good fit for piecewise-constant patches. We create a single feature vector of size D where the absolute $||x_i||_0$ values are accumulated for y_i.

4.1.2 SIFT-BoW algorithm

Sivic *et al.* proposed Bag-of-words (BoW) framework which is a well-known approach to image classification, [205]. This algorithm can also be posed as a dictionary learning algorithm. In this case, let $Y = [y_1, \ldots, y_N] \in \mathbb{R}^{N \times Z}$ be the local SIFT descriptors extracted from the texture patches in a N-dimensional feature space. The K-means clustering optimization problem can be formulated as

$$\min_{D} \sum_{i=1}^{N} \min_{c=1\ldots C} ||y_i - d_c||^2 \tag{4.3}$$

where $D = [d_1, \ldots, d_C]$ are the C cluster centers to be found, also named *codebook*,

which will correspond to the dictionary. In this specific case, let $X = [x_1, \ldots, x_N]$ be the indices that belong to a determinate cluster, then (4.3) can be re-formulated into a matrix factorization form as

$$\min_{D,X} \sum_{i=1}^{N} ||y_i - x_i D||^2 \text{ , subject to } ||x_i||_0 = 1 \tag{4.4}$$

where $||x_i||_0 = 1$ means that only one element is not zero. The activated index x_i indicates within which cluster belongs the vector y_i. Notice that (4.4) and (4.2) are almost identical. The main difference is that in sparse representations x_i have a small number of non-zero elements. Hence it is possible to say that K-SVD dictionary learning algorithm generalizes the K-means clustering process. Finally in the BoW approach, a single feature vector is computed as the average of x, which is the histogram representation of each texture image. These histogram feed a linear SVM for counterfeit texture detection.

4.1.3 SCSPM algorithm

Following K-SVD and SIFT-BoW, Yang *et al.* presented SCSPM which joins SIFT features and sparse coding instead of the K-means vector quantization, [242]. They used spatial pyramid matching kernel (SPM) to overcomes the problem of discarding the spatial order of local descriptors. When the set of local descriptors are encoded with a dictionary element a pooling function is needed. Different image statistics are built upon the decision of the pooling function. BoW uses an averaging pooling function, yielding to the histogram feature. SCSPM approach use a max pooling function on absolute sparse codes. A concatenation of the pooled features at different locations and scales are concatenated to form a spatial pyramid representation of the image.

As in K-SVD, the dictionary D initialization is created from random patches from the texture images. Once the initial estimation of D is fixed, code vector x_i for each input signal y_i in (4.2) is computed with the *feature-sign search* algorithm proposed by Lee *et al.*,[133]. Fixed the code vectors X from (4.2), it is converted to solve a least square with quadratic constraints problem, which they compute with the Lagrange dual as used in [133].

4.2 Performance metrics and statistical comparison

The performance criterion chosen to test the algorithms performance is the area under the receiver operating characteristic curve (AUC). For each dataset and method

AUC is

$$\overline{\text{AUC}} = \frac{1}{TF}\sum_{f=1}^{F}\sum_{t=1}^{T}\text{AUC}_{t,f} \tag{4.5}$$

where T denotes the total number of texture patches, F the total number of k-folds and $\text{Auc}_{t,f}$ the AUC value for the t texture and f-fold. Demsar work justified the use of Friedman's test and Nemenyi post hoc tests to test for significance of AUC when multiple datasets and multiple algorithms are used,[67, 91, 158]. Let r_j^i be the rank of the i-th algorithm on the j-th of M data sets. The Friedman test compares the average ranks of the algorithms R, as

$$R_i = \frac{1}{M}\sum_{j=1}^{M} r_j^i \tag{4.6}$$

Friedman statistic χ_F^2 defined in (4.7), is distributed according to the Chi-square distribution with $G-1$ degrees of freedom, being G the total number of algorithms. The null-hypothesis states that if the ranks R_i are equal the algorithms should be equivalent. If χ_F^2 is large enough the hypothesis can be rejected and there is difference between the algorithms.

$$\chi_F^2 = \frac{12M}{G(G+1)}\left(\sum_{i=1}^{G} R_i^2 - \frac{G(G+1)^2}{4}\right) \tag{4.7}$$

If the null-hypothesis is rejected, the post hoc Nemenyi test can be applied to find any significant differences between individual algorithms. Two or more algorithm performance results are significantly different if their average rank differ by at least the critical difference CD, as defined in (4.8). Here the q_α is based on the studentized range statistic divided by $\sqrt{2}$.

$$\text{CD} = q_\alpha\sqrt{\frac{G(G+1)}{6M}} \tag{4.8}$$

4.3 Experimental Set-up and Results

The patches selected at each data set have different sizes of 512×512 and 256×256 pixels. The minimum resolution threshold of the cropped banknotes that forms the dataset is 400 dpi. All the images have been resized to 600 dpi as working resolution for stable intrinsic feature detection of Intaglio,[143]. At each dataset a

5-fold approach is followed to sample a training set holding out 40% of the data for testing the algorithms.

To evaluate the performance of the proposed methods, we select three different state-of-the-art approaches from Chapter 2. We use FSIM to extract a 2 feature vector for each texture, which are the similarity scores for the grayscale and color image respectively. Second algorithm of comparison is the 17 feature vector of IQA measures. We will name this algorithm as 17Quality. Last comparison algorithm is the 2D-SIWPT with a grayscale histogram equalization as image source. We use the extracted 6 feature vector to detect counterfeit textures.

For the proposed benchmark we have set the algorithms parameters empirically. SIFT-BoW, K-SVD and SCSPM are set to use a dictionary size of 512. Experiments on our dataset with dictionary size of 1024 show a slight increment on performance, which is not justified by the increment on processing time. The SIFT-BoW approach use a fast library to approximate nearest neighbors (FLANN) to match the SIFT feature descriptors with the vocabulary. In K-SVD and SCSPM we use $100K$ training blocks extracted from the noisy images to create the initial estimation of dictionary D. A block size of 8×8 and 32×32, for K-SVD and SCSPM respectively obtains better performance. The interval in pixels between neighboring patches blocks is determined as 1 pixels and 6 pixels for K-SVD and SCSPM respectively. Finally the value $\sigma = 0.02$ and $\sigma = 0.15$, in K-SVD and SCSPM respectively, specify the noise power in dB (PSNR) used to determine the target error for sparse-coding each block. Other parameters are left as their default in their respective algorithms implementations. Finally we use a linear SVM to learn and classify all the algorithms for a fair comparison. All the algorithms are coded in MATLAB, except SIFT-BoW which we have implemented with Python in our computer Intel Xeon E5-1620 with 3.50GHz CPU and 16GB RAM.

Table 6.2 reports the $\overline{\text{AUC}}$ values of all 6 classifiers on the proposed benchmark. Friedman test statistic and corresponding p-value states that the results are significant and as a consequence the post hoc Nemenyi test can be applied to each class distribution. Being $p = 0.05$ the critical value for the two-tailed Nemenyi test $q_\alpha = 2.728$, then the critical difference CD = 2.0835. It is possible to appreciate that the proposed approaches in this paper perform much better than the comparison algorithms and are robust to noise when L_A images are added. It is thus possible to conclude that the techniques that use dictionaries are outperforming the current approaches to counterfeit background printing detection. Between the three proposed approaches, SCSPM has the highest score, being close to achieve a perfect counterfeit classification for the proposed datasets. However SCSPM is also the slowest algorithm as can be seen in table 4.2 being a handicap for its use in real-time applications. The performance of K-SVD and SIFT-BoW are close to the one of SCSPM, but it is not possible to say they are significantly different because

Table 4.1 – Benchmark results. $\overline{\text{AUC}}$ results on test set data sets.

	$\chi^2_F = 440.4083 \quad (p = 0.05)$					
	SIFT-BoW	K-SVD	SCSPM	FSIM	2D-SIWPT	17Quality
$B1_{L_N}$	0.9752	0.9907	**0.9997**	0.6834	0.7792	0.8999
$B2_{L_N}$	0.9745	0.9901	**0.9992**	0.8048	0.7527	0.8900
$C1_{L_N}$	0.9964	0.9981	**0.9998**	0.7439	0.8030	0.9211
$C2_{L_N}$	0.9923	0.9956	**1.0000**	0.7523	0.7792	0.8616
$D1_{L_N}$	0.9824	0.9911	**0.9992**	0.6884	0.6964	0.8741
$D2_{L_N}$	0.9592	0.9923	**1.0000**	0.6711	0.6916	0.8561
$B1_{L_{NA}}$	0.9646	0.9892	**0.9996**	0.6718	0.7656	0.8829
$B2_{L_{NA}}$	0.9606	0.9865	**0.9989**	0.7766	0.7448	0.8638
$C1_{L_{NA}}$	0.9859	0.9949	**1.0000**	0.6664	0.7552	0.8860
$C2_{L_{NA}}$	0.9822	0.9943	**1.0000**	0.7105	0.7510	0.8422
$D1_{L_{NA}}$	0.9799	0.9913	**0.9997**	0.6399	0.6843	0.8554
$D2_{L_{NA}}$	0.9643	0.9938	**1.0000**	0.6477	0.6734	0.8333
R	3.0000	2.0000	**1.0000**	5.8333	5.1667	4.0000

their rank do not differ by at least CD. The AUC results indicate that K-SVD and SCSPM outperform the rest of the algorithms, since they deal more efficiently with all possible texture ROIs variations due to the iterative update of the atoms in the dictionaries and sparse coefficients to represent each texture.

Among the comparison approaches, FSIM was performing the worst, which was expectable because is an structural IQA and it has to deal with non-perfectly registered patches in the current dataset. Despite the good counterfeit detection from the work in [95] using the WPT it could not deal with our dataset. We have observed that the histogram shape result from 2D-SIWPT of Intaglio regions of our ROIs does not correspond with the expected, which is due to luminance variations and some acquisition images which where originally under 600 dpi. Another reason of the poor results is mostly that we used Intaglio regions as ROIs, but there are some which are only fine-line patterns from the background. The best result among the comparison approaches is provided by the 17Quality algorithm, slightly increasing the expected 80% of the authors results. The combinations of different IQA measures compensates the noise that affects the structural texture similarity metrics and color luminance variations which gets poor color quality metrics.

Table 4.2 – Testing time for each different texture sizes in seconds.

	SIFT-BoW	K-SVD	SCSPM	FSIM	2D-SIWPT	17Quality
256×256	0.1063	1.2408	2.0997	0.2005	0.1895	0.9072
512×512	0.5265	3.5376	9.4853	0.2317	0.4985	3.5376

4.4 Conclusions and Future work

To the best of our knowledge the problem of background printing authentication has never been treated as a sparse representation problem. Applying dictionaries and sparse representations yields to a very good performance in counterfeit classification for the proposed benchmark improving the state of the art algorithms. Results have demonstrated than K-SVD and SCSPM are the best approaches being the last one slightly better. Our hyphotesis is that spatial location and the max pooling function are the key difference between them. The spatial location is an important matter to this kind of problem because a ROI could contain different isotropic textures patterns. Both approaches have proven of being capable of covering most of the camera-based uncontrolled environmental acquisition problems.

Although this scheme has proven to be efficient with the counterfeit samples generated with one printer, further research should be done with different inkjet and laser printers during the scan-printing procedure. Also, further study should be done to test which are the minimum counterfeits samples required to train a classifier to maintain an acceptable rating of forgery detections. Following this line of work it would be possible to pose the problem as an anomaly detection problem, where few counterfeit data samples are available. Further work that could be conducted is to study the influence of preprocessing methods on the image source which could lead to better detail texture, such as super-resolution algorithms.

5 Service-Oriented Architecture for counterfeit detection

Another contribution of this thesis is a mobile-server framework to detect counterfeit documents. The purpose to build this infrastructure is to create a Proof of Concept (POC) to transfer knowledge between the researched methods and the company that participates in this industrial thesis. The end-to-end system proposed provides: a low cost solution fit to be used with common smartphones, flexibility for further updates and robust validation methods. The mobile-server framework also intends to address the lack of tools to generate datasets acquired from smartphone devices [1].

5.1 System architecture and components

The system proposed in this work has been designed for ID documents, however, as mentioned before, it is generic enough so it can be used for other documents with security background texture as banknotes. The main functionality is the analysis of the document authenticity from a single image using a mobile phone camera within a non-controlled environment. This process is used by services or products that require a genuine identification of the client, such as renting a car, opening a bank account, applying for a loan, checking-in in an hotel, etc. Once authenticity of the document is validated, the purpose of the platform where the service is integrated can take place (reading and storing the personal information of the document holder).

We follow the document acquisition approach given by the authors in [25] and we build a service-oriented architecture (**SOA**) end-to-end counterfeit validation framework. The proposed SOA application is composed by integration of distributed, separately-maintained and deployed software components. The end-to-end system developed is scalable and provide fast responses. The image

[1] The framework code is available in https://github.com/gitabcworld/e-Counterfeit

acquisition procedure is easy and friendly for the user. Finally, this framework provides a way to store and manage the new data that is being sent to the server for further improvements.

5.2 Server Framework

We have built a server which communicates with a client mobile application, see Fig. 5.1. First a user acquires a document photo which sends through JSON REST API to our server. Through post/get messages we establish a handshake protocol to send the validation image and receive the response information. A web server is set up on top of the operating system to send the HTTP requests, but it could also serve static files like images, JavaScript files, HTML pages, etc. We use NGINX as our web server for its resource efficiency and responsiveness under load. Once the web server has the data, it process the JSON message with Flask, which is a micro-framework for Python focused at web application code. Since a web server cannot communicate directly with Flask, we implement a Web Server Gateway Interface (WSGI) to act as a proxy between the server and Python/Flask. As a summary we have HTTP requests routed from the web server to Flask, which Flask handles appropriately. The responses are then sent right back to the web server and, lastly, back to the end user application. The Flask module will unpack the JSON message containing the image to process. The image along with other data will be stored in a MySQL database. An ID is assigned to this image and is given back to the client. The image will not be processed immediately, it will be managed by Celery, a queue manager which will be constantly querying through multiple workers the database for new images to process. Meanwhile the mobile clients will establish a handshake protocol intermittently asking for the result to the server using the given ID. Finally each one of the queue manager workers will access the counterfeit module which will process the image and store the result in the database. The counterfeit module integrates into this framework languages as Matlab, OpenCV, VlFeat, C++, Python and Torch, with the purpose to evaluate different existing algorithms written in their respective languages by their authors. Identity documents are also preprocessed to find blurring and highlights although these algorithms are out of the scope of this paper.

5.3 Mobile client

The mobile client application is designed to aid a non-expert user through the steps of acquiring a valid photo, see Fig. 5.2. The first step helps the user guiding visually

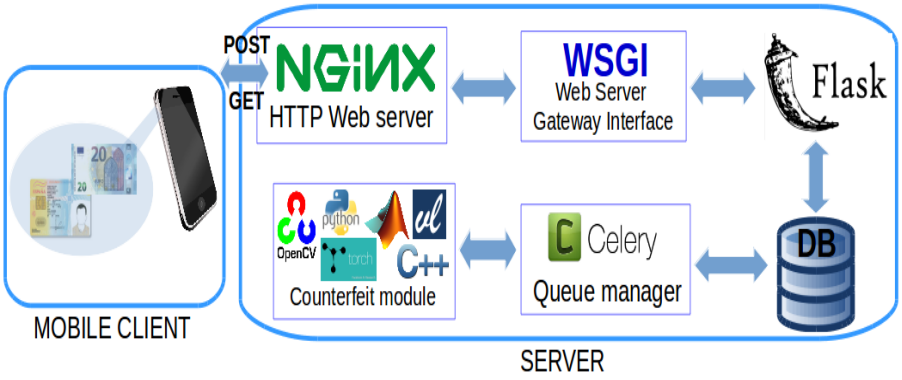
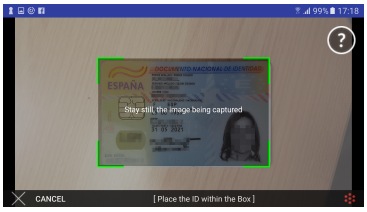


Figure 5.1 – Server-client counterfeit framework. A document is acquired with a mobile application by the user. The image is sent to the server which stores this image into a database through the web-server. Afterwards a queue manager manages several workers, which are reading simultaneously from the database to process the images with the Counterfeit module. Finally the results are sent back to the user. The WSGI module is used to connect the HTTP messages with Python Flask module that centralizes all the operations.

to fit the document around a rectangle, which adapts its size to the model of the document being acquired. The photo is automatically acquired after checking the document fits the visual guides and the camera is focused. Detecting perfectly the rectangle surrounding the document is a complicated task because of the non-controlled environment acquisition. Clutter, blurring and illumination can affect the precise cropping of the document.

In the second step we follow the pipeline in Fig. 5.3 to crop the document. We apply the GrabCut algorithm driven by the position of the visual guides [33]. We define the foreground as a zone inside the visual guides. The probable foreground will be a zone with a certain margin around the visual guides and the rest will be considered as background. In this operation the image is resized to a 15% of its size to speed-up the operations. We then binarize the image with the zones labeled as probable foreground returned by the GrabCut algorithm. To find the corners we calculate the contours of the binary mask and filter the lines which do not fulfill a minimum length. Afterwards we calculate all the possible intersection points of those lines, and select only four intersections which are closer to the borders of the image. All this methodology could be replaced by an automatic detection of the rectangle of the document of the document. However we have found that



(a) Adjust photo

(b) Crop

(c) Show results

Figure 5.2 – Screen shots from the mobile application. In 5.2a the application helps the user to acquire the auto-photo with visual guides. In 5.2b a GrabCut algorithm is applied for a better crop of the margins of the document. Finally a in 5.2c shows the validation of each one of the ROIs and the final decision (genuine or counterfeit) is overlayed. It also ask the user to collaborate with the groundtruth dataset. Better viewed in color.

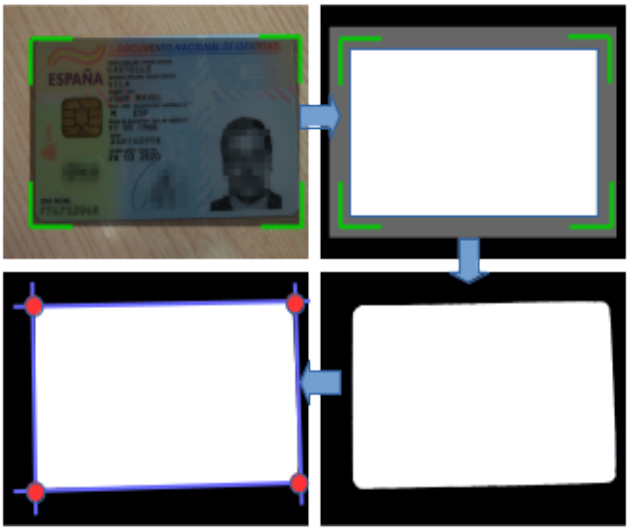


Figure 5.3 – The GrabCut algorithm and dewarping done in the mobile application. Top-left shows the visual guides to help the photo acquisition. At the top-right image the zones which are foreground (white, interior of visual guides), probably foreground (gray, interior and exterior of visual guides with a margin) and background (black). Bottom-right is the resulting cropping from GrabCut. At bottom-left we find the intersections of the longest lines to perform a dewarping operation to finally correct the perspective of the cropped document.

providing a user friendly interface with a visual guide ensures a minimum size, focus and correct cropping of the document to guarantee a correct further processing. Finally the dewarped document is sent to the server and wait asynchronously for its response. The last step of the client is to show the results. We overlay on the cropped documents the regions that we are processing and the results of the validation for each one of the regions of interest (ROIs), we also show the final decision for the document if its genuine or counterfeit. Before closing the current view, we ask the users to help for further development and contribute with our dataset labeling the current document if it is genuine or counterfeit. This label is sent to the server and the database is updated accordingly. The crowdsourcing task to generate ground truth can be disabled by the user in the configuration.

5.4 Counterfeit module

The back-end of the SOA architecture consists in the main module of the service. It is an interchangeable Counterfeit module which validates texture descriptors. It is also directly connected with the database which makes possible to train new models automatically as soon as enough images of a certain model are stored. We follow the idea presented by the authors in [56] and build a similar architecture for feature extraction, see Fig. 5.4. This architecture consists of the following tasks: Texture descriptor extraction, Principal component analysis (PCA), a pooling encoder to improve the representation of the descriptors and a linear Support Vector Machine classifier (SVM). We also include an additional layer that is the Bernoulli Naïves Bayes to construct the final decision of labeling a document as genuine or counterfeit. Let us further describe these tasks:

Texture descriptor

Although any texture feature can be used to represent the textures, we have selected **dense SIFT** because it is generally very competitive, outperforming specialized texture descriptors [25, 56].

Encoder

A pooling encoder converts the local descriptors to a single feature vector suitable for tasks such as classification with an SVM. We evaluate orderless and order-sensitive pooling encoders. The orderless encoder is invariant to permutations of the input meanwhile the order-sensitive is not. Order-sensitive encoder may be ineffective or even counter-productive in natural texture recognition, but on this counterfeit context it can be helpful to recognize different textured objects and a global description of the texture scene at each ROI.

