Robustness of a Blind Image Watermark Detector Designed by Orthogonal Projection

Cong Jin [*†] Jiaxiong Peng [*]

* *Institute for Pattern Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan* 430074, *P.R.China*;

† *Department of Computer Science, Central China Normal University, Wuhan* 430079, *P.R.China*

Received 28 May 2004; accepted 9 July 2004

Abstract

Digital watermarking is a key technique practical intellectual property protecting systems and concealment correspondence systems. In this paper, we discussed a blind detection method for the digital image watermark. The theories research show that the orthogonal projection sequence of a digital image is one-to-one correspondence with this digital image. By this conclusion, we designed a novel blind watermark detector. In this detector, to calculate the correlation value between the image and watermark, the intensity information of digital image is not used, and the orthogonal projection sequence of this image is used. Experiment results show that this watermark detector not only to have very strong resistant ability to translation and rotation attacks, but also to have the good robustness to Gaussian noise. Performance of this watermark detector is better than general detector designed by the intensity information directly. The conclusions of this paper are useful to the research in the future.

Key words Digital Watermark; Image Projective Sequence; Robust Detection

1 Introduction

Digital watermarking[1,2], the art of hiding information into multimedia data in a robust and invisible manner, has gained great interest over the past few years. There has been a lot of interest in the digital watermarking research, mostly due to the fact that digital watermarking might be used as a tool to protect the copyright of multimedia data. A digital watermark is an imperceptible signal embedded directly into the media content, and it can be detected from the host media for some applications. The insertion and detection of digital watermarks can help to identify the source or ownership of the media, the legitimacy of its usage, the type of the content or other

Correspondence to: jincong26@yahoo.com.cn

Recommended for acceptance by Francisco Perales

ELCVIA ISSN:1577-5097

Published by Computer Vision Center / Universitat Aut`onoma de Barcelona, Barcelona, Spain

accessory information in various applications. Specific operations related to the status of the watermark can then be applied to cope with different situations.

A majority of the watermarking algorithms proposed in the literature operate on a principle analogous to spread-spectrum communications. A pseudo-random sequence, which is called digital watermark, is inserted into the image. During extraction, the same pseudo-random sequence is correlated with the estimated pattern extracted from the image. The watermark is said to be present if the computed correlation exceeds a chosen threshold value. Among this general class of watermarking schemes, there are several variations that include choice of specific domain for watermark insertion, e.g. spatial, DCT, wavelet, etc; and enhancements of the basic scheme to improve robustness and reduce visible artifacts. The computed correlation depends on the alignment of the pattern regenerated and the one extracted from the image. Thus proper synchronization of the two patterns is critical for the watermark detection process. Typically, this synchronization is provided by the inherent geometry of the image, where pseudo-random sequences are assumed to be placed on the same image geometry. When a geometric manipulation is applied to the watermarked image, the underlying geometry is distorted, which often results in the de-synchronization and failure of the watermark detection process. The geometric manipulations can range from simple scaling and rotation or cropping to more complicated random geometric distortions as applied by Stirmark[3].

Different methods have been proposed in literature to reduce/prevent algorithm failure modes in case of geometric manipulations. For non-blind watermarking schemes, where the original image is available at the detector, the watermarked image may be registered against the original image to provide proper synchronization[4]. For blind watermarking schemes, where the original image is not available at the detector, proposed methods include use of the Fourier-Melin transform space that provides rotation, translation, scale invariance[5], and watermarking using geometric invariants of the image such as moments[6] or cross-ratios[7]. Hartung *et al*[8] have also proposed a scheme that divides the image into small blocks and performs correlation for rotations and translations using small increments, in an attempt to detect the proper synchronization.

In this paper, the orthogonal projective sequence of a digital image is analyzed. A blind image watermark detector is designed by using the orthogonal projective sequence of digital image. In Section 2, we first discuss definition and its properties of the orthogonal projective sequence of a digital image. A conclusion, the orthogonal projection sequence of a digital image is one-to-one correspondence with this digital image, is obtained. By this conclusion, we designed a blind watermark detector. Then, in Section 3, we present our experimental results. Experiment results show that this watermark detector not only to have very strong resistant ability to translation and rotation attacks, but also to have the good robustness to Gaussian noise. Finally, Section 4 contains our conclusions.

2 The Design Method of the Watermark Detector

We assume that the real image intensity function $I(x, y)$ is piecewise continuous, and has non-zero in a bounded domain, where $x = 0,1,\ldots,m-1;\ y = 0,1,\ldots,n-1,\ m \times n = N$.