The best-known orderless encoder is the Bag of Visual Words (**BoVW**), which characterizes the distribution of textons [136]. Similarly to BoVW, Vector of Locally-Aggregated Descriptors (**VLAD**) and Fisher vector (**FV**), assigns local descriptor to elements in a visual dictionary obtained with K-means and Gaussian Mixture Models (GMM) respectively [118, 166]. BoVW only stores visual words occurrences, meanwhile VLAD accumulates first-order descriptor statistics and FV uses both first and second order statistics of the local image descriptors. As a generalization of K-means, we also include as orderless encoder the **K-SVD** dictionary learning algorithm, which creates a dictionary for sparse representations via a singular value decomposition approach [14].

On the other hand, Spatial pyramid pooling (SPP) is the most common order-

sensitive encoder method [132]. It divides the image in subregions, computes any encoder for this regions and afterwards stacks the results. We use the spatial pyramid histogram representation **ScSPM** where the encoded descriptor is the concatenation of local histograms in various partitions of different scales [241].

PCA

The 128-dimensional descriptors extracted from the texture descriptors step are reduced using PCA. Besides improving the classification accuracy, this significantly reduces the size of the posterior encoding dimensionality. We also include a PCA after the encoder, because VLAD and FV are usually highly compressible vectors so we further reduce the descriptor encoding for comparison purposes [164].

Linear SVM

The learning uses a standard nonlinear SVM solver. We train a specific classifier for each ROI for every document. At this point we predict a genuine or counterfeit binary label value determining the ROI authenticity. We normalize the texture descriptors encodings to zero mean and unit variance before SVM classifier.

Bernoulli Naïves Bayes

From the previous step we obtain a binary feature vector for the ROIs, however we need the final document decision. We learn a naïve Bayes classifier according to multivariate Bernoulli distributions, where the decision rule is based on Eq. (6.1). The binary terms x_i represents the occurrence or absence of counterfeit ROIs. Being $P(x_i|y)$ the likelihood of x_i given a counterfeit/genuine document (y) and p_i is the a priori probability of counterfeit documents in the training set.

$$P(x|y) = \prod_{i=1}^{n} p_i^{x_i} (1-p_i)^{(1-x_i)} \tag{5.1}$$

5.5 Experimental Set-up and Results

For all the experiments in the training data we set a 10 k-fold cross-validation to optimize the SVM parameters. We repeat 5 times a boostrapping approach to hold out a 30% of the data for testing set at each dataset in all the following experiments. We repeat also 5 times the computational time experiments but using only a test image. For the proposed benchmark all parameters are set empirically. For feature extraction with dense SIFT we set a keypoint sampling with a step size of $s = 4$. The

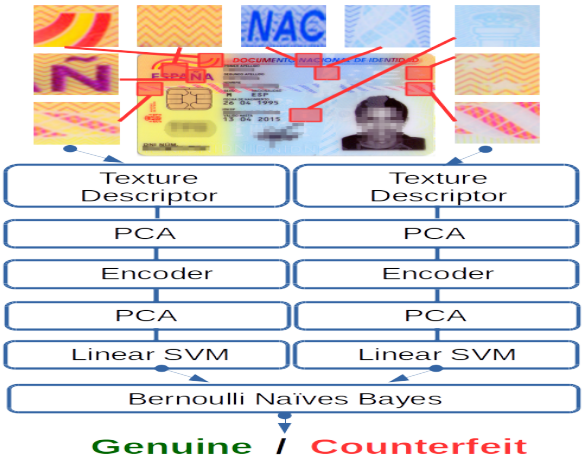


Figure 5.4 – Proposed architecture for document authentication. The texture descriptor is first reduced with a PCA. After an encoder is learned to improve the feature representation. The encoded texture descriptor dimensionality is again reduced with a PCA to classify each ROI with a linear SVM. A multivariate Bernoulli model predicts the final document decision authenticity.

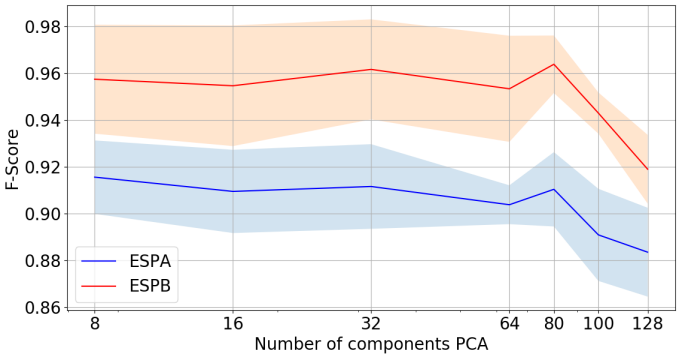


Figure 5.5 – Comparison between number of PCA components and μ/σ F1-score. PCA before BoVW encoder with $K = 512$. X-axis in logarithmic scale.

feature dimensionality from dense SIFT is further reduced to $D = 80$ using PCA, see Fig. 5.5.

5.5.1 Time evaluation

In Table 5.1 we find a decomposition of the complete time between the acquisition and the shown results from Fig. 5.2c. We include the average time for a non-experienced user from the moment they want to acquire a new document until he fits the visual guides near the document. The auto photo is the time spent to automatically acquire the photo with the best focus when the document corners are close to the visual guides. Right now, one of the bottlenecks, in time consumption, is the GrabCut and storing the image in the mobile device. However this step is needed if we want to reduce the time spent for the image transfer to the server. These times are calculated using a HSPA+ internet connection with a maximum upload speed of 5.76 Mbits/s. Image transfer and cropped image storing time can be reduced if instead sending the full image we send and store only the ROIs needed for the evaluation. The time would depend then on the number of evaluated ROIs. So it is possible to discard the less discriminative ROIs and speed-up the process. Further work needs to be done in the mobile application to reduce the acquisition and cropping time, which actually represents approximately 93% of the total time. The server side is processing the 10 ROIs and returning a genuine or counterfeit document response under 1 second. For the presented time results we use the smartphone BQ Acquaris M5 to calculate the mobile client times and the Intel(R) Xeon(R) CPU E5-1620 v3 @ 3.50GHz on the server side.

Table 5.1 – Average time in milliseconds for processing 10 ROIs of one ESPA document using BoVW with K=512.

		400 dpi	600 dpi	800 dpi
Mobile app	User Guide Position	2500	2500	2500
	Auto Photo	980	1053	1066
	GrabCut+Storing	4104	5930	8603
	Send Image	1043	2113	4376
Server	Highlight+Blurring	187	217	222
	Feature Extraction	389	667	861
	Classification	50	52	50
Total time		9253	12610	17678

Table 5.2 – μ and σ F1-score results from different encodings with the created datasets.

Banknote	BoVW	VLAD	FV	SCSPM	KSVD
ESPA	0.910 ± 0.015	0.9585 ± 0.002	$\mathbf{0.981 \pm 0.005}$	0.964 ± 0.008	0.884 ± 0.021
ESPB	0.963 ± 0.012	0.981 ± 0.005	0.988 ± 0.002	$\mathbf{0.988 \pm 0.001}$	0.939 ± 0.018

5.5.2 Evaluation of datasets

In table 7.1 we can see the results of applying different encoders to the reduced descriptor with PCA. We set $K = 512$ words for BoVW and K= 64 for the rest of the encoders. VLAD, FV and SCSPM use a much smaller codebook as these representations multiply the dimensionality of the descriptors. K-means can be considered as a generalization of K-SVD, where only one element of the dictionary is activated each time. Relaxing the sparsity term constraint to be more than one dictionary element, K-SVD augments the representativity of the dictionary with smaller codebook. For K-SVD we build an histogram with the absolute values of the coefficients returned from the Orthogonal Matching Pursuit algorithm (OMP). With SCSPM we partition the image into $2^l \times 2^l$ segments in different scales $l = 0, 1, 2$. With comparison purposes we train a PCA with $D = 512$, so all the sparse coding representations are reduced to the same size. FV is among the best encoding used followed close by SCSPM and VLAD. FV obtains a $\overline{FAR} = 2.88\% \pm 0.96, \overline{FRR} = 2.92\% \pm 1.27$ and $\overline{FAR} = 2.08\% \pm 0.37, \overline{FRR} = 2.31\% \pm 1.45$ for ESPA and ESPB respectively. VLAD and FV have a good performance because they encode enrich information about the visuals word's distribution. The max spatial pooling from SCSPM also prove is robust to local spatial translations. Although K-SVD results are slightly worse than

BoVW, the dictionary has been reduced by a factor of 8.

5.6 Conclusions and Future work

We have presented a novel application to detect ID counterfeit documents. This application is an end-to-end system that covers from the smartphone client acquisition to the evaluation of the document and final response to the client. Along the way we also build a dataset of security documents and the whole architecture schema is thought to be modular and scalable. Generating individual models for each ROI allows to introduce new documents to the system without the requirement of retraining previous models. The application can be easily extended to support banknote counterfeit detection due the strong correlation with ID background textures. One possible extension is the integration of detection and identification in the mobile application in a single step. This could be done with the recent CNN architecture presented in YOLO V2 [179]. Using a joined identification and detection would facilitate the user experience and would be able to send the dewarped image once the minimum required resolution is achieved.

From BoW towards CNN Part II

6 Feature statistical evaluation for counterfeit textures

The last two chapters show how it is possible to build efficiently a dictionary with different features and how this can be build into a complete framework. However, there is not a solid study which compares different feature extractors, validate in terms of counterfeit detection and it is scalable for the security document authentication framework. The contribution at this chapter is an exhaustive evaluation of different texture descriptors across several banknote and identity document datasets. We also compare the computational time efficiency between descriptors with the idea of a real industrial scenario usage.

6.1 Hand-crafted to learnt CNN textures

Since the introduction of Alexnet [128], hand-crafted features are outperformed in most cases by the learned features of the latests generations of deep CNNs. However, when the dataset is small sized, this is not always true and the classic hand-crafted features must be considered as well. We evaluate 6 different types of texture category descriptors: image quality assessments (IQA), gradient based descriptors, pattern binary based, array of band-pass filters (Filter banks), Convolutional Neural Networks (CNNs) based descriptors and a mixture of texture descriptors algorithms (Other).

6.1.1 IQA based descriptors

Full reference image quality assessments (IQA) like SSIM or FSIM are perceptual metrics, the first quantifies image quality degradation and the second measures the local structure and contrast information [229, 247]. These approaches are based on cross correlation of patches previously set. Also a 17 feature vector to detect banknotes made by inkjet and laser printers can be done with join pixel differences, similarity, frequency domain and human visual system related features [186]. As the authors in [25] we name it 17Quality. Another approach uses statistical indicators of

the gray-level co-occurrence matrix (GLCM) to describe texture in an image, where the spatial relationship of pixels is considered [105]. We select 13 textural GLCM indicators: Contrast, correlation, energy, homogeneity, mean, standard deviation, entropy, root-mean-square, Variance, Smoothness, Kurtosis, Skewness and Inverse Difference Movement, which we call Statistical.

Gradient based descriptors

Histograms of Oriented Gradients (HOG) are used to extract global texture features [66]. In the context of object recognition the best known local descriptor is SIFT [146]. We also evaluate SURF descriptor, which is several times faster and its authors claim to be more robust against different image transformations [24].

6.1.2 Binary pattern based descriptors

Variants of the standard Local Binary Patterns (LBP) operator are considered the state-of-the-art among texture descriptors in several datasets because of its robustness to lighting changes, ability to code fine details and low computational complexity [161]. Afterwards the quantized LBPs is averaged over the image to build a histogram. CSLBP compares center-symmetric pairs of pixels instead of comparing surrounding pixels with the center pixel in LBP [109]. It is tolerant to illumination changes and computationally efficient. CLPB solves the loss of magnitude information by the original LBP [97]. The algorithm assigns a 2P-bit code to the center pixel based on the gray values of a local neighborhood comprising P neighbors.

6.1.3 Filter banks based descriptors

Filter banks have traditionally played and important role in texture classification. Leung-Malik (LM) is a multi scale, multi orientation filter bank with 48 filters [136]. The filters contain 2 Gaussian derivative filters at 6 orientations and 3 scales, 8 Laplacian of Gaussian filters and 4 Gaussian filters representing a edges, bars and spot filters at multiple scales and orientations. They combine all the filters responses using a vector quantization algorithm to form textons which represents human texture perception. Similar to LM, the maximum Response (MR8) filter bank comprises 38 filters but only 8 filter responses [220]. The oriented filters corresponding to the bar and edge are reduced at each scale by using the maximum filter responses at all orientations. Collapsing the filters to 8 filter responses ensures that each filter in the filter bank is rotationally invariant. Frequency and orientation representations of the Gabor filter are similar to those of the human visual system. BGP algorithm removes the pre-training in LM or MR8 of learning by clustering a texton dictionary

and present a rotation invariant texture representation [248]. They form an image histogram of rotation invariant binary Gabor patterns at multiples scales. GIST is a global descriptor that convolves the image with 32 Gabor filters at 4 scales and 8 orientations in a $4x4$ grid to represent the dominant spatial structure of a scene [163]. More focused in banknotes the 2D incomplete shift invariant wavelet packet transform 2D-SIWPT detects counterfeit intaglio printed textures [144]. The authors build an histogram of wavelet coefficients to calculate a 6 dimensional feature vector with σ^2, kurtosis and skewness statistics.

6.1.4 CNNs based descriptors

Along with AlexNet, we also evaluate an improved version of the original VGG, which is a 16-layer model increasing depth using an architecture with very small (3x3) convolution filters [201]. Googlenet is a 22 layers deep network which introduces the inception modules, that act as multiple convolution filter inputs with the intuition that visual information should be processed at various scales and then aggregated so that the next stage can abstract features from different scales simultaneously [208].

6.1.5 Other hand-crafted descriptors

With comparison purposes we densely extract patches of size 3×3 and 7×7 of the input image, and flatten these patches to obtain 9 and 49 dimensional feature vectors. We also evaluate the color correlogram global histogram descriptor that captures the spatial correlation of colors in an image [113]. Segmentation based Fractal Texture Analysis (SFTA) decompose the input image in a set of binary images an then computes the fractal dimensions of the regions borders [58]. The authors claim this descriptor is 3.67 faster than Gabor and 1.6 faster than GCLM statistical indicators from [105] with higher performance. LPQ is a texture descriptor robust to blurring and invariant to uniform illumination changes [162]. It is based on binary coding of the quantized Fourier phase computed locally around each pixel. WLD histogram combines the relative intensity differences of a current pixel against its neighbors, the intensity and gradient orientation of the current pixel [52]. LPQ and WLD have obtained very good results in texture analysis task and both are related but complementary to the LBP method. Inspired in LBP and LPQ, BSIF computes a binary string for each pixel in an image to represent the local structure [121]. Each bit within the BSIF descriptor is the quantized response of a linear filter, outperforming state-of-the-art results in textures datasets.

6.2 Architecture

We build a classical computer vision classification pipeline in order to compare raw texture descriptors, see Fig. 6.1. After extracting the texture descriptor we apply the well-known orderless encoder, Bag of Visual Words (BoVW). We continue with the linear Support Vector Machine (SVM) as binary classifier for each one of the ROIs of each model. Once we have the learned threshold for the decision function we form a binary vector with the raw responses of each ROI from the SVM, $x_i = \{0,1\}$. The binary terms x_i represent the occurrence or absence of counterfeit ROIs, but we still need the final decision of the document. We want all the checked ROIs, either genuine or counterfeit, to explicitly penalize the non-occurrence of a feature x_i. For this purpose, we learn a naïve Bayes classifier according to multivariate Bernoulli distributions, where the decision rule is based on Eq. (6.1). Being $P(x_i|y)$ the likelihood of x_i given a counterfeit (y) document and being p_i the a priori probability of counterfeit documents.

$$P(x|y) = \prod_{i=1}^{n} p_i^{x_i}(1-p_i)^{(1-x_i)} \tag{6.1}$$

6.3 Experimental Set-up and Results

6.3.1 Computational time efficiency

In Fig. 6.2 we display F1-score/time results with the ESPA document for all the presented algorithms in section 6.1. The time evaluation also includes preprocessing steps like cropping the ROIs, analysis of blurring and highlights; and posterior classification, which is the same for all texture algorithms. HOG descriptor stands out as the best classification result with a processing time of 610 ms for the 10 ROIs. The second best descriptors are the CNN based, showing lower computational time and similar F1-score with small variances between them. Most of IQA and binary pattern based descriptors have low computational time requirements but they are not at the top F1-scores. The filter bank descriptor category presents the slowest time behavior and inside the mixed category LPQ produces a good F1-score/time ratio. Looking at these results we can form a general idea of which texture descriptors are more suitable to use for an application, but we still do not know if their F1-score differences are kept for the datasets from Table 3.3 and if they are statistically significant.

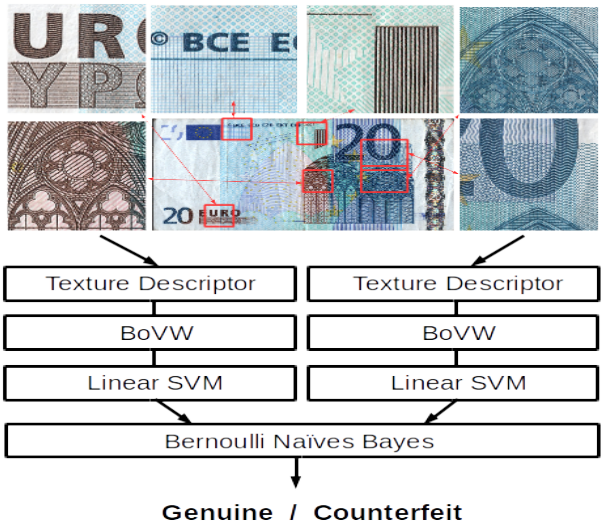


Figure 6.1 – Architecture pipeline. After the texture descriptor, BoVW is used as descriptor encoder. Linear SVM is applied for ROI classification and Bernoulli Naïve Bayes evaluates the inter-ROIs predictions to classify the final document response. The image ROIs inputs are from €20 A dataset.

6.3.2 Statistical evaluation

Table 6.2 reports the results for the algorithms presented in section 6.1 for each dataset. From these results we conduct Friedman test X_F^2 with the Nemenyi post-hoc test to verify if there is a significant statistical difference between the performance between the different presented algorithms over multiple datasets [67]. We obtain $X_F^2 = 158.63$ and $X_F^2 = 44.12$ for the *Banknote* and *ID* datasets respectively, both reject the null hypothesis because are higher than the critical value 42.56. The rejection of the null hypothesis was expected because the opposite would mean there is no difference between the average ranks and all the algorithms have the same responses across the datasets. We know there are significantly differences of the methods but we do not know which specific classifiers are different. The post-hoc Nemenyi test returns a critical difference CD which is the value the average rank from the algorithms should differ. We found that this test was capable of detecting the best and the worst algorithms, but does not provide any insight about the intermediate performing algorithms due to it discards the variance between the bootstrapped datasets. Taking into account the analysis of variance from the

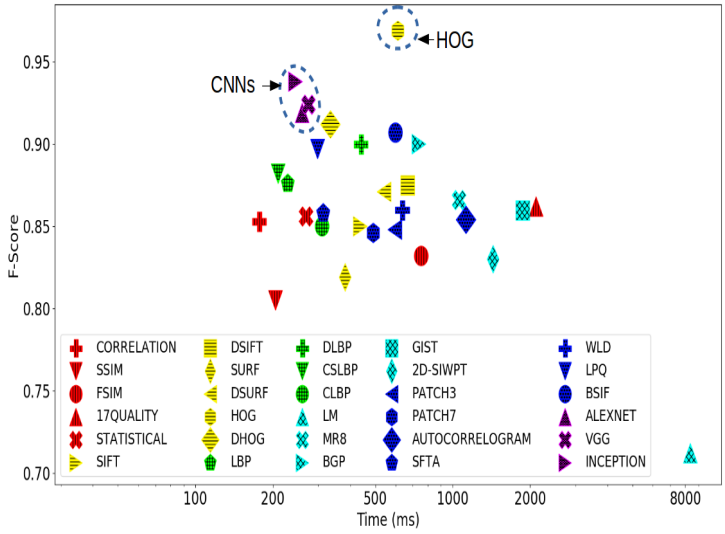


Figure 6.2 – Test time and F1-score performance of evaluated texture descriptors of *ID* dataset. The markers correspond to the algorithms in 6.1. Test time includes: cropping 10 ROIs of ESPA, highlight and blurring evaluation, feature extraction and evaluation. X-axis in logarithmic scale. Better viewed in color.

datasets partitions we applied one-way ANOVA with the Tukey's Honestly Significant Difference (HSD) post-hoc test [87, 214]. We set the groups of the one-way ANOVA as the 30 texture descriptor algorithms and the samples for each group are the number of datasets times the number of k-folds, so we have 30 and 10 samples for *Banknote* and *ID* datasets respectively. We have used the tool in [3] to calculate the one-way ANOVA and HSD values, which returns $p \approx 0$ for both datasets hence allow us to also reject the null hypothesis. In the next section we compare each one of the algorithms from the HSD results[1] with all the previous statistical results.

6.3.3 Results comparison

From HSD values we can affirm there is no statistical differences between HOG, CNN based algorithms, DHOG, DLBP, BGP and BSIF in both datasets outperforming the rest of the texture descriptors included in the comparison. For the *Banknote* dataset we can state that the IQA based algorithms (except Correlation), SURF

[1] https://github.com/gitabcworld/icdar2017/blob/master/evalTexture/anova_hsd.txt.

and SIFT from the gradient category, 2D-SIWPT, Correlogram and WLD perform statistically worse than the majority of the rest descriptors. We can also find others descriptors like LM and MR8 that are significantly better than CSLBP. In the *ID* dataset we also found that MR8 filter bank achieves better results than LM in *ID*. 2D-SIWPT and IQA based algorithms does not suffer from the unbalanced €5 dataset and have a same statistical behavior than the majority algorithms. Next we follow with a deeper insight into the performance of the selected algorithms by categories:

IQA based

Correlation is significantly different than other IQA algorithms in *Banknote*. We argue that incorporating the structural spatial information prior knowledge of the match template compensates the fact that the rest of IQA descriptor have short dimensionality descriptors which are not able to discriminate the variability between ROI patches. This prior knowledge from the correlation does not hold in *ID*, because there is more variance in the texture patches.

Gradient based

SIFT and SURF dense sampling works better than their corresponding keypoint detectors because they are not loosing important keypoints in noisy texture zones. HoG is already doing a dense sampling with its blocks and cells, it is why statistically is the same as its dense version.

Binary Pattern based

CSLBP tries to address the dimension problem of the traditional LBP and retain the ability of texture descriptor, although in the current dataset the vector quantization scheme LBP_u already resolves this issue performing better than CSLPB. CLBP has similar performance at *Banknote* than LBP_u, but it is outperformed by $DLBP_u$.

Filter Banks based

A well designed Gaussian filter bank is thought to be a good model of how humans distinguish texture, it is why most of the filter bank algorithms manage to capture most of the texture variations in *Banknote* dataset, but lacks a better filter bank design for *ID*.

CNN based

The three CNN descriptors show good computational time behavior and robustness across datasets. This fact, confirms the high capacity of the presented convolutional

networks to generalize for different types of datasets.

Others

Algorithms such as $\text{PATCH}_{3\times3,7\times7}$ have a good texture classification, thanks to the BoVW dictionary learned. The Correlogram does not include any spatial information and the genuine and counterfeit patches from the *Banknote* dataset sometimes are difficult to differentiate using only color information. Despite SFTA is statistically worse than HOG and CNNs, its simplicity, low dimensionality and fast extraction times make us consider this descriptor for further testing or combine with other algorithms. LPQ statistically does not outperforms LBP_u in both datasets. The edge detection and robustness to noise and illumination from WLD was expected to be one of the better algorithms, but was unable to cope with *Banknote* difficulty. The authors in [121] claim that BSIF has a better overall performance than LBP and LPQ, but the computed HSD statistics do not provide enough evidences to claim so. However we can confirm that their learned filters from a small set of natural images work in different applications as the current datasets.

6.4 Conclusions and future work

We have statistically evaluated the state-of-the-art descriptors for texture description in security documents. We have divided the datasets in two groups by their different challenging conditions to evaluate the presented algorithms. Hand-crafted feature descriptors are outperformed nowadays by CNN based descriptors. However we have seen that several texture hand-crafted descriptors performance does not differ from the CNN descriptors and should not be discarded a priori. HOG features are the more suitable descriptors if we take into account the memory and computation time limitations ratio present in an industrial application for both datasets. CNN fine-tunning usually outperforms an existing, pretrained CNN for an specific dataset because it progressively concentrates into the details of the new data classes characteristics. However a drawback to this knowledge transfer, in our case, is the unbalanced dataset that we dispose to further training, because naturally we will always have a lack of counterfeit samples. Another drawback is that, if we fine-tune a specific CNN for each ROI is not possible to maintain a memory-scalable system and if we train a single CNN model for all ROIs, then we would have to retrain for each new ROI. Further research should be done towards the creation of a single model which could differentiate the introduction of artifacts between genuine and counterfeit textures regardless of which type of document or texture we are dealing with.

Descriptor	Banknotes					
	€5 A	€5 B	€10 A	€10 B	€20 A	€20B
CORRELATION	**0.94 ± 0.04**	0.90 ± 0.05	**0.93 ± 0.01**	**0.94 ± 0.01**	0.87 ± 0.01	0.90 ± 0.10
SSIM	0.91 ± 0.03	0.48 ± 0.03	0.92 ± 0.01	0.91 ± 0.00	0.85 ± 0.03	0.76 ± 0.01
FSIM	0.16 ± 0.19	0.39 ± 0.20	0.75 ± 0.01	0.79 ± 0.02	0.78 ± 0.01	0.78 ± 0.03
17QUALITY	0.86 ± 0.02	**0.90 ± 0.03**	0.88 ± 0.07	0.76 ± 0.03	0.79 ± 0.03	0.78 ± 0.03
STATISTICAL	0.64 ± 0.06	0.58 ± 0.05	0.72 ± 0.02	0.77 ± 0.02	**0.89 ± 0.01**	0.73 ± 0.07
SIFT	0.78 ± 0.03	0.84 ± 0.03	0.80 ± 0.05	0.78 ± 0.07	0.93 ± 0.01	0.84 ± 0.03
DSIFT	**0.99 ± 0.00**	**0.98 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	0.99 ± 0.02	**1.00 ± 0.00**
SURF	0.54 ± 0.11	0.51 ± 0.10	0.76 ± 0.05	0.77 ± 0.01	0.91 ± 0.03	0.79 ± 0.04
DSURF	0.95 ± 0.02	0.95 ± 0.01	0.97 ± 0.00	0.97 ± 0.00	0.98 ± 0.00	0.97 ± 0.01
HOG	0.98 ± 0.01	**0.98 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	**1.00 ± 0.00**	**0.99 ± 0.00**
DHOG	0.97 ± 0.01	0.97 ± 0.01	0.98 ± 0.00	0.96 ± 0.01	0.99 ± 0.00	0.99 ± 0.00
LBP_u	0.86 ± 0.04	0.93 ± 0.03	0.92 ± 0.01	0.93 ± 0.01	0.95 ± 0.01	0.94 ± 0.01
$DLBP_u$	**0.94 ± 0.01**	**0.98 ± 0.01**	**0.98 ± 0.00**	**0.98 ± 0.00**	**0.99 ± 0.00**	**0.98 ± 0.00**
CSLBP	0.84 ± 0.03	0.91 ± 0.01	0.92 ± 0.01	0.90 ± 0.02	0.93 ± 0.00	0.86 ± 0.03
CLBP	0.94 ± 0.02	0.97 ± 0.01	0.94 ± 0.03	0.93 ± 0.01	0.93 ± 0.01	0.83 ± 0.02
LM	**1.00 ± 0.00**	0.99 ± 0.00	**0.99 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	0.99 ± 0.00
MR8	0.99 ± 0.00	**1.00 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	0.99 ± 0.00
BGP	0.99 ± 0.01	0.99 ± 0.00	0.99 ± 0.09	**0.99 ± 0.00**	**0.99 ± 0.00**	1.00 ± 0.00
GIST	0.99 ± 0.01	0.99 ± 0.00	0.98 ± 0.00	0.98 ± 0.01	**0.99 ± 0.00**	0.99 ± 0.00
$2D-SIWPT$	0.00 ± 0.00	0.00 ± 0.00	0.75 ± 0.03	0.79 ± 0.02	0.77 ± 0.01	0.79 ± 0.01
ALEXNET	**0.98 ± 0.00**	0.98 ± 0.01	**0.99 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	0.99 ± 0.00
VGG	0.98 ± 0.01	0.98 ± 0.01	**0.99 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	0.99 ± 0.00
INCEPTION	0.98 ± 0.02	**0.99 ± 0.01**	0.98 ± 0.00	0.98 ± 0.00	**0.99 ± 0.00**	**1.00 ± 0.00**
$PATCH_{3x3}$	0.98 ± 0.02	0.98 ± 0.02	0.98 ± 0.00	0.96 ± 0.01	**0.99 ± 0.00**	0.88 ± 0.02
$PATCH_{7x7}$	**0.98 ± 0.01**	**0.99 ± 0.01**	**0.99 ± 0.00**	0.94 ± 0.01	0.97 ± 0.01	0.90 ± 0.00
CORRELOGRAM	0.58 ± 0.08	0.75 ± 0.05	0.83 ± 0.03	0.79 ± 0.02	0.82 ± 0.01	0.79 ± 0.02
SFTA	0.96 ± 0.01	0.97 ± 0.01	0.97 ± 0.00	0.92 ± 0.01	0.98 ± 0.00	0.95 ± 0.01
WLD	0.80 ± 0.04	0.79 ± 0.04	0.76 ± 0.05	0.88 ± 0.02	0.84 ± 0.01	0.81 ± 0.03
LPQ	0.93 ± 0.03	0.95 ± 0.02	0.93 ± 0.01	0.92 ± 0.04	0.96 ± 0.00	0.95 ± 0.00
BSIF	0.98 ± 0.02	0.97 ± 0.01	**0.99 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**	**0.99 ± 0.00**

Table 6.1 – Benchmark results for banknotes. $\mu_{\text{F1-score}}*$ and $\sigma_{F1-score}$ of the 5 bootstrapping test sets. Each block corresponds to the algorithm types in 6.1. In bold the best descriptors by category and dataset.

Descriptor	ID	
	ESPA	ESPB
$CORRELATION$	0.85 ± 0.00	$\mathbf{0.93 \pm 0.00}$
$SSIM$	0.80 ± 0.02	0.92 ± 0.00
$FSIM$	0.83 ± 0.03	0.91 ± 0.00
$17QUALITY$	$\mathbf{0.86 \pm 0.01}$	0.90 ± 0.01
$STATISTICAL$	0.85 ± 0.00	0.91 ± 0.00
$SIFT$	0.85 ± 0.02	0.90 ± 0.01
$DSIFT$	0.87 ± 0.01	0.92 ± 0.01
$SURF$	0.81 ± 0.03	0.91 ± 0.00
$DSURF$	0.87 ± 0.01	0.91 ± 0.01
HOG	$\mathbf{0.96 \pm 0.00}$	$\mathbf{0.98 \pm 0.00}$
$DHOG$	0.91 ± 0.00	0.92 ± 0.01
LBP_u	0.87 ± 0.01	0.91 ± 0.00
$DLBP_u$	$\mathbf{0.90 \pm 0.00}$	$\mathbf{0.93 \pm 0.00}$
$CSLBP$	0.88 ± 0.01	0.92 ± 0.01
$CLBP$	0.85 ± 0.01	0.91 ± 0.00
LM	0.71 ± 0.07	0.93 ± 0.01
$MR8$	0.86 ± 0.01	0.92 ± 0.01
BGP	$\mathbf{0.90 \pm 0.01}$	$\mathbf{0.95 \pm 0.00}$
$GIST$	0.86 ± 0.00	0.93 ± 0.01
$2D-SIWPT$	0.83 ± 0.01	0.89 ± 0.01
$ALEXNET$	0.91 ± 0.01	0.97 ± 0.00
VGG	0.92 ± 0.01	$\mathbf{0.98 \pm 0.00}$
$INCEPTION$	$\mathbf{0.93 \pm 0.01}$	$\mathbf{0.98 \pm 0.00}$
$PATCH_{3x3}$	0.84 ± 0.00	0.90 ± 0.01
$PATCH_{7x7}$	0.84 ± 0.01	0.91 ± 0.01
$CORRELOGRAM$	0.85 ± 0.00	0.91 ± 0.00
$SFTA$	0.85 ± 0.01	0.91 ± 0.02
WLD	0.86 ± 0.01	0.91 ± 0.00
LPQ	0.89 ± 0.02	0.91 ± 0.01
$BSIF$	$\mathbf{0.90 \pm 0.02}$	$\mathbf{0.92 \pm 0.01}$

Table 6.2 – Benchmark results for IDs. $\mu_{\text{F1-score}}*$ and $\sigma_{F1-score}$ of the 5 bootstrapping test sets. Each block corresponds to the algorithm types in 6.1. In bold the best descriptors by category and dataset.

7 Recurrent Comparator for counterfeit detection

Previous banknote and security document counterfeit detection algorithms can be summarized as no-reference classification algorithms. We change this philosophy and convert the task of counterfeit detection in a end-to-end full-reference game of spotting the differences between a genuine and the evaluated document. The contribution in this chapter is the application and adaptation of an end-to-end full-reference deep learning network, which iteratively peeks different regions of the security texture backgrounds to spot the counterfeit documents, from now on denoted as Counterfeit Recurrent Comparator (CRC). The principal hypothesis is that playing the game of spot the differences between images, which humans usually use to compare objects, focusing each time the glimpse in a different region is sufficient to detect common counterfeit documents produced by the *scanning-printing* operation[1].

7.1 Human visual object comparison

We follow the idea presented by Shyam et al. [198] where their interpretation of how humans compare objects, referred as *human way*, is based in the iterative comparison of two different objects until a final decision about their similarity is given. Humans use to look back and forth both images, repeatedly, until a final observation is made. The observation, or *glimpse* for the next image, will be conditioned by the previous glimpse. For each glimpse, a scale and contextual position is determined by the previous glimpse of the observer. When several regions of the images are compared, the human can determine the degree of similarity for this pair of images. When two images look-alike but belong to different objects more glimpses are needed to differentiate them. The Siamese network pipeline is a similar estimation system for scoring the similarity of two images [36]. It extracts invariant features from two different inputs through two shared-weight sub-networks joined

[1] The code is publicly available at https://github.com/gitabcworld/ConvArc

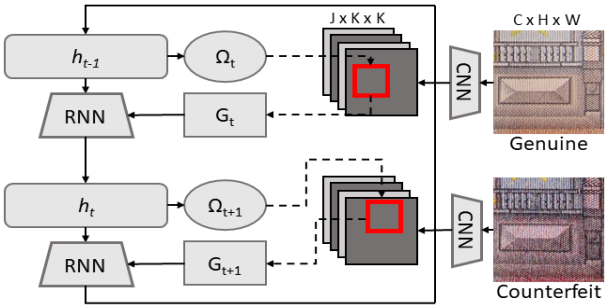


Figure 7.1 – Architecture of Recurrent Comparator. Two images are alternatively compared. At each time-step the attention mechanism changes the region parameters Ω_t of each glimpse. Ω_t is calculated with the previous RNN h_{t-1} state projected from W. RNN internal state h_t depends on h_{t-1} and G_t from the previous glimpse. Dotted line represents the Attention mechanism.

at the head. The two networks learn how to extract the most salient features for each object. In the last stage, the salient features are fused into a similarity score. Hence, the features, which represent a higher abstract level, are independent from each object until the moment of the fusion. Later, Schroff et al. [195] introduced the *triplet loss* to improve the Siamese embedding, using an anchor image, encouraging a relative distance constraint. On the other hand, *human way* of comparing objects, information is fused in the early stages and the knowledge is accumulated through the glimpses. Glimpses will benefit from fusing the more relevant patterns at each stage of the iterative recurrent comparator, due it evaluates the scale and position of the next glimpse based on the previous knowledge, resembling the human foveation. We apply the same schema to spot the counterfeit background textures, which looses the background resolution by the *scan-printing* operation, when compared with genuine backgrounds.

7.2 Recurrent Comparators

In [198], the authors present an algorithmic imitation of the *human way*, see Figure 7.1. The model is based in a recurrent neural network controller and an attention mechanism. Let $I_a = I_g$, $I_b = I_c$ or I_g be a pair of images and I_g, $I_c \in R^{C \times H \times W}$ represents a genuine and counterfeit background textures respectively. The recurrent comparator feeds the network iteratively $I_a \rightarrow I_b \rightarrow I_a \rightarrow I_b \ldots I_a \rightarrow I_b$ a fixed

number of T times. The image I_t a time-step t is determined via Eq. (7.1):

$$\begin{aligned} I_t &= \begin{cases} I_a, & \text{if } t \text{ is even} \\ I_b, & \text{otherwise} \end{cases} \\ Z_t &= \text{CNN}(I_t) \in \mathbb{R}^{J \times K^2} \end{aligned} \tag{7.1}$$

where CNN represents a fully convolutional network, J the number of output filters from the last convolutional layer and K the output filter size. CNN can be the identity matrix $\mathbb{I}$ and feed directly the input image to the recurrent neural network without any use of convolutional features extractors, however in [198] it is demonstrated the significant boost in performance using stack of $2D$ features maps. Θ represents the parameters of the attention glimpse, which consists of the location and size of the glimpse window, see Eq. (7.2). G_t is determined by the projection matrix W_Ω which maps the previous step of the RNN controller h_{t-1} state to the trainable number of attention parameters. Afterwards the attention mechanism A will use the output convolutional features Z_t and the glimpse window parameters Θ_t parameters to calculate the glimpse G_t.

$$\begin{aligned} \Theta_t &= W_\Omega \times h_{t-1} \\ G_t &= A(\Theta_t, Z_t) \end{aligned} \tag{7.2}$$

The next hidden state, see Eq. (7.3), can be computed from the glimpse G_t and the last hidden state observation h_{t-1}, where RNN recurrent controller could be any sequence model, such as a vanilla RNN, Bidirectional RNN, LSTM or GRU.

$$h_t = \text{RNN}(G_t \times h_{t-1}) \tag{7.3}$$

7.3 Where to look? Attention models

To benefit from the early fusion of the glimpses we use the two dimensional form of attention mechanism *DRAW* proposed by Gregor et al. in [96], where it yields an image region of smoothly varying location and zoom, applying an array of 2D Gaussian filters to the input feature map. The $N \times N$ Gaussian filters are located on the image of size K^2 by the grid center coordinates (g_x, g_y) and the stride δ between adjacent filters. The zoom is controlled by the stride, employing a large values of stride enlarges the field-of-view and using a lower stride will increase the resolution of the image region, see Figure 7.2. Five parameters, $(g_x, g_y, \delta, \sigma^2, \gamma)$, are

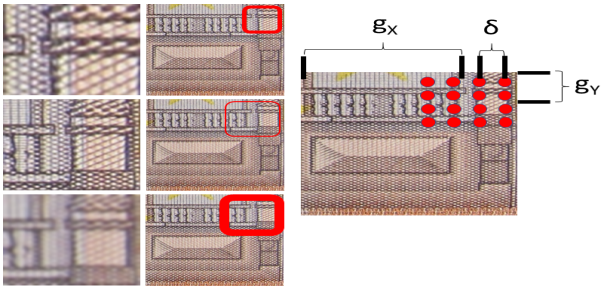


Figure 7.2 – Right column: A 4 × 4 grid of filters superimposed on a background texture. δ corresponds to the stride and the center location (g_x, g_y). Middle column: the red rectangles represent different boundary and precision of the patches (σ) over three patches of 224 × 224 extracted from the input image. Left Column: resulting after applying the 2D grid of Cauchy Kernel. The top image has a small δ and high σ, causing a zoomed-in blurred patch. The middle patch downsamples the image with a large δ and low σ; bottom patch blurs and downsamples the image with a high δ and σ.

dynamically computed at each time step:

$$\begin{aligned} g_x &= (K-1)\frac{\hat{g_x}+1}{2} \quad g_y = (K-1)\frac{\hat{g_y}+1}{2} \\ \delta &= \frac{K-1}{N-1}|\hat{\delta}| \quad \gamma = e^{1-2|\hat{\delta}|} \end{aligned} \tag{7.4}$$

where σ^2 is the isotropic variance of the Gaussian filters and γ a scalar intensity, which multiplies the filter responses. μ_x^i, μ_y^i determine the mean location in the patch of the filter at row i and column j:

$$\begin{aligned} \mu_x^i &= g_x + (i-(N+1)/2)\delta \\ \mu_y^j &= g_y + (j-(N+1)/2)\delta \end{aligned} \tag{7.5}$$

The horizontal $F_x \in \mathbb{R}^{N\times K}$ and vertical $F_x \in \mathbb{R}^{N\times K}$ filterbank matrices are computed in Eq. (7.6), where λ_x and λ_y are normalization constants, to make certain $\sum_a F_x[i,a] = 1$ and $\sum_b F_y[j,b] = 1$, and (i,j), (a,b) are points in the attention patch

and input image, respectively.

$$F_x[i,a] = \frac{1}{\lambda_x}\left\{\pi\gamma\left[1+\left(\frac{a-\mu_x^i}{\gamma}\right)^2\right]\right\}^{-1}$$
$$F_y[j,b] = \frac{1}{\lambda_y}\left\{\pi\gamma\left[1+\left(\frac{b-\mu_y^i}{\gamma}\right)^2\right]\right\}^{-1} \tag{7.6}$$

Finally, the attention mechanism G_t applied on an input image patch of size $N \times N$ can be computed in Eq. (7.7).