The geometric moments[9] of order $(p+q)$ of $I(x, y)$ are defined as

$$M_{pq} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} x^p y^q I(x, y)dxdy \tag{1}$$

where $p, q=0,1,2,\ldots,\infty$. By [10], we know that the infinite sequence $\{M_{pq}\}$ is one-to-one correspondence with image intensity function $I(x, y)$ whenever $I(x, y)$ is piecewise continuous. If the integral value is calculated by

equation (1), we can add the definition $I(x, y)=0$ in the outside bounded domain.

Let H be a Hibert space, and $\{g_i(x,y)\}_{i=1}^{\infty}$ be normal orthogonal basis of H. We have

$$\iint_A g_i(x,y)g_j(x,y)dxdy = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}.$$

Let $I(x, y)\in H$ and be square integrable function, we define

$$\alpha_i = \alpha(g_i(x,y))_A = \iint_A I(x,y)g_i(x,y)dxdy, \quad i = 1,2,... \quad . \tag{2}$$

Where, α_i is called the coordinate of $I(x, y)$ with respect to this basis, also is called the orthogonal projection.

Is it one-to-one correspondence between infinite sequence $\{\alpha_i\}_{i=1}^{\infty}$ and image function $I(x, y)$? Because the existence of function $I(x, y)$, to satisfy the equation (2), can't be guaranteed only by arbitrarily infinite sequence $\{\alpha_i\}_{i=1}^{\infty}$, this one-to-one correspondence can't exist generally. But if $\{\alpha_i\}_{i=1}^{\infty}$ satisfying the some conditions, this one-to-one correspondence may exist. This is conclusion of our Theorem.

Theorem If the function series $\sum_{j=1}^{\infty}\alpha_j g_j(x,y)$ is uniformly convergent, then there is an unique function $I(x, y)$ such that $I(x, y)$ satisfy the equation (2).

Proof Let $I(x,y)=\sum_{j=1}^{\infty}\alpha_j g_j(x,y)$. By uniformly convergent of the function series $\sum_{j=1}^{\infty}\alpha_j g_j(x,y)$, we indicate that $I(x, y)$ exists, and

$$\iint_A I(x,y)g_i(x,y)dxdy = \iint_A g_i(x,y)\{\sum_{j=1}^{\infty}\alpha_j g_i(x,y)\}dxdy, \quad i = 1,2,... \quad .$$

To exchange calculus order between the integral and sum and to use the normal orthogonality of the function systems $\{g_i(x,y)\}_{i=1}^{\infty}$, we may obtain

$$\iint_A I(x,y)g_i(x,y)dxdy = \alpha_i, \quad i = 1,2,... \; .$$

Therefore, $I(x, y)$ satisfies the equation (2). Following, we discuss uniqueness of image $I(x, y)$.
Let $I_1(x,y) \neq I_2(x,y),\ (x,y)\in A$, and their projection sequences are same. We notice that

$$\alpha_i = \iint_A I_1(x,y)g_i(x,y)dxdy, \qquad \alpha_i = \iint_A I_2(x,y)g_i(x,y)dxdy, \quad i = 1,2,\ldots .$$

By subtraction of these two equations, we obtain

$$\iint_A g_i(x,y)\{I_1(x,y) - I_2(x,y)\}dxdy = 0, \quad i = 1,2,\ldots .$$

By the completeness[10] of the basis, $I_1(x,y) = I_2(x,y)$ can be obtained, where $(x,y)\in A$. This is contradictory with assumption of Theorem, therefore $I(x, y)$ is unique.

By this Theorem we know that the orthogonal projective sequence $\{\alpha_i\}_{i=1}^{\infty}$, obtained by general normal orthogonal basis $\{g_i(x,y)\}_{i=1}^{\infty}$, is one-to-one correspondence with image intensity function $I(x, y)$ under the

condition of Theorem. Therefore, the infinite sequence $\{\alpha_i\}_{i=1}^{\infty}$ is a feature sequence of digital image $I(x, y)$.

Because only finite terms can be researched in the $\{g_i(x,y)\}_{i=1}^{\infty}$, we let $S=\{g_i(x,y)\}_{i=1}^{N}$. From now, we research digital watermark is only on the S.