$$G_t(I_t,\Omega_t) = F_y I_t F_x^T \tag{7.7}$$

7.3.1 Co-attention for conditioned dependency

Wu et al. [237] introduced the idea of a co-dependency attention model inside the iterative comparison of image pairs. They focus on identifying the most relevant and crucial parts of the images conjoined using an attention map over the two inputs image features before calculating the first hidden state h_t in the recurrent comparator. This method provides and insight of the input images, detecting and localizing common patches, in contrast with the attention mechanism presented in section 7.3. They argue that the recurrent screening on two images is treated independently, without referring to the dependency conditioned on one and another, making unable to memorize which sets of local patterns are critical for the objects differentiation. Their observations can play an important role in the background texture evaluation, focusing only in the more distinctive regions based in the co-dependency initial observation of both input images. Inside the Co-Attn module, see Figure 7.3, the affinity matrix L is computed, see Eq. (7.8). Being $W_L \in \mathbb{R}^{J\times J}$ a trainable weight matrix.

$$L = Z_g^T W_L Z_c \in \mathbb{R}^{K^2\times K^2} \tag{7.8}$$

Each weight $L_{i,j}$ represents the similarity between the feature i in I_c and the feature j in I_g. Softmax is used to normalize all L scores, which generates the probability distribution conditioned on the target features maps, see Eq. (7.9). Each i-th row in T_c of size $\mathbb{R}^{K^2}$, represents the importance of each feature in Z_c respect each i-th feature in Z_g. Analogously the j-th row in T_g defines the importance of each feature

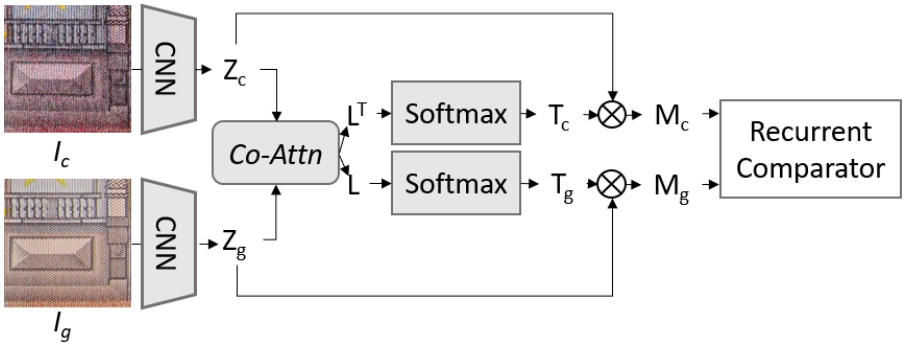


Figure 7.3 – Co-attention encoder over two inputs images, (I_c, I_g) counterfeit and genuine respectively. The computed feature map using a *CNN* for both images (Z_c, Z_g) is used for the calculation of affinity matrices (L_c, L_g) through the *Co-Attn* module, afterwards the affinity matrices are normalized (T_c, T_g). Finally the output features maps (Z_c, Z_g) from each image are weighted using the normalized co-dependent affinity matrices into M_c, M_g.

in Z_g respect each j-feature in Q_a.

$$\begin{aligned} T_c &= \text{softmax}(L) \in \mathbb{R}^{K^2 \times K^2} \\ T_g &= \text{softmax}(L^T) \in \mathbb{R}^{K^2 \times K^2} \end{aligned} \tag{7.9}$$

The attention summaries for the Z_c with respect to Z_g, and viceversa, can be computed with T_c and T_g respectively:

$$\begin{aligned} M_c &= Z_c T_c \in \mathbb{R}^{J \times K^2} \\ M_g &= Z_g T_g \in \mathbb{R}^{J \times K^2} \end{aligned} \tag{7.10}$$

7.4 Experimental Set-up and Results

Another important change introduced in the dataset is the use of the full banknote for feature extraction. In Chapters 6 and 5, previously cropped regions of interest are used knowing it may be beneficial for counterfeit detection because contains highly textured zones. Using the full banknote we are learning an end-to-end model regardless of which region of the document is analyzing. We prepared 2 dataset

configurations for the experimental evaluation:

- No-reference: patches from the images are sampled independently.
- Full-reference: We sample pairs of patches between two different images. The first image is always genuine (I_a) and the second can either be genuine or counterfeit (I_b) in the *Siamese* and *CRC* networks. We set the learning batches to contain 50% of genuine pairs of the same class, 25% of genuine and counterfeit pairs of the same class and the rest are pairs of different classes. The Triplet network also belongs to this category . It always samples a genuine image (I_{a_1}), an anchor image (I_{a_2}) and a counterfeit image ($I_b = I_c$) to form each triplet. If the documents belong to the same class, we crop the patch at the same position of the document. Full-reference comparison provides a prior knowledge which is essential to spot counterfeits documents in real applications. Full-reference information is also accessible and highly valuable in cases such as font type comparison, card holder's portrait against ghost image, signature comparison, etc.

For both dataset configurations we use for training moderate data augmentation consisting of randomly change the brightness, contrast and saturation. We also randomly augment the data applying affine transformations of the image keeping center invariant. Additionally for both training and testing, we randomly crop patches of size $(H, W, C) = (224, 224, 3)$. We discard images under 400 dpis and resize the rest of the images to 600 dpis, established as minimum working resolution for counterfeit Intaglio feature detection [144].

For the Non-reference, as a baseline we use local and global descriptors which were used for counterfeit detection in Chapter 6: LBP [63], HoG [66], SIFT [147], 13 texture features from Haralick [105], GLCM+YIQ [29]. LBP extracts a feature vector of size 26. Only the most relevant 10 keypoints are extracted with SIFT from each patch, which after concatenation outputs a feature vector of size 1,280 for each patch. For GLCM+YIQ we concatenate 6 GLCM properties to the 256 bins luminance histogram to form a 262 feature vector. We also extract 1,568 and 52 features from HOG and Haralick respectively. In Haralick we concatenate the 13 features along the 4 directions. A XGDBoost [53] ensemble method is trained using 5-fold cross validation with each one of the features extracted from these descriptors. We set 140 decision trees with depth 5. Furthermore, we also evaluate PeleeNet [227], an optimized deep learning network approach in terms of size and processing time efficiency, aiming for smartphone deployment.

In Full-reference dataset we use as baseline the Siamese and Triplets networks. We set PeleeNet as CNN to extract the embedding for both architectures. CNN is sequentially composed of CNN_E, CNN_C, which are the feature extraction blocks

and final classification block respectively. CNN_C usually consists of an average pooling and a fully-connected layer. The loss function for Siamese is denoted as:

$$\begin{aligned}\mathscr{L} =& \mathscr{L}_{\text{CT}}(||\text{CNN}_E(I_a)||^2, ||\text{CNN}_E(I_b)||^2) + \\ &+ \mathscr{L}_{\text{CE}}(W_{\mathscr{L}}, \text{CNN}_C(\text{CNN}_E(I_b))),\end{aligned} \tag{7.11}$$

being $\mathscr{L}_{\text{CT}}$ the Contrastive loss [98] and $\mathscr{L}_{\text{CE}}$ the standard cross entropy loss. Similarly for Triplets, we set the loss as:

$$\begin{aligned}\mathscr{L} =& \mathscr{L}_{\text{T}}(||\text{CNN}_E(I_{a1})||^2, ||\text{CNN}_E(I_{a2})||^2, ||\text{CNN}_E(I_b)||^2) + \\ &+ \mathscr{L}_{\text{CE}}(W_{\mathscr{L}}, \text{CNN}_C(\text{CNN}_E(I_b))),\end{aligned} \tag{7.12}$$

being $\mathscr{L}_{\text{T}}$ the Triplet loss [195]. Like in [195] we L_2-normalize the embedding from CNN_E to specify a fixed distance similarity margin for the loss. We set the margin loss to 0.2 for $\mathscr{L}_{\text{CT}}$ and $\mathscr{L}_{\text{T}}$. For the propposed CRC approach we remove the last blocks from CNN_E to have a filter output size of $K = 14^2$ and $J = 512$. We use a LSTM controller as RNN in Eq. (7.3) with 512 hidden states. The number of glimpses is fixed to 8 which makes a total of 16 recurrent steps. For glimpse resolution we set 4×4 size. Binary cross entropy is used as criterion to detect the counterfeits and genuine targets. The rest of not mentioned parameters are set as proposed by their authors or set empirically. Finally, we repeat 100 times the test of each Set and report the mean AUC and σ in table 7.1. As we work with random crop patch positions of the full document, the repetitions ensures almost all document image is covered. For the presented approaches, the model size is 17.8M and 18.1M parameters, with an inference time of 42.1 ms and 46.3 ms for CRC+Attn and CRC+Co-Attn respectively. PeleeNet model size alone represents 2.8M parameters and 12.8 ms. Experiments are done using a NVIDIA TITAN Xp GPU.

From Table 7.1 the results from the classic texture descriptor struggle as expected to learn the counterfeit scan-printing details from *SET1* and drop significantly the performance in *SET2*. It is worth mentioning as showed in 6, HOG manages to capture the global texture information to differentiate counterfeits with a reasonable AUC even in *SET2*. PeleeNet trained as a binary classification problem is outperforming other non-reference methods, being robust when changing to *SET2*. When using the full-reference datasets, the Siamese and Triplet architecture are not able to outperform significantly the classic texture descriptors. Triplets overfits quickly with the training set and is not able to capture the lack of background texture resolution, resulting in wrong predictions for either *SET1* or *SET2* test sets. CRC+Atnn and CRC+Co-Attn achieve the best counterfeit detection result due its more natural way of learning relative representations w.r.t paired images. It should be taken into account that PeleeNet for full-reference was shrinked, re-

Table 7.1 – Benchmark results. AUC and σ of the 100 test set iterations. Non-reference and Full-reference dataset settings above and below the middle lines separator, respectively, see section 3.5.

Algorithm	*SET1* (€+ ID)	*SET2* (€)
LBP [63]	0.778 ± 0.098	0.684 ± 0.042
HOG [66]	0.703 ± 0.012	0.731 ± 0.070
Haralick [105]	0.743 ± 0.014	0.598 ± 0.082
SIFT [147]	0.675 ± 0.077	0.623 ± 0.083
GLCM+YIQ [29]	0.729 ± 0.096	0.644 ± 0.066
PeleeNet [227]	$\mathbf{0.966 \pm 0.003}$	$\mathbf{0.851 \pm 0.003}$
Siamese	0.785 ± 0.023	0.721 ± 0.075
Triplets	0.635 ± 0.091	0.602 ± 0.088
CRC+Attn	$\mathbf{0.984 \pm 0.025}$	0.879 ± 0.071
CRC+Co-Attn	0.982 ± 0.024	$\mathbf{0.899 \pm 0.076}$

moving the final 2 stages [227], having less learnable parameters in comparison with the non-reference version. CRC+Co-Attn outperforms the rest in terms of generalization. We believe the proposed methods should generalize well to other different similarity tasks for the full-reference settings. We have performed the one-way Analysis of variance (ANOVA) with a significance level (α) of 0.05 to *SET1* and *SET2*, to determine whether there are any statistically differences between the binary PeleeNet classifier and the 2 CRC algorithms. Being 2 and 97 the degrees of freedom (DF), between and within individual samples, the result of the ANOVA is $F_{SET1}(2,97) = p \approx 0$, $F_{SET2}(2,97) = p \approx 0$. As $p < \alpha$ for both sets, we can reject the null hypothesis. Conversely, a paired t-test between CRC+Attn and CRC+Co-Attn and 99 DF draw p-values of 0.353 and 0.317 for *SET1* and *SET2*, respectively. Given such p-values the null hypothesis can not be rejected by any of the typical significance levels ($\alpha = 0.05$ or 0.1). In summary, the attention, or co-attention, mechanisms clearly outperform architectures without such mechanisms. Conversely, we still do not have enough statistical evidence to determine the superiority of co-attention models with regard to the attention models and further research has still to be done.

7.5 Conclusions and Future work

We have applied a recurrent comparator architecture with attention models to the counterfeit detection task to evaluate counterfeit documents through spotting the differences between a genuine and a reference image. We detect the differences by iteratively centering the attention in different positions of the security background textures searching for the lack of resolution due a *scanning-printing* operation. Reported results show that attention models improve the performance of architectures without such mechanisms. We also introduce a new dataset which seeks the generalization of a single learned model to detect counterfeits at unseen documents with very different security background designs. From the results obtained we think it is possible to apply this solution into a real industrial scenario. A future line of research is to reduce the size of the CNN models and to stop dynamically the number of glimpses needed during inference once the network has enough confidence to determine the patch similarity.

Outliers Part III

8 Outliers for counterfeit detection

Anomaly detection is an important problem within diverse research areas and application domains. We approach the detection of outliers in an unsupervised manner, creating a sphere manifold for each class and a hypersphere containing the inter and intra-variances of the different genuine classes. Whereas the outliers fall outside the global sphere. We demonstrate how generating adversarial samples fall close outside the hypersphere boundaries, meanwhile unseen objects, different from the training classes are cast far away from the center of the hypersphere manifold. The proposed model is trained end-to-end and outperforms state of the art models for the presented datasets[1].

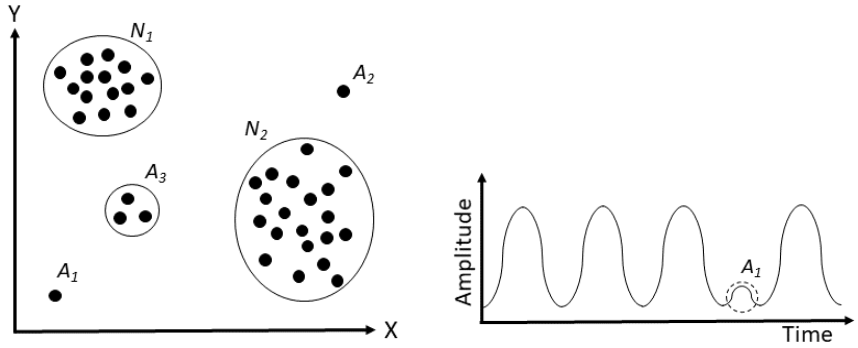
8.1 Introduction

Anomaly detection refers to the task of finding patterns in the data that do not conform to a well-defined notion of *normal*[2] behaviour [49]. Anomalies can be caused by errors in the data but sometimes are indicative of a new, previously unknown, underlying process. With the ever increasing amount of data being collected universally, it is of the utmost importance to detect these anomalies in a data-driven fashion. Anomalies events occurs relatively infrequently, but can have very significant consequences and it is mandatory discern if they represent a threat to the system.

Anomalies and outliers are the most popular terms in the literature for these irregular observations, however names such as novelty, exceptions and surprises can be found in different application domains. Novelty detection is the identification of this new or unobserved patterns in the data [155]. Not all unobserved patterns in the data are considered as anomalous data points. A novelty score can be assigned

[1] The code is publicly available at https://github.com/gitabcworld/DeepOneClassBanknote.git

[2] We use the word "normal" in layman's terms, not as a reference to the normal distribution in statistics.



(a) Point and collective anomaly example

(b) Contextual anomaly example

Figure 8.1 – Types of anomalies. Left illustration corresponds to the point and collective example in a two-dimensional space. Right figure represents a contextual anomaly in periodic signal over time.

to this new data and set a decision threshold to classify it as an anomaly or as a regular data for the model [172]. These points which significantly deviate from the decision threshold can be considered as anomalies.

Based on its composition and relation to the rest of the data, anomalies can be classified into the following three categories [20, 49]:

- Point pattern anomalies: If one data instance can be observed against other instances as anomaly. No structure is assumed among data instances. A_1 and A_2 are anomalies respect the point distributions N_1 and N_2, see Figure 8.1a.
- Contextual pattern anomalies: If the data instance is anomalous in some defined context, also known as conditional anomaly. In Figure 8.1b, a periodic context is present. Data instance A_1 is anomalous because it differs from the periodic context.
- Collective pattern anomalies: Individual data instances can not be anomalous in this case, only collection of related data anomalies. In Figure 8.1a, A_3 collection of data points are an anomaly respect N_1 and N_2 distributions, but are not anomalous between them.

Although on the abstract level detection of anomalies could seem a relatively simple task and it has been studied for many years. However this task is very challenging due several reasons, i.e. define the boundaries of the normal regions.

Normal data and anomalies can be very close to the margin of these boundaries and easily mistaken between them. Malicious actions, like fraud, it is considered an anomaly. Usually attackers try to adapt their actions to the normal behaviour, making anomaly identification a hard task. What is considered normal today can be not normal in the future, behaviour and business systems can change overtime. Most of the trained models for an specific anomality detection domain are ineffective in other fields, which makes the knowledge transfer specially difficult. Last but not least, due the nature of the infrequent behaviour of anomalities, training and validation data availability is a major issue. The difficulty of obtaining enough labeled data to characterize anomalies, causes that most anomality detection systems operates in an unsupervised setting, where only the normal data is used.

8.2 Deep Learning methods for anomaly detection

In Figure 8.2, a taxonomy based on the type of deep anomaly detection (DAD) models is presented [49]. From this chart, it does not even appear supervised anomaly detection methods. The supervised DAD requires both normal and anomalous data samples for training a binary or multi-class classifiers [44, 45]. This approaches assumes the availability of labeled instances from both normal and anomalous classes. Being this an unrealistic assumption due the lack of anomaly available data. This fact makes these deep learning-based methods less popular than the unsupervised ones.

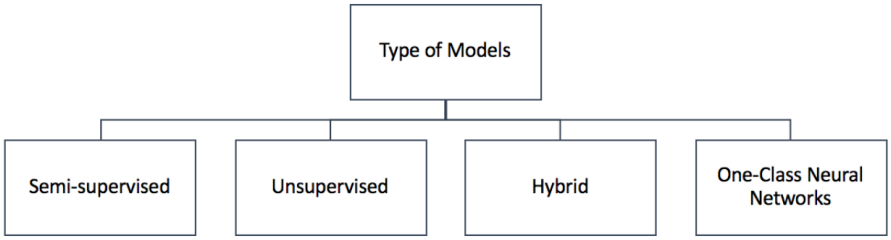


Figure 8.2 – Taxonomy based on the type of deep learning models for anomaly detection.

8.2.1 Semi-supervised methods

Semi-supervised DAD models are widely adopted thanks to the fact labels of normal instances are easier to obtain than anomaly labels. These techniques uses exist-

ing labels of single (usually genuine class) to separate outliers. Having sufficient training samples with no anomalies, is possible to train deep autoencoders. Deep autoencoders would produce low reconstruction errors for this normal instances, or normal class in the training data, over unusual events [156, 206].

8.2.2 Unsupervised methods

Unsupervised approaches detects anomalies only by intrinsic properties of data instances. Since labeled data is very hard to obtain, unsupervised DAD techniques can be used to automatically label these data. In domains such as cyber-security variants of unsupervised DAD models, like the one presented in [215], have outperformed traditional methods such as Isolation Forest [138, 139]. Isolation Forest is an outlier detection technique built on an ensemble of binary (isolation) trees. From the unsupervised methods, Autoencoders are the core of all unsupervised DAD techniques. These models assume a high prevalence of normal instances than abnormal data instances errors which may result in a high FPR.

8.2.3 Hybrid models

Deep learning-based hybrid models for DAD use deep neural networks, usually autoencoders as features extractors. The features learnt from the hidden layers of the autoencoders are the input to traditional anomaly detection algorithms such as one-class SVM (OC-SVM), explained in more detail in section 8.3. In [80] a variant of hybrid model trains jointly the feature extractor and the OC-SVM objective to maximize the detection performance. Hybrid approaches has a considerable drawback. These models usually fail to extract rich differential features to detect anomalies, due the lack of trainable objective functions customized for this objective.

8.2.4 One-Class Neural Networks

To solve the limitations of deep learning Hybrid models respect the lack of trainable objective functions for anomaly detection, One class neural networks (OC-NN) are introduced [46]. OC-NN methods are inspired by kernel-based one-class classification. It takes advantage of the progressively richer representation of the data and the one-class objective of enclosing tightly the normal data within a manifold. Here, the data representation in the hidden layer is driven by the OC-NN objective function, customized for anomaly detection. A variant of OC-NN architectures is the approach Deep Support Vector Data Description (Deep-SVDD) [183]. The authors propose to train a deep neural network to extract common factors of variation by closely mapping the normal data instances to the center of a hyper-sphere. We use

the idea by these authors, and extend a novel approach by considering multiple sub-spheres contained within the hyper-sphere. In the next section, we explain in detail how it is possible to go mathematically from a kernel-based one-class to a deep one-class classification approach.

8.3 From Kernel-based to Deep One-Class Classification

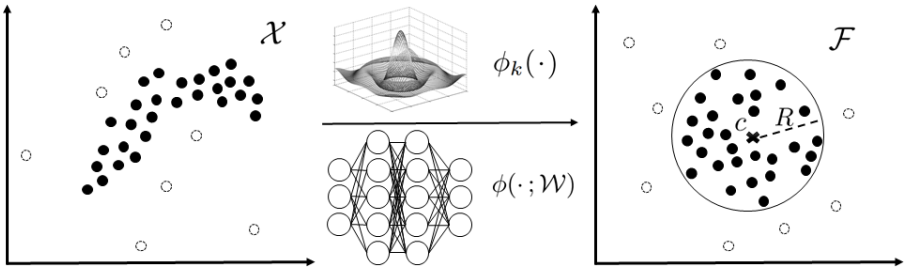


Figure 8.3 – Mapping from input space $\mathcal{X} \subseteq$ to output space $\mathcal{F} \subseteq \mathbb{R}^p$ to fit most of the data into the hypersphere with center c and radius R. The points falling outside the boundaries of boundaries of the sphere are considered anomalous. $\phi_k(\cdot)$ corresponds to a kernel based mapping and $\phi(\cdot, W)$ represents a neural network transformation with weights W.

Let $\mathcal{X} \subseteq \mathbb{R}^d$ be the data space. Let $k : \mathcal{X} \times \mathcal{X} \to [0, \infty]$ be a positive-definite kernel (PSD) [154], $\mathcal{F}_k$ it's associated Reproducing Kernel Hilbert Space (RKHS), in which point evaluation is a continuous linear functional, and $\phi_k : \mathcal{X} \to \mathcal{F}_k$ its associated feature mapping. Then $k(x, \hat{x}) = \langle \phi_k(x), \phi_k(\hat{x}) \rangle_{\mathcal{F}_k}$ for all $x, \hat{x} \in \mathcal{X}$ where $\langle \cdot, \cdot \rangle_{\mathcal{F}_k}$ is the dot product in Hilbert space $\mathcal{F}_k$ [18].

One-Class SVM (OC-SVM) is the most known algorithm for kernel-based method for one-class classification, the authors extended the SVM methodology to handle training using only positive information in [192]. Briefly, this methodology consists in transforming the feature via a kernel, treating the origin as the only member of the second class. Using "relaxation parameters" the authors separate the data of one class from the origin. Then standard techniques of two-class SVM are used. Framing the problem mathematically, the objective of OC-SVM is to find a maximum margin hyperplane in feature space, $w \in \mathcal{F}_k$, that divides best the origin from the projected data. Let $D_n = \{x_1, \ldots, x_n\}$ be training examples with $x_i \in \mathcal{X}$, then

OC-SVM solves the following quadratic programming problem

$$\min_{w,\rho,\varepsilon} \frac{1}{2}||w||^2_{\mathscr{F}_k} + \frac{1}{\nu n}\sum_{i=1}^{n}\varepsilon_i - \rho \tag{8.1}$$

subject to

$$\langle w, \phi_k(x_i)\rangle_{\mathscr{F}_k} \geq \rho - \varepsilon_i, \quad i = 1,2,\ldots,n \quad ,\varepsilon_i \geq 0 \tag{8.2}$$

where the relaxation parameters are represented by the non-negative slack variables $\varepsilon = (\varepsilon_1,\ldots,\varepsilon_n)^T$, which allows the margin to be soft, but violations ε_i get penalized. $||w||^2_{\mathscr{F}_k}$ is a regularizer on the hyperplane w where $||\cdot||_{F_k}$ is the norm induced by $\langle\cdot,\cdot\rangle_{\mathscr{F}_k}$. The hyperparameter ν controls the trade-off in the objective, allowing the incorporation of a prior probability into the model about the fraction of outliers present in the training data, also known as *ν-property* [192]. If w and ρ solve the problem, then the decision function

$$f(x) = \langle w, \phi_k(x)\rangle_{\mathscr{F}_k} - \rho \tag{8.3}$$

will be positive for most examples x_i contained in the training set, meanwhile the negative scores of $f(x)$ are considered anomalous.

The idea of splitting the hyperplane into two spaces, performed by OC-SVM characterises a dataset to fall into one of the two spaces divided by the hyperplane. Although this classification covers all training data, it is also including superflous space at each side of the hyperplane. Support Vector Data Description (SVDD), inspired by the Support Vector Classifier (SVC) and hence related to OC-SVM, obtains a hyper-sphere shaped boundary around a dataset and analogous to SVC it can be made flexible by using other kernel functions. The boundary of the spherical shaped boundary is used to detect novel data or outliers. The objective of SVDD is to find the smallest hypersphere with radius $R > 0$ and $c \in \mathscr{F}_k$ which encloses most of the data $\mathscr{X} \in \mathscr{F}_k$. The SVDD quadratic programming problem is given by

$$\min_{R,c,\varepsilon} R^2 + \frac{1}{\nu n}\sum_{i=1}^{n}\varepsilon_i \tag{8.4}$$

such that

$$||\phi_k(x_i) - c||^2_{\mathscr{F}_k} \leq R^2 + \varepsilon_i, \quad i = 1,2,\ldots,n \quad ,\varepsilon_i \geq 0 \tag{8.5}$$

Similarly to OC-SVD, the hyperparameter $\nu \in (0,1]$ add to the model the prior belief of the outlier distribution, controlling the trade-off between the penalties ε_i

and the hypershpere volume. Then, the decision function,

$$f(x) = ||\phi_k(x) - c||_{\mathscr{F}_k} - \rho \tag{8.6}$$

determines that the points projected oustide the hypersphere will be considered anomalous.

Both OC-SVM and SVDD has similar drawbacks. To be able to use any of this approaches, it is required to perform a explicit feature enginnering. Before using them, a previous step is required to train a model ϕ which maps data from $\mathscr{X} \rightarrow \mathscr{F}$. Another associated problem with kernel-based methods is its high computational cost associated with kernel matrices. The cost is at least quadratically in the number of training data points [193], unless some approximation is used for efficient kernel learning [199]. Finally but not least, kernel prediction requires the storage of support vectors which can demand large amounts of memory. Is it possible to overcome this drawbacks learning feature representations of the data together with the one-class classification objective [183], using a neural network which is jointly trained to map the data into a hypershpere of minimum volume. Let $\phi(\cdot, \mathscr{W}) : \mathscr{X} \rightarrow \mathscr{F}$ be a neural network with $L \in \mathbb{N}$ where W^l are the weights of layer $l \in 1, \ldots, L$. The authors propose the *soft-boundary Deep SVDD* objective as

$$\min_{R,W} R^2 + \frac{1}{\upsilon n} \sum_{i=1}^{n} max\{0, ||\phi(x_i; W) - c^2|| - R^2\} + \frac{\lambda}{2} \sum_{l=1}^{L} ||W^l||_F^2 \tag{8.7}$$

where they minimize the volume of the hypershere jointly with the network parameters W. Similarly to SVDD, the volume of the hypershere is reduced by R^2. The second term penalizes all data points from input space $\mathscr{X}^d \subseteq \mathbb{R}^d$ that fall outside sphere after projecting the point into the output space $\mathscr{F} \subseteq \mathbb{R}^p$, if its distance to the center $||\phi(x_i; W) - c||$ is greater than radius R. As in SVDD, $\upsilon \in (0, 1]$ controls the proportion of outliers which can violate the boundaries of the hypersphere. The last term acts a weight decay regularizer on the network parameters W with hyperparameter > 0, where $||\cdot||_{\mathscr{F}}$ denotes the Frobenius norm. Optimizing the objective from 8.4.1 allows the network weights W, to learn the common factors of the data to map normal examples close to the center c. Obtaining this compact description of the normal class also implies to map further away of the hypershpere the anomalous samples.

8.4 Multi Class Deep-SVDD

We have observed that the Deep-SVDD does not perform well with the banknote or identity background dataset problem. Each banknote or identity document

contains several zones with completely different textures. If we feed Deep-SVDD with the randomly crop background textures, the deep learning algorithm performs poorly. We hypothesize the reason for these behaviour is the high intra-variability of background textures within the same class of security document. The one-class Deep-SVDD approach when the normal samples within the manifold are complex make the algorithm to not converge to a satisfactory solution. We believe the patches within a same class should be related inside the hyper-sphere, pushing away other normal data which is from a different document class. Hence we propose a new loss function to model this behaviour.

8.4.1 Attraction and repulsion loss function

We adapt the *soft-boundary Deep SVDD* objective from [183]. We create a new loss function which contains three kinds different forces in the objective, see Figure 8.4. The optimization of this objective relies in the compromise between these three forces:

1. Attraction to c: All the sub-spheres will be attracted to the center of the global hypersphere.
2. Attraction of x to the center of the sub-spheres c_f. the intra-dependencies of each cluster learns common variations in the data.
3. Repulsion of the sub-spheres against each other. Each cluster center should be as far as possible of each of the other sub-spheres centers.

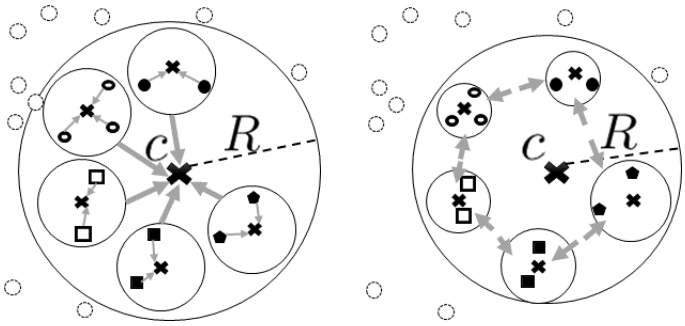
We model mathematically the objective loss function as

$$\begin{aligned}
&\min_{R,W} R^2 + \frac{1}{\nu n}\sum_{i=1}^{n} max\{0, ||\phi(x_i;W) - c_k^2|| - R^2\} \\
&+\frac{1}{nK}\sum_{i=1}^{n}\sum_{f=1}^{K}\sum_{g=f}^{K} max\{0, ||r_{if} + r_{ifg}||^2 - ||c_{if} - c_{ifg}||^2\} \\
&+max(0, \frac{1}{K}\sum_{f=1}^{K} ||r_f - R||^2) + \frac{\lambda}{2}\sum_{l=1}^{L} ||W^l||_F^2
\end{aligned} \tag{8.8}$$

such that

$$||\phi_k(x_i) - c||_{\mathscr{F}_k}^2 \leq R^2 + \varepsilon_i, \quad i = 1,2,\ldots,n \quad ,\varepsilon_i \geq 0, \quad k \in [0...K] \tag{8.9}$$

being K the number of classes, c_k, r_f the cluster centers and radius of the sub-spheres, R the radius of the hyper-sphere and n the number of samples in the dataset.



(a) Attraction force example (b) Repulsion force

Figure 8.4 – Attraction-Repulsion Loss function. The loss function we propose it is based in attraction and repulsion forces. The genuine objects from the same class will gravitate towards the center of its internal sub-sphere. At the same time is repulsed from other internal sub-spheres. Finally all the internal sub-spheres are attracted by the center of the general hyper-sphere. All the anomalies always fall outside the general hyper-sphere

8.5 Creating the anomaly detection dataset

To be able to compare any new proposed approach we need to create a baseline with classical anomaly detection approaches. We follow an hybrid model approach for the classical methods. First we extract the features with different models and then we apply different approaches for anomaly detection.

Research in anomaly detection suffers from a lack of realistic and publicly-available problem sets [79]. As we created our own banknote dataset, we over-sampled the counterfeit documents, making it unrealistic to the real scenario. Some statistics of the second configuration of the dataset, see section 3.5, are as follows: The IDs andbanknotes samples represent 3.1K and 11.5K respectively. The dataset is bias to contain € and IDs with a total of 9.7K samples. The counterfeits are only produced for the € bankotes and IDs with a total of 3.6K samples, representing a 37.7% for this set and a 25% of the total dataset. This percentage of counterfeits samples is much higher of what an anomaly detection problem expects. If we expect a normal distribution of data instances, we can define an outlier as any point that is outside the 5σ interval, which should encompass 99.5% of the data instances. Then around 0.5% of the data instances are expected to be be outliers. We follow the proposition in [79] to generate datasets that vary along three important dimensions:

(a) point difficulty, (b) relative frequency of anomalies, and (c) clusteredness.

(a) Computing point difficulty: we simulate an omniscient oracle by applying Logistic Regression (LR) to fit a conditional probability model $P(y|x)$ to the data [245]. Anomalies are labeled with $y = 0$ and normal instances as $y = 1$. For each candidate anomaly data instance we compute the logistic response. Instances easy to differentiate from the normal class will have responses $P(y = 1|x)$ close to 0, while points that LR confuses with the normal class will have responses above 0.5. In [79], they assign each anomalous instance to one of four difficulty categories:

- *easy* : Difficulty score $\in (0, 0.1\bar{6})$
- *medium* : Difficulty score $\in [0.1\bar{6}, 0.\bar{3})$
- *hard* : Difficulty score $\in [0.\bar{3}, 0.5)$
- *very hard* : Difficulty score $\in [0.5, 1)$

(b) Relative frequency: corresponds with the percentage of anomaly data instances in the dataset. Some typical relative frequencies range from 0.1% to 10% of outliers, being $[0.001, 0.005, 0.01, 0.05, 0.1]$ the common values selected.

(c) Clusteredness: given a set of candidate anomalous data samples, the authors in [79] generate sets of desired size, that are either widely disperse or tightly clustered. The desired size of K anomalous instances will be determined by the relative frequency. We differ from the authors in how we create these sets. We create three different sets: a random set, a disperse anomaly set and a tightly anomaly clustered set. The random set consists of randomly sampling K anomalous samples. To generate K disperse samples, we use the Farthest Point Sampling (FPS), to chose a subset of data anomalous samples $s_1, s_2, \ldots, s_K$, such that the selected random anomalous data point s_0 is the most distant point from the $s_1, s_2, \ldots, s_K$. FPS has better coverage than random sampling given the number of centroids. The tightly clustered anomaly dataset, is generated by selecting a seed point at random and then compute the $K-1$ data samples that are closest to it in Euclidean distance. We use K-Nearest Neighbors (k-NN) algorithm to select these closest instances. Once the anomaly samples have been selected then they are joined with the normal data instances. The normalized clusteredness is then defined as ratio of the sample variance of the normal samples to the sample variance of K selected anomalous samples. When the clusteredness is less than 1, the anomalous samples exhibit greater semantic variance than the normal points. When clusteredness is greater than 1, the anomalous samples are more tightly clustered

than the normal samples (on average). In [79] the authors group the clusteredness scores into six qualitative levels: *high scatter* $(0, 0.25)$, *medium scatter* $(0.25, 0.5)$, *low scatter* $(0.5, 1)$, *low clusteredness* $(1, 2)$, *medium clusteredness* $(2, 4)$, and *high clusteredness* $(4, \infty)$.

8.6 Experimental Set-up and Results

The experimental set-up and results of this sections are done using the third configuration of the dataset from section 3.5. We follow an hybrid approach to detect anomalies, which is why we first extract hand-crafted and learnt features descriptors. Later these features descriptors are used for anomaly detection.

To make a complete study we extract hand-crafted texture features, keypoint features and learnt feature descriptors. We have reused some of the features descriptors that have been used along the previous chapters. The hand-crafted texture descriptors we use in this section are: Luminance histogram, Bhavani [28], Haralick [105] and HOG [66]. We select as keypoint feature descriptors: SIFT [147], SURF [24], BRIEF [39] and ORB [182]. BRIEF stands for Binary Robust Independent Elementary Features and as its name indicates uses binary strings as an efficient feature point descriptor. Their authors claims that yields similar or better results than SURF and with the advantage of being much faster. Oriented FAST and Rotated BRIEF (ORB) was developed as an efficient and viable alternative to SIFT and SURF, using FAST as keypoint detector and the BRIEF descriptor. Finally for the learnt features, we use known convolutional neural networks architectures: MobileNet v2 [189], Resnext [239], ShuffleNet v2 [149], Inception v3 [209] and PeleeNet [227].

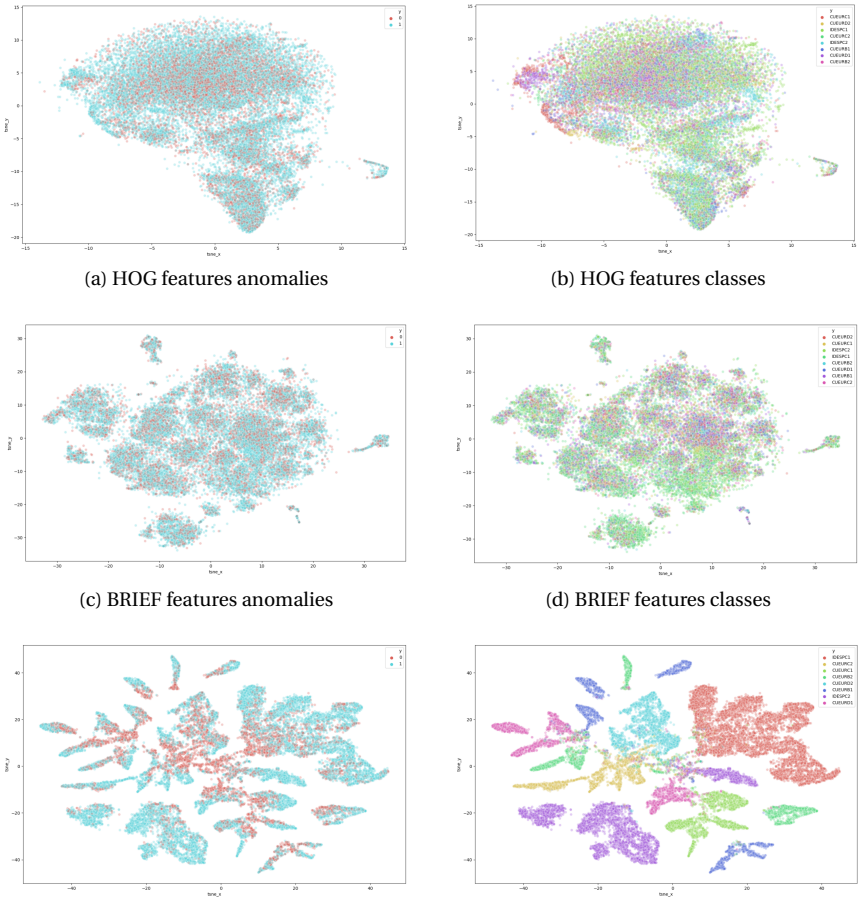
We select five different classifiers to calculate the point difficulty: LR, LR Smote (LRSmote), Multi-layer Perceptron (MLP) regressor [111], Random Forest (RF) regressor [34] and a XGBoost (XGBoost) [53] regressor. Smote is a technique similar to upsampling and it uses nearest neighbors algorithms to generate new synthetic data. It is usually used for dealing with imbalanced datasets. MLP regressor is a neural network model that trains using backpropagation with no activation function in the output layer. It may also be seen like using the identity function as activation function. Hence, MLP regressor uses the square error as the loss function, and the output is a set of continuous values. A RF regressor are an ensemble learning methods for regression, which fits a number of classifying decision trees on various sub-samples of the dataset and uses averaging to improve the predictive accuracy and control over-fitting. XGBoost regressor is a decision-tree-based ensemble machine learning algorithm, that uses a gradient boosting framework and is designed for speed and performance.

Finally we use different types of state-of-art algorithms for anomaly detection:

Isolation Forest (IF), which is an outlier ensemble. The proximity-based anomaly detector Local Outlier Factor (LOF) [35]. A fully connected neural network Autoencoder [13], which uses the reconstruction error as the outlier score. We also include a Single-Objective Generative Adversarial Active Learning (SO_GAAL) [141], which directly generate informative potential outliers based on the mini-max game between a generator and a discriminator.

When training the keypoint features we train a Gaussian Mixture Model (GMM) and Fisher Vectors (FV) as done in Chapter 5 to extract a single feature vector. We set the number of clusters for the GMM to 256. To reduce memory requirements, we reduce the dimensionality of the resulting FV, by performing a PCA with 256 components. During all this process of keypoint feature learning we only use the normal data instances. We also only use the normal data instance to learn all the learn features using convolutional networks architectures. We set the learning as a supervised problem where each security document is a different class, being the anverse and reverse of the document different classes. We select random patches within each class to learn the background security textures. In Figure 8.5 we can see how the learnt features outperform the keypoint and the hand-crafted features. Visualizing it as a 2D T-SNE representation [150].

For our experiments we had to limit the huge amount of combinations it can result from the different types of point difficulties, the relative frequencies and clusteredness. We restrict the combinations to a single set of parameters, being the relative frequency set to 0.10, the computing point difficulty to *medium* and the clusteredness to *medium scatter*. All these settings are set as overall to medium difficulty. In Table 8.1 we can see the results ordered by hand-crafted, keypoint and learnt feature descriptors. We also set the relative frequency to 0.10, the classifier to point difficulty using MLP regressor and the outlier detector to IF. We can see that as expected the algorithm approaches which work with general texture descriptors does not manage to perform well, with exception of HOG for the Set1, as we saw in Chapter 6. Keypoint descriptors perform better than the texture algorithms, however their performance is worse than the convolutional neural network approaches. Finally, the neural network approaches can initially cluster better the features of each class, later IF has a clear decision on how it can divide the anomalies from the genuine samples. The performance of the learnt approaches is similar, being Resnext the one with better performance, which we believe is because its higher learning capacity in terms of number of learning parameters.



(a) HOG features anomalies

(b) HOG features classes

(c) BRIEF features anomalies

(d) BRIEF features classes

(e) Resnext features anomalies

(f) Resnext features classes

Figure 8.5 – T-SNE 2D representation of the learnt features of HOG, BRIEF and Resnext feature descriptors. The left column, contains the anomaly point representation. Being the blue points the normal data and the red points the anomalies. On the right column we can see how the features represents each ones of the classes present in the Set1 from the third configuration of the dataset 3.5.

Table 8.1 – Benchmark results for anomaly detection. AUC and σ of the 10 test set iterations. , see section 3.5 for dataset information.

Algorithm	*SET1* (€+ ID)	*SET2* (€)
Luminance histogram [243]	0.524 ± 0.016	0.510 ± 0.098
Bhavani [29]	0.611 ± 0.550	0.585 ± 0.033
Haralick [105]	0.658 ± 0.084	0.608 ± 0.022
HOG [66]	0.751 ± 0.052	0.701 ± 0.170
SIFT [147]	0.696 ± 0.088	0.637 ± 0.053
SURF [24]	0.655 ± 0.099	0.623 ± 0.106
BRIEF [39]	0.695 ± 0.157	0.634 ± 0.021
ORB [182]	0.726 ± 0.093	0.685 ± 0.013
Mobilenet v2 [189]	0.826 ± 0.013	0.795 ± 0.067
Resnext [239]	0.869 ± 0.003	0.834 ± 0.055
ShuffleNet v2 [149]	0.834 ± 0.043	0.780 ± 0.093
Inception v3 [209]	0.860 ± 0.068	0.813 ± 0.016
PeleeNet [227]	0.806 ± 0.011	0.780 ± 0.066

8.7 Conclusions and Future work

We transform the detection of background counterfeit in security document to an anomaly detection problem. We extract some results of how it does perform the created dataset with state-of-art algorithms. We also propose a novel approach, based in the Deep-SVDD algorithm to use the repulsion and attraction forces within the sub-spheres wrapped in the hyper-sphere. We intend to learn the intra-variabilities produced between the texture regions of the same class of security document. We also propose a new way to create subsets of the dataset in terms of: *point difficulty*, *relative frequency* and *clusteredness*. The subsets created transforms the created dataset to an anomaly dataset.

As a future line of research we need to do a more complete evaluation of all the combinations of possible subsets, feature descriptors and anomaly detectors. Finally, we have to compare Deep-SVDD and the proposed novel approach with the baseline of state-of-art anomaly detectors.

Clausula Part IV

9 Closing remarks

In this chapter we summarize all the contributions this thesis brings for the research community. First we introduce the main conclusions we can extract for each one of the chapters we present through the thesis. Ending the conclusions we present what we have learnt bringing together all the pieces of this thesis. We already introduce at each end of the chapters a future work that could be done at each one of this pieces. The future work at this section, collects all these thoughts and explains them together with a more general view. These view intends to help future researchers, who will work in counterfeit document detection, selecting a better path with the prior information contained in this thesis. Later we present a summary of the contributions. Afterwards the scientific articles published during this thesis, the contribute code and contributed datasets. Lastly the courses done inside this industrial PhD and the assistance to conferences and courses.

9.1 Conclusions

In this PhD dissertation we have addressed the problem of forensic analysis of background textures in banknotes and identity documents for counterfeit detection. The application scenarios are the services or products that require a genuine identification of highly secured documents where a smartphone is available, in a non-controlled environment for document acquisition and without the need of specialized equipment like UV or IR lamps.

The analysis must be done using only a single image coming from the mobile phone camera and the full document must present in the image. Being these restrictions initially conditions within the frame of this industrial thesis. These restrictions poses two main problems; first, a non-controlled environment causes image noise distortions such as the ambient illumination of the scene, or perspective distortions caused by the non-rigid surfaces of banknotes and occluding parts, due some security documents images are being acquired with the user holding the documents with his hand. The second is that images are analyzed with much lower

resolution than in a forensic laboratory. Mobile devices are not able to provide the same resolutions of image acquisition as for instance a microscope. Moreover, as the full documents needs to be present and acquired in a single frame, we can not move closer the smartphone to the inspected surface, increasing the effective working resolution in a certain area. The aim is to develop new machine learning approaches, conditioned by the previous restrictions, which will help expert and amateur forensic examiners to detect counterfeit background textures in security documents. Here we take the opportunity to summarize the findings of this work. Although, we already introduce at each chapter ending a specific future work, this section provides a general view of the trajectory of this thesis combining all of them.

When searching for previous solutions for the posed problem, we found that the previous state-of-art in security features for security documents was lacking in many topics, not showing the level of completeness required for an inexpert reader in the area. That is why we present our own survey, focusing in the anti-counterfeit security measures which can be solved automatically by computer vision algorithms. The survey is presented as the related work of this thesis in Chapter 2. We add sections which were not usually treated at other surveys, such as history, effects of forgery in society or document experts, with the objective that readers without the previous knowledge in counterfeit detection understand the basics and difficulties of this field. The explanation of the anti-counterfeits measures, what they are and how it is possible to detect them, were also scattered through all previous literature. We join most of the anti-counterfeit features based in three categories: The security substrates, the security inks and the security printings. With this categories we cover all the stages of production of a security document. Nowadays the research of algorithms for detect tampering is more needed than ever. That is why we also cover digital tampering as an important topic, compared with the non-existence of it in most of the previous surveys. Ultimately we discuss some of the compared algorithms and the pros and cons of applying them for future research. We believe one of the main purposes of these algorithms is to provide a wide range of population a set of tools to check for counterfeits in an accessible, affordable and comprehensible fashion.

In the first part of this dissertation we first focus on creating the dataset which defines the type of counterfeit we want to solve. Here we found one of the main drawbacks for comparing anti-counterfeit algorithms. There is no public available datasets for counterfeit detection in IDs and banknotes. This leads to every researcher to build their own private datasets where it will extract some results that in most cases nobody would be able to reproduce. Also the difficulty of create these datasets to gather both genuine and counterfeit samples, makes that each private dataset contain generally few samples. We create a public available couterfeit datasets for banknotes in Chapter 3, keeping in mind the restrictions

of this industrial thesis we previously mentioned. The counterfeits are generated through the *scan-printing* procedure. Initially we were only focus in identity documents, however we found difficult to gather samples due privacy issues. Then we made the observation that the majority of the security features presented in identity documents, were first designed for banknotes, so we built a banknote dataset instead.

Afterwards we focus in detecting the counterfeits using hand-crafted texture algorithms, treating the problem as a sparse representation problem in Chapter 4. Applying dictionaries and sparse representations yields to a very good performance in counterfeit classification for the proposed benchmark improving the state of the art algorithms. Approaches like, K-SVD and SCSPM, have proven of being capable of covering most of the camera-based uncontrolled environmental acquisition problems. Later we want to translate this study of the previous approaches to a proof of concept for an industrial application to detect ID counterfeit documents. We present an end-to-end system that covers from the smartphone client acquisition to the evaluation of the document and final response to the client in Chapter 5. Along the way we also build a database of security documents and the whole architecture schema is thought to be modular and scalable. Generating individual models for each ROI allows to introduce new documents to the system without the requirement of retraining previous models. The application can be easily extended to support banknote counterfeit detection due the strong correlation with ID background textures.

In the second part of this dissertation we focus in studying which texture features are better suited for the background texture counterfeit detection. Furthermore, we are also interested in proving if the results are statistically relevant and if they generalize to unseen background textures. We have statistically evaluated the state-of-the-art descriptors for texture description in security documents in Chapter 6. We have divided the datasets in two groups by their different challenging conditions to evaluate the presented algorithms. Hand-crafted feature descriptors are outperformed nowadays by CNN based descriptors. However we have seen that several texture hand-crafted descriptors performance does not differ from the CNN descriptors and should not be discarded a priori. HOG features are the more suitable descriptors if we take into account the memory and computation time limitations ratio present in an industrial application for both datasets. CNN fine-tunning usually outperforms an existing, pretrained CNN for an specific dataset because it progressively concentrates into the details of the new data classes characteristics. However a drawback to this knowledge transfer, in our case, is the unbalanced dataset that we dispose to further training, because naturally we will always have a lack of counterfeit samples. Another drawback is that, if we fine-tune a specific CNN for each ROI is not possible to maintain a memory-scalable system and if we

train a single CNN model for all ROIs, then we would have to retrain for each new ROI.

Inside this second part, we also ask ourselves if the regions of the background we have been selecting are the correct ones. Until this point, all the images we were using for training and testing were manually selected in background regions we believe are relevant, like Guilloches, Intaglio or Vignettes. Here it raises the question, can we find automatically where to center the attention at each patch? To that end, we have applied a recurrent comparator architecture with attention models to the counterfeit detection task to evaluate counterfeit documents through spotting the differences between a genuine and a reference image in Chapter 7. We detect the differences by iteratively centering the attention in different positions of the security background textures searching for the lack of resolution due a *scanning-printing* operation. Reported results show that attention models improve the performance of architectures without such mechanisms. The patches are selected randomly at any position in the background. This random selection, proves the generalization of the algorithm. However, we believe it is possible to create in a future approach a more intelligent and automatic way to study which zones are better suited for the background texture analysis.

In the third part of this thesis we pose the problem as an anomaly detection. Counterfeit samples are hard to gather resulting in unbalanced datasets. The lack of counterfeit samples motivates the creation of models which can represent a robust manifold of the non-anomalous data. Any anomalous data falling outside of this manifold can be considered as a counterfeit sample. In Chapter 8 we present a novel algorithm for anomaly detection adapting a previous approach for one-class (D-SVDD), to multi-class. Using attraction and repulsion forces inside the hyper-sphere, we create class related sub-spheres. These data within the sub-spheres have intra and inter relations with the other classes. Attracting similar samples from the same class to the center of its sub-sphere and repelling the other classes. Without the sub-spheres we found that the anomality model is not able to deal with all the variability of background textures within the same denomination of banknote. Forcing the model to create clusters within the hyper-sphere improves the performance for the counterfeit background analysis. We also add an extensive testing of state-of-art approaches as a baseline to compare the proposed approach.

We think that it may not exist a single visible deterrent feature which is readily recognizable, highly durable, difficult to counterfeit or simulate, costly affordable, and easy to produce. A best strategy is to select a combination of features, which adds complexity to the counterfeiter's task and increase the number of counterfeiting steps to the point that the casual counterfeiter would eventually "give up". The analysis of background texture, should not be the unique security feature and needs to be combined with other deterrents to detect counterfeit in security documents.

The approaches presented to discover counterfeit documents using the background texture represents another stone in the path of a counterfeiter, that they must sort. For this reason we believe that the proposed approaches would have an important impact on the practical deployment of anti-counterfeit systems.

9.2 Future Work

This section takes the opportunity to summarize all the future work that can be done to improve the presented thesis in several areas. These improvements also represent key insights to further advance the knowledge in the analysis of background textures for counterfeit detection in security documents. At each chapter a specific future work is presented, here we combine them and present new ideas.

The main drawback of this thesis has been the restrictions imposed by the company inside the frame of this industrial thesis. The fact that we only process single images coming from the smartphone, discards most of the anti-counterfeit measures which are highly dependent upon viewing angle hence having availability of different frames, such as OVD or OVI security features. The second restriction of having the full image of the security document acquired with a single image, made not possible to move closer the camera to background texture increasing the working resolution, like the authors in [145].

Both restrictions are affecting directly the final working resolution to analyze the textures. The ideal approach would be having the microscopic resolution as forensics experts have in their laboratories. Nowadays this level of resolution is impossible with the current technology of smartphone cameras. However there are techniques to move closer to that objective. If video frames can be used, a multiframe super-resolution algorithm that creates a complete RGB image directly from a burst of CFA raw images [236]. They build a super-resolution zoom feature able to runs at 100 milliseconds per 12-megapixel RAW input burst frame on mass-produced mobile phones. This level of resolution would make checking microtext much more robust as with our approach. Other algorithms achieve super-resolution with only a single image, directly learn an end-to-end mapping between the low-resolution image as the input and outputs the high-resolution one [73, 126, 249]. Although this fits our approach, even with our current restrictions, the models to output high resolution images are learnt with natural images, and not with the designs present in the banknotes or IDs. We want to preserve the structure of the fine-line patterns when converting to high resolution images to find counterfeit alteration clues. As a future line of work, this approaches should be retrained with security backgrounds and test its feasibility.

To be able to retrain any model, collecting the dataset will continue to be an

issue. Further study should be done in how it could be possible to create these datasets, without infrincting PII and copyright issues, to share for the research community and create a baseline of results. In this work, we focus only in identity and banknotes. Both share similar anti-counterfeiting security features. A future line of work, would be doing the same analysis of tamper-evident labels, cheques, product authentication, stock certificates, postage stamps, etc. Then compare which of these objects has similar security features and which ones has easier available datasets. The objective would be two-fold. First study to possibility of using security detection algorithms of one object to the other. Second study if its possible to transfer knowledge between models trained in one printing security object dataset to the other.

The proposed idea of using sparse dictionary learning, to find a sparse representation of the input data has proven to be efficient with the counterfeit samples generated with one printer, further research should be done with different inkjet and laser printers during the scan-printing procedure. Also, further study should be done to test which are the minimum counterfeits samples required to train a classifier to maintain an acceptable rating of forgery detections. However from the statistical evaluation of different texture descriptors in Chapter 6, learnt features with CNNs can outperform dictionary approaches due its higher capacity. We also reason during that statistical evaluation, that a single model should be created which could differentiate the introduction of artifacts between genuine and counterfeit textures. Regardless of which type of document or texture we are dealing with.

The recurrent comparator model solves the need of creating a unique model for all the textures. A future line of research is to reduce the size of the CNN models with the aim to do the classification on-device. Another improvement is to stop dynamically the number of glimpses needed during inference once the network has enough confidence to determine the patch similarity. Right now the number of glimpses is fixed, if the model has enough confidence at one intermediate glimpse, there is no motive to continue doing the rest of the glimpses. Reduced computational time is important for an industrial scenario. Further studies should be conducted to create a loss function which rewards early stopping. Furthermore we conducted experiments to improve learning time of the recurrent comparator model, skipping updates in the recurrent neural network [40]. However we did not achieve the same results as with the complete updates, more research should be conducted in this topic.

We presented a SoA architecture to transfer all these ideas to a proof of concept. The main component to improve is the mobile application. By far, is the element in the pipeline which consumes more time. One possible extension is the integration of detection and identification in the mobile application in a single step. This could

be done with the recent CNN architecture presented in YOLO V2 [179]. Using a joined identification and detection would facilitate the user experience and would be able to send the dewarped image once the minimum required resolution is achieved.

Finally from an academic point of view, anomaly detection have matured in a short period of time. As presented in this thesis, new models are showing very promising generalization capabilities and accurate results, when exposed to new unseen data [141, 187, 251].

These, among many others, are the current open problems in background security counterfeit detection. We hope that this summary and discussion could serve to motivate researcher to take some of these challenges, with the final goal of bringing counterfeit detection a step closer.

9.3 Contributions

In this PhD dissertation we have made both practical and theoretical contributions to background texture forensic analysis in banknotes and identity documents. In the scope of introducing the problem of counterfeit detection we contribute to the research community with:

- A survey in anti-counterfeit security measures present in identity documents and banknotes.
- A public dataset for banknote counterfeit detection.

Previous to this work, there was few literature related with background security approaches for counterfeit detection. We further expand the knowledge in this area by:

- Relate the background printing as a sparse representation problem.
- Evaluate BoW, K-SVD and ScSPM against state-of-art using the banknote dataset.
- Statistical evaluation of texture descriptors and state-of-art CNNs with the baknote and identity document dataset.
- Pose the background counterfeit analysis as a full-reference game of spotting the differences. A recurrent comparator network is proposed to this end.

Datasets of counterfeit detection usually contains much more genuine samples than counterfeit data. With the aim of solving the problem of unbalanced data within the datasets, we contribute by:

- Compare and evaluate state-of-art algorithms in anomaly detection with the current dataset.
- Propose a novel multi-class anomaly detection model based on sub-spheres within a hyper-sphere.

Finally, within the industrial frame of this dissertation, we contribute with a framework that can help future researchers to deploy and test their applications with:

- We build a service-oriented architecture to detect counterfeit documents. The mobile-server framework can be used for any other purpose.

We hope our contributions will help the research community to keep on advancing in the problem background counterfeit detection. Moreover the ideas proposed within this thesis can also be applied to other problems and can be used as general purpose approaches.

9.4 Scientific Articles

This dissertation has led to the following communications:

9.4.1 Submitted Journals

- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. "Identity document and banknote security forensics: a survey." 2019. Submitted to Pattern Recognition.

9.4.2 International Conferences and Workshops

- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. Banknote counterfeit detection through background texture printing analysis. In 2016 12th IAPR Workshop on Document Analysis Systems (DAS), pages 66–71, April 2016.
- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. "E-Counterfeit: A Mobile-Server Platform for Document Counterfeit Detection," 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR), Kyoto, 2017, pp. 15-20.
- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. "Evaluation of Texture Descriptors for Validation of Counterfeit Documents."

2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR). Vol. 1. IEEE, 2017.

- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. "Recurrent Comparator with attention models to detect counterfeit documents." 2019 15th IAPR International Conference on Document Analysis and Recognition (ICDAR). IEEE, 2019.

9.4.3 Local Conferences and Workshops

- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. Document Identity Fraud Detection using Mobile Images. 11th CVC Workshop on Computer Vision Trends and Challenges CVCR&RD. Computer Vision Center. 2015.

- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. Document counterfeit detection through background texture printing analysis. 12th CVC Workshop on Computer Vision Trends and Challenges CVCR&RD. Computer Vision Center. 2016.

- **Albert Berenguel**, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. Document counterfeit detection through background texture printing analysis. 13th CVC Workshop on Computer Vision Trends and Challenges CVCR&RD. Computer Vision Center. 2017.

9.5 Contributed Code and Datasets

- Banknote dataset for counterfeit analysis. See chapter 3 for further information.

- SoA framework for counterfeit detection. See chapter 5. https://github.com/gitabcworld/e-Counterfeit.

- Code for Recurrent Comparator for counterfeit detection, see chapter 7. https://github.com/gitabcworld/ConvArc

- Matching Networks for One Shot Learning [224]. Re-implementation of the original paper to Pytorch code. https://github.com/gitabcworld/MatchingNetworks

- Optimization as a Model for Few-Shot Learning [178]. Re-implementation of the original paper to Pytorch code. https://github.com/gitabcworld/FewShotLearning

- Skip RNN: Learning to Skip State Updates in Recurrent Neural Networks [40]. Re-implementation of the original paper to Pytorch code. https://github.com/gitabcworld/skiprnn_pytorch
- Code for Multi-sphere Deep-SVDD for anomality detection, see chapter 8. https://github.com/gitabcworld/DeepOneClassBanknote.

Bibliography

[1] Bloomberg.

[2] Gemalto passport security design.

[3] Pyvttbl library.

[4] Wikihow.

[5] *History of Forgery*, pages 47–54. Humana Press, Totowa, NJ, 2007.

[6] Counterfeiters are using ai and machine learning to make better fakes, 2017.

[7] Kinde anti-counterfeiting labels, *Guangdong Zhengdi (Kinde) Network Technology Co., Ltd.*, 2019.

[8] Penalties by country for creating counterfeit money, 2019.

[9] Product overview on bubbletag, ramdot, fibertag, *Prooftag SAS*, 2019.

[10] Superdollar, 2019.

[11] Svetlana Abramova et al. Detecting copy–move forgeries in scanned text documents. *Electronic Imaging*, 2016(8):1–9, 2016.

[12] Acuity. The global national eid industry report: 2017 edition, 2019.

[13] Charu C Aggarwal. Outlier analysis. In *Data mining*, pages 237–263. Springer, 2015.

[14] Michal Aharon, Michael Elad, and Alfred Bruckstein. rmk-svd: An algorithm for designing overcomplete dictionaries for sparse representation. *IEEE Transactions on signal processing*, 54(11):4311–4322, 2006.

[15] Michal Aharon, Michael Elad, and Alfred Bruckstein. K-svd: An algorithm for designing overcomplete dictionaries for sparse representation. *Signal Processing, IEEE Transactions on*, 54(11):4311–4322, 2006.

[16] Amr Gamal Hamed Ahmed and Faisal Shafait. Forgery detection based on intrinsic document contents. In *2014 11th IAPR International Workshop on Document Analysis Systems*, pages 252–256. IEEE, 2014.

[17] Mohammad H Alshayeji, Mohammad Al-Rousan, and Dunya T Hassoun. Detection method for counterfeit currency based on bit-plane slicing technique. *International Journal of Multimedia and Ubiquitous Engineering*, 10(11):225–242, 2015.

[18] Nachman Aronszajn. Theory of reproducing kernels. *Transactions of the American mathematical society*, 68(3):337–404, 1950.

[19] Meika Ball. Reserve bank of australia. recent trends in banknote counterfeiting, 2019.

[20] Arindam Banerjee, Varun Chandola, Vipin Kumar, Jaideep Srivastava, and Aleksandar Lazarevic. Anomaly detection: A tutorial. In *Tutorial SIAM Conf. on Data Mining*, 2008.

[21] European Central Bank. Biannual information on euro banknote counterfeiting, 2015.

[22] Jawadul H Bappy, Amit K Roy-Chowdhury, Jason Bunk, Lakshmanan Nataraj, and BS Manjunath. Exploiting spatial structure for localizing manipulated image regions. In *Proceedings of the IEEE international conference on computer vision*, pages 4970–4979, 2017.

[23] Charles T. Barlow. The roman government and the roman economy, 92-80 b.c. *The American Journal of Philology*, 101(2):202–219, 1980.

[24] Herbert Bay, Tinne Tuytelaars, and Luc Van Gool. Surf: Speeded up robust features. In *ECCV*. Springer, 2006.

[25] Albert Berenguel, Oriol Ramos Terrades, Josep Lladós, and Cristina Cañero. Banknote counterfeit detection through background texture printing analysis. In *DAS*. IEEE, 2016.

[26] Romain Bertrand, Petra Gomez-Krämer, Oriol Ramos Terrades, Patrick Franco, and Jean-Marc Ogier. A system based on intrinsic features for fraudulent document detection. In *2013 12th International Conference on Document Analysis and Recognition*, pages 106–110. IEEE, 2013.

[27] Romain Bertrand, Oriol Ramos Terrades, Petra Gomez-Krämer, Patrick Franco, and Jean-Marc Ogier. A conditional random field model for font forgery detection. In *2015 13th International Conference on Document Analysis and Recognition (ICDAR)*, pages 576–580. IEEE, 2015.

[28] R Bhavani and A Karthikeyan. A novel method for counterfeit banknote detection. *International Journal of Computer Sciences and Engineering*, 02(4):165–167, Apr 2014.

[29] R Bhavani and A Karthikeyan. A novel method for counterfeit banknote detection. *Int. J. Comput. Sci. Eng*, 2014.

[30] Howard Bodenhorn. Moneymakers: The wicked lives and surprising adventures of three notorious counterfeiters by ben tarnoff. *The Business History Review*, 86:156–158, 01 2012.

[31] Luca Bondi, Silvia Lameri, David Güera, Paolo Bestagini, Edward J Delp, and Stefano Tubaro. Tampering detection and localization through clustering of camera-based cnn features. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1855–1864. IEEE, 2017.

[32] Peter Bower. Operation bernhard: The german forgery of british paper currency in world war ii. In *The Exeter Papers. London: The British Association of Paper Historians*, pages 43–65, 2001.

[33] Yuri Boykov and Gareth Funka-Lea. Graph cuts and efficient nd image segmentation. *IJCV*, 2006.

[34] Leo Breiman. Random forests. *Machine learning*, 45(1):5–32, 2001.

[35] Markus M Breunig, Hans-Peter Kriegel, Raymond T Ng, and Jörg Sander. Lof: identifying density-based local outliers. In *ACM sigmod record*, volume 29, pages 93–104. ACM, 2000.

[36] Jane Bromley, Isabelle Guyon, Yann LeCun, Eduard Säckinger, and Roopak Shah. Signature verification using a" siamese" time delay neural network. In *Adv Neural Inf Process Syst*, 1994.

[37] Arcangelo Bruna, Giovanni Maria Farinella, Giuseppe Claudio Guarnera, and Sebastiano Battiato. Forgery detection and value identification of euro banknotes. *Sensors*, 13(2):2515–2529, 2013.

[38] James DR Buchanan, Russell P Cowburn, Ana-Vanessa Jausovec, Dorothee Petit, Peter Seem, Gang Xiong, Del Atkinson, Kate Fenton, Dan A Allwood, and Matthew T Bryan. Forgery:'fingerprinting'documents and packaging. *Nature*, 436(7050):475, 2005.

[39] Michael Calonder, Vincent Lepetit, Christoph Strecha, and Pascal Fua. Brief: Binary robust independent elementary features. In *European conference on computer vision*, pages 778–792. Springer, 2010.

[40] Victor Campos, Brendan Jou, Xavier Giró i Nieto, Jordi Torres, and Shih-Fu Chang. Skip RNN: learning to skip state updates in recurrent neural networks. *CoRR*, abs/1708.06834, 2017.

[41] Seung-Hoon Chae, Jong Kwang Kim, and Sung Bum Pan. A study on the korean banknote recognition using rgb and uv information. In *International Conference on Future Generation Communication and Networking*, pages 477–484. Springer, 2009.

[42] Sujoy Chakraborty and Matthias Kirchner. Prnu-based image manipulation localization with discriminative random fields. *Electronic Imaging*, 2017(7):113–120, 2017.

[43] Trisha Chakraborty, Nikita Nalawade, Abhishri Manjre, Akansha Sarawgi, and Pranali P Chaudhari. Review of various image processing techniques for currency note authentication. *Int. J. Comput. Eng. Res. Trends*, 3(3):119–122, 2016.

[44] Raghavendra Chalapathy, Ehsan Borzeshi, and Massimo Piccardi. An investigation of recurrent neural architectures for drug name recognition. pages 1–5, 01 2016a.

[45] Raghavendra Chalapathy, Ehsan Borzeshi, and Massimo Piccardi. Bidirectional lstm-crf for clinical concept extraction. 11 2016b.

[46] Raghavendra Chalapathy, Aditya Krishna Menon, and Sanjay Chawla. Anomaly detection using one-class neural networks. 02 2018.

[47] J. Chambers, W. Yan, A. Garhwal, and M. Kankanhalli. Currency security and forensics: a survey. *Multimedia Tools and Applications*, 74(11):4013–4043, 2015.

[48] Jarrett Chambers, W Yan, A Garhwal, and M Kankanhalli. Currency security and forensics: a survey. *Multimedia Tools and Applications*, 74(11):4013–4043, 2015.

[49] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. *ACM computing surveys (CSUR)*, 41(3):15, 2009.

[50] Chin-Chen Chang, Tai-Xing Yu, and Hsuan-Yen Yen. Paper currency verification with support vector machines. In *Signal-Image Technologies and Internet-Based System, 2007. SITIS'07.*, pages 860–865, 2007.

[51] Can Chen, Scott McCloskey, and Jingyi Yu. Image splicing detection via camera response function analysis. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 5087–5096, 2017.

[52] Jie Chen, Shiguang Shan, Chu He, Guoying Zhao, Matti Pietikainen, Xilin Chen, and Wen Gao. Wld: A robust local image descriptor. *PAMI*, 2010.

[53] Tianqi Chen and Carlos Guestrin. Xgboost: A scalable tree boosting system. In *KDD*, 2016.

[54] Thomas H Chia and Michael J Levene. Detection of counterfeit us paper money using intrinsic fluorescence lifetime. *Optics Express*, 17(24):22054–22061, 2009.

[55] Giovanni Chierchia, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. A bayesian-mrf approach for prnu-based image forgery detection. *IEEE Transactions on Information Forensics and Security*, 9(4):554–567, 2014.

[56] Mircea Cimpoi, Subhransu Maji, Iasonas Kokkinos, and Andrea Vedaldi. Deep filter banks for texture recognition, description, and segmentation. *IJCV*, 2016.

[57] William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J Alex Halderman, and Edward W Felten. Fingerprinting blank paper using commodity scanners. In *2009 30th IEEE Symposium on Security and Privacy*, pages 301–314. IEEE, 2009.

[58] Alceu Ferraz Costa, Gabriel Humpire-Mamani, and Agma Juci Machado Traina. An efficient algorithm for fractal analysis of textures. In *SIBGRAPI*. IEEE, 2012.

[59] Ingemar J Cox, Matthew L Miller, Jeffrey Adam Bloom, and Chris Honsinger. *Digital watermarking*, volume 53. Springer, 2002.

[60] Davide Cozzolino and Luisa Verdoliva. Camera-based image forgery localization using convolutional neural networks. In *2018 26th European Signal Processing Conference (EUSIPCO)*, pages 1372–1376. IEEE, 2018.

[61] Davide Cozzolino and Luisa Verdoliva. Noiseprint: a cnn-based camera model fingerprint. *IEEE Transactions on Information Forensics and Security*, 2019.

[62] Davide Cozzolino Giovanni Poggi Luisa Verdoliva. Extracting camera-based fingerprints for video forensics. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 130–137, 2019.

[63] F. Cruz, N. Sidère, M. Coustaty, V. P. D'Andecy, and J. Ogier. Local binary patterns for document forgery detection. In *ICDAR*, 2017.

[64] Adam Crymble. How criminal were the irish? bias in the detection of london currency crime, 1797–1821. *The London Journal*, 43(1):36–52, 2018.

[65] Wikimedia commons.

[66] Navneet Dalal and Bill Triggs. Histograms of oriented gradients for human detection. In *CVPR*. IEEE, 2005.

[67] Janez Demšar. Statistical comparisons of classifiers over multiple data sets. *J. Mach. Learn. Res.*, 7:1–30, December 2006.

[68] Sharmishta Desai, Shraddha Kabade, Apurva Bakshi, Apeksha Gunjal, and Meghana Yeole. Implementation of multiple kernel support vector machine for automatic recognition and classification of counterfeit notes. *Int. J. Sci. Eng. Res.*, 5:882–886, 2014.

[69] Thomas Dewaele, Maurits Diephuis, Taras Holotyak, and Sviatoslav Voloshynovskiy. Forensic authentication of banknotes on mobile phones. *Electronic Imaging*, 2016.

[70] Maurits Diephuis and Sviatoslav Voloshynovskiy. Physical object identification based on famos microstructure fingerprinting: Comparison of templates versus invariant features. In *2013 8th International Symposium on Image and Signal Processing and Analysis (ISPA)*, pages 119–123. IEEE, 2013.

[71] Maurits Diephuis, Svyatoslav Voloshynovskiy, Taras Holotyak, Nabil Stendardo, and Bruno Keel. A framework for fast and secure packaging identification on mobile phones. In *Media Watermarking, Security, and Forensics 2014*, volume 9028, page 90280T. International Society for Optics and Photonics, 2014.

[72] Tamarafinide V Dittimi and Ching Y Suen. Mobile app for detection of counterfeit banknotes. In *Advances in Artificial Intelligence: 31st CCAI*, 2018.

[73] Chao Dong, Chen Change Loy, Kaiming He, and Xiaoou Tang. Image super-resolution using deep convolutional networks. *IEEE transactions on pattern analysis and machine intelligence*, 38(2):295–307, 2015.

[74] Iyad Abu Doush and AL-Btoush Sahar. Currency recognition using a smartphone: Comparison between color sift and gray scale sift algorithms. *Journal of King Saud University-Computer and Information Sciences*, 29(4):484–492, 2017.

[75] ECB. European central bank. the new 100 and 200 banknotes, 2018.

[76] W.G. Eckert. *Introduction to Forensic Sciences, Second Edition*. CRC Press, 1996.

[77] Mohamed Hamdy Eldefrawy and Muhammad Khurram Khan. Banknote validation through an embedded rfid chip and an nfc-enabled smartphone. *Mathematical Problems in Engineering*, 2015.

[78] Sara Elkasrawi and Faisal Shafait. Printer identification using supervised learning for document forgery detection. In *2014 11th IAPR International Workshop on Document Analysis Systems*, pages 146–150. IEEE, 2014.

[79] Andrew F Emmott, Shubhomoy Das, Thomas Dietterich, Alan Fern, and Weng-Keen Wong. Systematic construction of anomaly detection benchmarks from real data. In *Proceedings of the ACM SIGKDD workshop on outlier detection and description*, pages 16–21. ACM, 2013.

[80] Tolga Ergen, Ali Hassan Mirza, and Suleyman Serdar Kozat. Unsupervised and semi-supervised anomaly detection with lstm neural networks. *arXiv preprint arXiv:1710.09207*, 2017.

[81] Europol website, 2016.

[82] Hany Farid and Siwei Lyu. Higher-order wavelet statistics and their application to digital forensics. In *2003 Conference on Computer Vision and Pattern Recognition Workshop*, volume 8, pages 94–94. IEEE, 2003.

[83] PETER FARQUHAR. Sweden is already four-fifths of the way to becoming a genuine cashless society, 2014.

[84] Bo-Yuan Feng, Mingwu Ren, Xu-Yao Zhang, and Ching Y Suen. Extraction of serial numbers on bank notes. In *2013 12th International Conference on Document Analysis and Recognition*, pages 698–702. IEEE, 2013.

[85] Bo-Yuan Feng, Mingwu Ren, Xu-Yao Zhang, and Ching Y Suen. Automatic recognition of serial numbers in bank notes. *Pattern recognition*, 47(8):2621–2634, 2014.

[86] Pasquale Ferrara, Tiziano Bianchi, Alessia De Rosa, and Alessandro Piva. Image forgery localization via fine-grained analysis of cfa artifacts. *IEEE Transactions on Information Forensics and Security*, 7(5):1566–1577, 2012.

[87] Ronald A Fisher. Statistical methods and scientific inference. 1956.

[88] Forbes. Meet The Man Fighting America's Trade War Against Chinese Counterfeits (It's Not Trump), 2018.

[89] Electronic Frontier Foundation. List of printers which do or do not display tracking dots, 2017.

[90] Electronic Frontier Foundation. Secret code in color printers lets government track you, 2017.

[91] Milton Friedman. A comparison of alternative tests of significance for the problem of m rankings. *The Annals of Mathematical Statistics*, 11(1):pp. 86–92, 1940.

[92] Mark Funkb, Eugen Gillichb, Helene Dörksenb, Volker Lohwegb, Jürg Hofmanna, Thomas Türkea, Daniel Chassota, and Johannes Schaedea. Intaglio quality measurement. *Optical Document Security, Reconnaissance International*, 2016.

[93] Johann Gebhardt, Markus Goldstein, Faisal Shafait, and Andreas Dengel. Document authentication using printing technique features and unsupervised anomaly detection. In *ICDAR*, 2013.

[94] Gemalto. National id cards: 2016-2019 facts and trends, 2019.

[95] Stefan Glock, Eugen Gillich, Johannes Schaede, and Volker Lohweg. Feature extraction algorithm for banknote textures based on incomplete shift invariant wavelet packet transform. In *Pattern Recognition*, volume 5748 of *Lecture Notes in Computer Science*, pages 422–431. Springer Berlin Heidelberg, 2009.

[96] Karol Gregor, Ivo Danihelka, Alex Graves, Danilo Rezende, and Daan Wierstra. Draw: A recurrent neural network for image generation. PMLR, 2015.

[97] Zhenhua Guo, Lei Zhang, and David Zhang. A completed modeling of local binary pattern operator for texture classification. *IEEE Trans. Image Process.*, 2010.

[98] Raia Hadsell, Sumit Chopra, and Yann LeCun. Dimensionality reduction by learning an invariant mapping. In *CVPR*, 2006.

[99] Tom S.F. Haines, Oisin Mac Aodha, and Gabriel J. Brostow. My Text in Your Handwriting. In *Transactions on Graphics*, 2016.

[100] Kevin G. Hall. U.s. counterfeiting charges against n. korea based on shaky evidence, 2008.

[101] Kevin G. Hall. Wikipedia: Adolf eichmann, 2019.

[102] Kevin G. Hall. Wikipedia: Adolfo kaminsky, 2019.

[103] Kevin G. Hall. Wikipedia: Alexander solonik, 2019.

[104] Kevin G. Hall. Wikipedia: Kim jong-nam, 2019.

[105] Robert M Haralick. Statistical and structural approaches to texture. *Proceedings of the IEEE*, 1979.

[106] Masaki Hashiyada. Development of biometric dna ink for authentication security. *The Tohoku journal of experimental medicine*, 204:109–17, 11 2004.

[107] Alsadig Bashir Hassan and Yahia A Fadlalla. A survey on techniques of detecting identity documents forgery. In *2017 Sudan Conference on Computer Science and Information Technology (SCCSIT)*, pages 1–5. IEEE, 2017.

[108] Zhongwei He, Wei Lu, Wei Sun, and Jiwu Huang. Digital image splicing detection based on markov features in dct and dwt domain. *Pattern Recognition*, 45(12):4292–4299, 2012.

[109] Marko Heikkilä, Matti Pietikäinen, and Cordelia Schmid. Description of interest regions with center-symmetric local binary patterns. In *CVGIP*. Springer, 2006.

[110] S Higgins. Chasing a rainbow. *Chemistry in Britain*, 39:26–29, 06 2003.

[111] Geoffrey E Hinton. Connectionist learning procedures. In *Machine learning*, pages 555–610. Elsevier, 1990.

[112] J Hofmann, T Türke, D Chassot, E Gillich, H Dörksen, and V Lohweg. New strategies in image processing for standardized intaglio quality analysis in the printing process. *Optical Document Security. Reconnaissance International*, 2014.

[113] Jing Huang, S Ravi Kumar, Mandar Mitra, Wei-Jing Zhu, and Ramin Zabih. Image indexing using color correlograms. In *CVPR*. IEEE, 1997.

[114] Minyoung Huh, Andrew Liu, Andrew Owens, and Alexei A Efros. Fighting fake news: Image splice detection via learned self-consistency. In *Proceedings of the European Conference on Computer Vision (ECCV)*, pages 101–117, 2018.

[115] Subariah Ibrahim, Masoud Afrakhteh, and Mazleena Salleh. Adaptive watermarking for printed document authentication. In *5th International Conference on Computer Sciences and Convergence Information Technology*, pages 611–614. IEEE, 2010.

[116] Interpol website, 2016.

[117] Joanna Izdebska and Sabu Thomas. *Printing on polymers: fundamentals and applications*. William Andrew, 2015.

[118] Hervé Jégou, Matthijs Douze, Cordelia Schmid, and Patrick Pérez. Aggregating local descriptors into a compact image representation. In *Computer Vision and Pattern Recognition (CVPR), 2010 IEEE Conference on*, pages 3304–3311. IEEE, 2010.

[119] Ye Jin, Ling Song, Xianglong Tang, and Ming Du. A hierarchical approach for banknote image processing using homogeneity and ffd model. *IEEE Signal Processing Letters*, 15:425–428, 2008.

[120] S. Kaminsky and M. Mitchell. *Adolfo Kaminsky: A Forger's Life*. Consortium Book Sales & Dist, 2016.

[121] Juho Kannala and Esa Rahtu. Bsif: Binarized statistical image features. In *ICPR*. IEEE, 2012.

[122] Mona Kasra, Cuihua Shen, and James F O'Brien. Seeing is believing: How people fail to identify fake images on the web. In *Extended abstracts of the 2018 CHI conference on human factors in computing systems*, page LBW516. ACM, 2018.

[123] Kirill Keller, Aleksandr V Yakovlev, Elena V Grachova, and Alexandr V Vinogradov. Inkjet printing of multicolor daylight visible opal holography. *Advanced Functional Materials*, 28(21):1706903, 2018.

[124] Oleg Khitalsky. Watermark conference-2017, 2017.

[125] Hae Yong Kim and Joceli Mayer. Data hiding for binary documents robust to print-scan, photocopy and geometric distortions. In *XX Brazilian Symposium on Computer Graphics and Image Processing (SIBGRAPI 2007)*, pages 105–112. IEEE, 2007.

[126] Jiwon Kim, Jung Kwon Lee, and Kyoung Mu Lee. Accurate image super-resolution using very deep convolutional networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1646–1654, 2016.

[127] Gregory Koch, Richard Zemel, and Ruslan Salakhutdinov. Siamese neural networks for one-shot image recognition. In *ICML deep learning workshop*, volume 2, 2015.

[128] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. In *Adv Neural Inf Process Syst*, 2012.

[129] Chandan Kumar, Amit Kumar Singh, and Pardeep Kumar. A recent survey on image watermarking techniques and its application in e-governance. *Multimedia Tools and Applications*, 77(3):3597–3622, 2018.

[130] Young-bin Kwon and Jeong-hoon Kim. Recognition based verification for the machine readable travel documents. In *International Workshop on Graphics Recognition (GREC 2007), Curitiba, Brazil*. Citeseer, 2007.

[131] Christoph H Lampert, Lin Mei, and Thomas M Breuel. Printing technique classification for document counterfeit detection. In *2006 International Conference on Computational Intelligence and Security*, volume 1, pages 639–644. IEEE, 2006.

[132] Svetlana Lazebnik, Cordelia Schmid, and Jean Ponce. Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories. In *Computer vision and pattern recognition, 2006 IEEE computer society conference on*, volume 2, pages 2169–2178. IEEE, 2006.

[133] Honglak Lee, Alexis Battle, Rajat Raina, and Andrew Y Ng. Efficient sparse coding algorithms. In *Advances in neural information processing systems*, pages 801–808, 2006.

[134] Ji Lee, Hyung Hong, Ki Kim, and Kang Park. A survey on banknote recognition methods by various sensors. *Sensors*, 17(2):313, 2017.

[135] Keon-Ho Lee and Tae-Hyoung Park. Image segmentation of uv pattern for automatic paper-money inspection. In *2010 11th International Conference on Control Automation Robotics & Vision*, pages 1175–1180. IEEE, 2010.

[136] Thomas Leung and Jitendra Malik. Representing and recognizing the visual appearance of materials using three-dimensional textons. *IJCV*, 2001.

[137] Meijie Li, Youri Meuret, René Geelen, Jürgen Jung, Michael Vervaeke, Hugo Thienpont, and Fabian Duerr. Optical modeling of changeable laser image functionality with analysis of the viewing performance. *Applied optics*, 54(20):6162–6171, 2015.

[138] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining*, pages 413–422. IEEE, 2008.

[139] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation-based anomaly detection. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 6(1):3, 2012.

[140] Ruizhen Liu and Tieniu Tan. An svd-based watermarking scheme for protecting rightful ownership. *IEEE transactions on multimedia*, 4(1):121–128, 2002.

[141] Yezheng Liu, Zhe Li, Chong Zhou, Yuanchun Jiang, Jianshan Sun, Meng Wang, and Xiangnan He. Generative adversarial active learning for unsupervised outlier detection. *IEEE Transactions on Knowledge and Data Engineering*, 2019.

[142] V. Lohweg. UCI banknote authentication data set, 2012.

[143] Volker Lohweg, H Dörksen, E Gillich, R Hildebrand, JL Hoffmann, and J Schaede. Mobile devices for banknote authentication–is it possible? In *Optical Document Security-The Conference on Optical Security and Counterfeit Detection*, volume 3, pages 1–12, 2012.

[144] Volker Lohweg, H Dörksen, E Gillich, R Hildebrand, JL Hoffmann, and J Schaede. Mobile devices for banknote authentication–is it possible? In *Optical Document Security*, 2012.

[145] Volker Lohweg, Jan Leif Hoffmann, Helene Dörksen, Roland Hildebrand, Eugen Gillich, Jürg Hofmann, and Johannes Schaede. Banknote authentication with mobile devices. In *Media Watermarking, Security, and Forensics*, volume 8665, pages 866507–866507–14, 2013.

[146] David G Lowe. Object recognition from local scale-invariant features. In *ICCV*. IEEE, 1999.

[147] David G Lowe. Distinctive image features from scale-invariant keypoints. *International journal of computer vision*, 60(2):91–110, 2004.

[148] Jan Lukáš, Jessica Fridrich, and Miroslav Goljan. Detecting digital image forgeries using sensor pattern noise. In *Security, Steganography, and Watermarking of Multimedia Contents VIII*, volume 6072, page 60720Y. International Society for Optics and Photonics, 2006.

[149] Ningning Ma, Xiangyu Zhang, Hai-Tao Zheng, and Jian Sun. Shufflenet v2: Practical guidelines for efficient cnn architecture design. In *Proceedings of the European Conference on Computer Vision (ECCV)*, pages 116–131, 2018.

[150] Laurens van der Maaten and Geoffrey Hinton. Visualizing data using t-sne. *Journal of machine learning research*, 9(Nov):2579–2605, 2008.

[151] Shital Mahajan and KP Rane. A survey on counterfeit paper currency recognition and detection. In *International Conference on Industrial Automation and Computing (ICIAC)*, 2014.

[152] Clarisse MANDRIDAKE, Amine OUDDAN, Mathieu HOARAU, and Kévin WIN-LIME. Towards fully automatic id document frauds detection.

[153] Manisha Mann, S Shukla, and Shruti Gupta. A comparative study on security features of banknotes of various countries. *Int. J. Multidiscip. Res. Dev*, 2:83–91, 2015.

[154] J Mercer. Functions of positive and negative type and their connection with the theory of integral equations, philosophical transsaction of the royal society of london, ser, 1909.

[155] Dubravko Miljković. Review of novelty detection methods. In *The 33rd International Convention MIPRO*, pages 593–598. IEEE, 2010.

[156] Mutahir Nadeem, Ochaun Marshall, Sarbjit Singh, Xing Fang, and Xiaohong Yuan. Semi-supervised deep neural network for network intrusion detection. 10 2016.

[157] Nayax. First cashless country, 2018.

[158] Peter Nemenyi. *Distribution-free multiple comparisons*. PhD thesis, Princeton University, New Jersey, USA, 1963.

[159] Sophie J. Nightingale, Kimberley A. Wade, and Derrick G. Watson. Can people identify original and manipulated photos of real-world scenes? *Cognitive Research: Principles and Implications*, 2(1):30, Jul 2017.

[160] OECD. Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, 2016.

[161] Timo Ojala, Matti Pietikainen, and Topi Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Trans. Pattern Anal. Mach. Intell*, 2002.

[162] Ville Ojansivu and Janne Heikkilä. Blur insensitive texture classification using local phase quantization. In *ICSIP*. Springer, 2008.

[163] Aude Oliva and Antonio Torralba. Modeling the shape of the scene: A holistic representation of the spatial envelope. *IJCV*, 2001.

[164] Omkar M Parkhi, Karen Simonyan, Andrea Vedaldi, and Andrew Zisserman. A compact and discriminative face track descriptor. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 1693–1700, 2014.

[165] Cecilia Pasquini, Giulia Boato, and Fernando Pérez-González. Statistical detection of jpeg traces in digital images in uncompressed formats. *IEEE Transactions on Information Forensics and Security*, 12(12):2890–2905, 2017.

[166] Florent Perronnin and Christopher Dance. Fisher kernels on visual vocabularies for image categorization. In *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on*, pages 1–8. IEEE, 2007.

[167] Burt Perry, Scott Carr, and Phil Patterson. Digital watermarks as a security feature for identity documents. In *Optical Security and Counterfeit Deterrence Techniques III*, volume 3973, pages 80–87. International Society for Optics and Photonics, 2000.

[168] A Pfeifer, E Gillich, V Lohweg, and J Schaede. Detection of commercial offset printing in counterfeited banknotes. In *Optical Document Security*, 2016.

[169] Marc Michel Pic, Clarisse Mandridake, Mathieu Hoarau, and Kevin Win-Lime. Docscope: Id printing techniques signatures. In *2014 IEEE Joint Intelligence and Security Informatics Conference*, pages 334–334. IEEE, 2014.

[170] Justin Picard, Claus Vielhauer, and Niels Thorwirth. Towards fraud-proof id documents using multiple data hiding technologies and biometrics. In *Security, Steganography, and Watermarking of Multimedia Contents*, 2004.

[171] John Pickering. The history of paper money in china. *Journal of the American Oriental Society*, 1(2):136–142, 1844.

[172] Marco AF Pimentel, David A Clifton, Lei Clifton, and Lionel Tarassenko. A review of novelty detection. *Signal Processing*, 99:215–249, 2014.

[173] B Sai Prasanthi and D Rajesh Setty. Indian paper currency authentication system using image processing. *Int. J. Sci. Res. Eng. Technol*, 4:973–981, 2015.

[174] Emma L Prime and David H Solomon. Australia's plastic banknotes: fighting counterfeit currency. *Angewandte Chemie International Edition*, 49(22):3726–3736, 2010.

[175] Sumin Qian, Xianzhang Zuo, Yunze He, Guiyun Tian, and Hong Zhang. Detection technology to identify money based on pulsed eddy current technique. In *The 17th International Conference on Automation and Computing*, pages 230–233. IEEE, 2011.

[176] Yinlong Qian, Jing Dong, Wei Wang, and Tieniu Tan. Deep learning for steganalysis via convolutional neural networks. In *Media Watermarking, Security, and Forensics 2015*, volume 9409, page 94090J. International Society for Optics and Photonics, 2015.

[177] Ubaid Ur Rahman, Allah Bux Sargano, and Usama Ijaz Bajwa. Android-based verification system for banknotes. *J. Imaging*, 2017.

[178] Sachin Ravi and Hugo Larochelle. Optimization as a model for few-shot learning. In *In International Conference on Learning Representations (ICLR)*, 2017.

[179] Joseph Redmon and Ali Farhadi. YOLO9000: better, faster, stronger. *CoRR*, abs/1612.08242, 2016.

[180] Ankush Roy, Biswajit Halder, Utpal Garain, and David S Doermann. Machine-assisted authentication of paper currency: an experiment on indian banknotes. *IJDAR*, 2015.

[181] Ron Rubinstein, Michael Zibulevsky, and Michael Elad. Efficient implementation of the k-svd algorithm using batch orthogonal matching pursuit. *CS Technion*, 40(8):1–15, 2008.

[182] Ethan Rublee, Vincent Rabaud, Kurt Konolige, and Gary R Bradski. Orb: An efficient alternative to sift or surf. In *ICCV*, volume 11, page 2. Citeseer, 2011.

[183] Lukas Ruff, Nico Görnitz, Lucas Deecke, Shoaib Ahmed Siddiqui, Robert Vandermeulen, Alexander Binder, Emmanuel Müller, and Marius Kloft. Deep one-class classification. In *International Conference on Machine Learning*, pages 4390–4399, 2018.

[184] V Rusanov, K Chakarova, and T Madolev. Mössbauer spectroscopy investigation of the properties and stability of dollar bank note pigments. *Applied spectroscopy*, 56(9):1228–1236, 2002.

[185] V Rusanov, K Chakarova, H Winkler, and AX Trautwein. Mössbauer and x-ray fluorescence measurements of authentic and counterfeited banknote pigments. *Dyes and Pigments*, 81(3):254–258, 2009.

[186] Seung-Jin Ryu, Hae-Yeoun Lee, Il-Weon Cho, and Heung-Kyu Lee. Document forgery detection with svm classifier and image quality measures. In *PCM*. Springer, 2008.

[187] Mohammad Sabokrou, Mohsen Fayyaz, Mahmood Fathy, Zahra Moayed, and Reinhard Klette. Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes. *Computer Vision and Image Understanding*, 172:88–97, 2018.

[188] Sofia Safaryan, Vladislav Slabov, Svitlana Kopyl, Konstantin Romanyuk, Igor Bdikin, Semen Vasilev, Pavel Zelenovskiy, Vladimir Ya Shur, Evgeny A Uslamin, Evgeny A Pidko, et al. Diphenylalanine-based microribbons for piezoelectric applications via inkjet printing. *ACS applied materials & interfaces*, 10(12):10543–10551, 2018.

[189] Mark Sandler, Andrew Howard, Menglong Zhu, Andrey Zhmoginov, and Liang-Chieh Chen. Mobilenetv2: Inverted residuals and linear bottlenecks. In *CVPR*, 2018.

[190] Aziza Satkhozhina, Ildus Ahmadullin, and Jan P Allebach. Optical font recognition using conditional random field. In *Proceedings of the 2013 ACM symposium on Document engineering*, pages 119–122. ACM, 2013.

[191] Victor Schetinger, Manuel M Oliveira, Roberto da Silva, and Tiago J Carvalho. Humans are easily fooled by digital images (vol 68, pg 142, 2017). *COMPUTERS & GRAPHICS-UK*, 70:327–327, 2018.

[192] Bernhard Schölkopf, John C Platt, John Shawe-Taylor, Alex J Smola, and Robert C Williamson. Estimating the support of a high-dimensional distribution. *Neural computation*, 13(7):1443–1471, 2001.

[193] Bernhard Scholkopf and Alexander J Smola. *Learning with kernels: support vector machines, regularization, optimization, and beyond*. MIT press, 2001.

[194] Ben Schouten and Bart Jacobs. Biometrics and their use in e-passports. *Image and Vision Computing*, 27(3):305–312, 2009.

[195] Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. In *CVPR*, 2015.

[196] Ashlesh Sharma, Lakshminarayanan Subramanian, and Eric A Brewer. Paperspeckle: microscopic fingerprinting of paper. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 99–110. ACM, 2011.

[197] Frank Y Shih. *Digital watermarking and steganography: fundamentals and techniques*. CRC press, 2017.

[198] Pranav Shyam, Shubham Gupta, and Ambedkar Dukkipati. Attentive recurrent comparators. *CoRR*, 2017.

[199] Si Si, Cho-Jui Hsieh, and Inderjit S Dhillon. Memory efficient kernel approximation. *The Journal of Machine Learning Research*, 18(1):682–713, 2017.

[200] Jay A Siegel and Pekka J Saukko. *Encyclopedia of forensic sciences*. Academic Press, 2012.

[201] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014.

[202] Steven Simske, Guy Adams, Jason Aronoff, and Margaret Sturgill. New findings in security printing and imaging. In *NIP & Digital Fabrication Conference*, volume 2009, pages 158–160. Society for Imaging Science and Technology, 2009.

[203] Ms Neha Singh and Sandeep Joshi. Digital image forensics: progress and challenges. In *Proceedings of 31st National convention of Electronics and Telecommunication Engineers, Researchgate (October 2015)*, 2016.

[204] Prabhishek Singh and RS Chadha. A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9):165–175, 2013.

[205] Josef Sivic and Andrew Zisserman. Video google: A text retrieval approach to object matching in videos. In *Computer Vision. Proceedings.*, pages 1470–1477, 2003.

[206] Hongchao Song, Zhuqing Jiang, Aidong Men, and Bo Yang. A hybrid semi-supervised anomaly detection model for high-dimensional data. *Computational Intelligence and Neuroscience*, 2017:1–9, 11 2017.

[207] Margaret Sturgill, Galia Golodetz, Steven Simske, and Jason Aronoff. Security printing deterrents: a comparison of thermal ink jet, dry electrophotographic, and liquid electrophotographic printing. *Journal of Imaging Science and Technology*, 52(5):50201–1, 2008.

[208] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke, and Andrew Rabinovich. Going deeper with convolutions. In *CVPR*, 2015.

[209] Christian Szegedy, Vincent Vanhoucke, Sergey Ioffe, Jon Shlens, and Zbigniew Wojna. Rethinking the inception architecture for computer vision. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 2818–2826, 2016.

[210] G+D Currency Technology. G+d currency technology, 2019.

[211] Songpon Teerakanok and Tetsutaro Uehara. Copy-move forgery detection: A state-of-the-art technical review and analysis. *IEEE Access*, 7:40550–40568, 2019.

[212] Kharittha Thongkor and Thumrongrat Amornraksa. Digital image watermarking for photo authentication in thai national id card. In *2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*, pages 1–4. IEEE, 2012.

[213] Ehsan Toreini, Siamak F Shahandashti, and Feng Hao. Texture to the rescue: Practical paper fingerprinting based on texture patterns. *ACM Transactions on Privacy and Security (TOPS)*, 20(3):9, 2017.

[214] John W Tukey. Comparing individual means in the analysis of variance. *Biometrics*, 1949.

[215] Aaron Tuor, Samuel Kaplan, Brian Hutchinson, Nicole Nichols, and Sean Robinson. Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. In *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*, 2017.

[216] A. Upadhyaya, V. Shokeen, and G. Srivastava. Counterfeit currency detection techniques. In *Confluence*, 2018.

[217] Joost Van Beusekom, Faisal Shafait, and Thomas M Breuel. Text-line examination for document forgery detection. *International Journal on Document Analysis and Recognition (IJDAR)*, 16(2):189–207, 2013.

[218] Rudolf L. van Renesse. Ordering the order: a survey of optical document security features, 1995.

[219] Rudolf L Van Renesse and Rudolf L Van Renesse. *Optical document security*. Artech House Boston, 2005.

[220] Manik Varma and Andrew Zisserman. Texture classification: Are filter banks necessary? In *CVPR*. IEEE, 2003.

[221] Luisa Verdoliva, Davide Cozzolino, and Giovanni Poggi. A feature-based approach for image tampering detection and localization. In *2014 IEEE international workshop on information forensics and security (WIFS)*, pages 149–154. IEEE, 2014.

[222] Antanas Verikas, Jens Lundström, Marija Bacauskiene, and Adas Gelzinis. Advances in computational intelligence-based print quality assessment and control in offset colour printing. *Expert Systems with Applications*, 38(10):13441–13447, 2011.

[223] Anna Vila, N Ferrer, J Mantecon, D Breton, and JF Garcia. Development of a fast and non-destructive procedure for characterizing and distinguishing original and fake euro notes. *Analytica Chimica Acta*, 559(2):257–263, 2006.

[224] Oriol Vinyals, Charles Blundell, Tim Lillicrap, Daan Wierstra, et al. Matching networks for one shot learning. In *Advances in Neural Information Processing Systems*, pages 3630–3638, 2016.

[225] Sviatoslav Voloshynovskiy, Maurits Diephuis, Fokko Beekhof, Oleksiy Koval, and Bruno Keel. Towards reproducible results in authentication based on physical non-cloneable functions: The forensic authentication microstructure optical set (famos). In *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 43–48. IEEE, 2012.

[226] Aline Vuarnoz, Olivier Amrein, and Patrick Veya. Ink composition comprising optically variable pigments, use of the composition, optically variable pigment and method of treating said pigment, June 3 2008. US Patent 7,381,758.

[227] Robert J Wang, Xiang Li, and Charles X Ling. Pelee: a real-time object detection system on mobile devices. In *NeurIPS*, 2018.

[228] Wei Wang, Jing Dong, and Tieniu Tan. A survey of passive image tampering detection. In *International Workshop on Digital Watermarking*, pages 308–322. Springer, 2009.

[229] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image quality assessment: from error visibility to structural similarity. *IEEE Trans. Image Process.*, 2004.

[230] Li Wenhong, Tian Wenjuan, Cao Xiyan, and Gao Zhen. Application of support vector machine (svm) on serial number identification of rmb. In *2010 8th World Congress on Intelligent Control and Automation*, pages 6262–6266. IEEE, 2010.

[231] Wikipedia. Counterfeit money.

[232] Business Wire. Security paper market, 2023 by component (substrates, watermarks, threads, holograms), application (banknotes, passports, identity cards, certificates, legal government documents, cheques, stamps), 2019.

[233] David Wolman. *The end of money: Counterfeiters, preachers, techies, dreamers–and the coming cashless society*. Da Capo Press, 2013.

[234] Chau-Wai Wong and Min Wu. A study on puf characteristics for counterfeit detection. In *2015 IEEE International Conference on Image Processing (ICIP)*, pages 1643–1647. IEEE, 2015.

[235] Chau-Wai Wong and Min Wu. Counterfeit detection based on unclonable feature of paper using mobile camera. *IEEE Transactions on Information Forensics and Security*, 12(8):1885–1899, 2017.

[236] Bartlomiej Wronski, Ignacio Garcia-Dorado, Manfred Ernst, Damien Kelly, Michael Krainin, Chia-Kai Liang, Marc Levoy, and Peyman Milanfar. Handheld multi-frame super-resolution. *arXiv preprint arXiv:1905.03277*, 2019.

[237] Lin Wu, Yang Wang, Junbin Gao, and Dacheng Tao. Deep co-attention based comparators for relative representation learning in person re-identification. *CoRR*, 2018.

[238] Yue Wu, Wael AbdAlmageed, and Premkumar Natarajan. Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 9543–9552, 2019.

[239] Saining Xie, Ross Girshick, Piotr Dollár, Zhuowen Tu, and Kaiming He. Aggregated residual transformations for deep neural networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1492–1500, 2017.

[240] Chunlin Yang. Fingerprint biometrics for id document verification. In *2014 9th IEEE Conference on Industrial Electronics and Applications*, pages 1441–1445. IEEE, 2014.

[241] Jianchao Yang, Kai Yu, Yihong Gong, and Thomas Huang. Linear spatial pyramid matching using sparse coding for image classification. In *Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on*, pages 1794–1801. IEEE, 2009.

[242] Jianchao Yang, Kai Yu, Yihong Gong, and Tingwen Huang. Linear spatial pyramid matching using sparse coding for image classification. In *Computer Vision and Pattern Recognition*, pages 1794–1801, 2009.

[243] Chi-Yuan Yeh, Wen-Pin Su, and Shie-Jue Lee. Employing multiple-kernel support vector machines for counterfeit banknote recognition. *Applied Soft Computing*, 2011.

[244] Ido Yerushalmy and Hagit Hel-Or. Digital image forgery detection based on lens and sensor aberration. *International journal of computer vision*, 92(1):71–91, 2011.

[245] Hsiang-Fu Yu, Fang-Lan Huang, and Chih-Jen Lin. Dual coordinate descent methods for logistic regression and maximum entropy models. *Machine Learning*, 85(1-2):41–75, 2011.

[246] Markos Zampoglou, Symeon Papadopoulos, and Yiannis Kompatsiaris. Large-scale evaluation of splicing localization algorithms for web images. *Multimedia Tools and Applications*, 76(4):4801–4834, 2017.

[247] Lin Zhang, Lei Zhang, Xuanqin Mou, and David Zhang. Fsim: A feature similarity index for image quality assessment. *IEEE Trans. Image Process.*, 2011.

[248] Lin Zhang, Zhiqiang Zhou, and Hongyu Li. Binary gabor pattern: An efficient and robust descriptor for texture classification. In *ICIP*. IEEE, 2012.

[249] Yulun Zhang, Yapeng Tian, Yu Kong, Bineng Zhong, and Yun Fu. Residual dense network for image super-resolution. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 2472–2481, 2018.

[250] Ting-ting Zhao, Ji-yin Zhao, Rui-rui Zheng, and Lu-lu Zhang. Study on rmb number recognition based on genetic algorithm artificial neural network. In *2010 3rd International Congress on Image and Signal Processing*, volume 4, pages 1951–1955. IEEE, 2010.

[251] Yue Zhao, Zain Nasrullah, Maciej K Hryniewicki, and Zheng Li. Lscp: Locally selective combination in parallel outlier ensembles. In *Proceedings of the 2019 SIAM International Conference on Data Mining*, pages 585–593. SIAM, 2019.

[252] Lilei Zheng, Ying Zhang, and Vrizlynn LL Thing. A survey on image tampering and its detection in real-world photos. *Journal of Visual Communication and Image Representation*, 58:380–399, 2019.

[253] Peng Zhou, Xintong Han, Vlad I Morariu, and Larry S Davis. Learning rich features for image manipulation detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pages 1053–1061, 2018.