It is very common that the digital watermarking is embedded using multiplicative embedding method. The watermarked image data $J(x, y)$ are now formed from the digital watermarking $W(x, y)$ and the original image data $I(x, y)$ according to

$$J(x,y)=I(x,y)+\omega\cdot I(x,y)\cdot W(x,y),\quad x=0,1,\ldots,m-1;\quad y=0,1,\ldots,n-1 \tag{3}$$

where ω is the strength factor controlling the watermarking strength. This way of embedding digital watermarking was proposed, among others, by *Cox et.al*.[11].

We denote the finite projective sequence of digital watermarking $W(x, y)$ is $\boldsymbol{w}=\{w_i\}_{i=1}^{N}$. One can attack watermarked image $J(x, y)$ by general image processing operations, such as translation, rotation, noise, etc., or by combining these operations. Attacked image $\tilde{J}(x,y)$ of $J(x, y)$ may be obtained. We denote the finite projective sequence of attacked image $\tilde{J}(x,y)$ is $\boldsymbol{\gamma}=\{\gamma_i\}_{i=1}^{N}$.

Many measurements have been proposed for blind watermark detection[12]. Among them, a frequently used one is the normalized correlation measurement, which measures the cosine angle of the two feature vectors. In this paper, we let two feature vectors are $\boldsymbol{w}$ and $\boldsymbol{\gamma}$ respectively, by means of

$$c=\frac{\sum_{i=1}^{N} w_i\gamma_i}{\sqrt{\sum_{i=1}^{N} w_i^2}\sqrt{\sum_{i=1}^{N}\gamma_i^2}} \tag{4}$$

To detect a watermark in a possibly watermarked image $\tilde{J}(x,y)$, we calculate the correlation between the image $\tilde{J}(x,y)$ and the $W(x, y)$. In general, $W(x, y)$ generated using different keys have very low correlation with each other. Therefore, during the detection process the correlation value will be very high for a $W(x, y)$ generated with the correct key and would be very low otherwise. During the detection process, it is common to set a threshold ρ to decide whether the watermark is detected or not. If the correlation exceeds a certain threshold ρ, the watermark detector determines that image $\tilde{J}(x,y)$ contains watermark $W(x, y)$.

Although the Fourier transformation[10] has many advantages for image signal processing, its operation speed is influenced by the real and imaginary part calculated respectively. We know that Walsh function system[13] is a complete normal orthogonal basis, therefore, it can become a basis when orthogonal projection sequence of digital image is calculated. In addition, each Walsh function value is always 1 or -1, and it is easy to obtain the kernel matrix, so the calculation is simple and operation speed can be increased.

According to arrangement order, the Walsh function can be generated by three methods. In this paper, the Walsh function is generated using the Hadamard matrix.

By the one dimensional Walsh function systems, the two dimensional Walsh function systems can be generated according to following as arrangement order

Walsh(0, *x*) *Walsh*(0, *y*),	*Walsh*(0, *x*) *Walsh*(1, *y*),	…	, *Walsh*(0, *x*) *Walsh*(*n*-1, *y*),
Walsh(1, *x*) *Walsh*(0, *y*),	*Walsh*(1, *x*) *Walsh*(1, *y*),	…	, *Walsh*(1, *x*) *Walsh*(*n*-1, *y*),
…	…		…

$$Walsh(m\text{-}1, x)\,Walsh(0, y), \quad Walsh(m\text{-}1, x)\,Walsh(1, y), \ldots \quad , Walsh(m\text{-}1, x)\,Walsh(n\text{-}1, y)$$

The $m\times n$ two dimensional Walsh functions are generated altogether. For a digital image, according to the above method, we can obtain projection matrix of this digital image. The projection matrix has the same size with this digital image. Of course, if the digital image has bigger size, we can't use too many two dimensional Walsh functions. How much two dimensional Walsh functions are used, it should be decided according to actual situation.

3 Experiment Results and Discussion

In these experiments, we will investigate the robust detection problem of blind digital watermarking. Let us consider 512×512 grayscale images. Let Fig.1 be an original image. 1000 stochastic matrixes W_i (i=1, 2, …, 1000), their elements drawn from a zero-mean Gaussian distribution, are generated randomly. Among them, the W_{500} is a digital watermarking generated with the correct key, and otherwise generated with the incorrect key. Each W_i is a $m\times n$ matrix. Fig.2 is the watermarked image for embedding W_{500} into Fig.1 using multiplicative method, when ω =0.03.

Fig.1 The original image

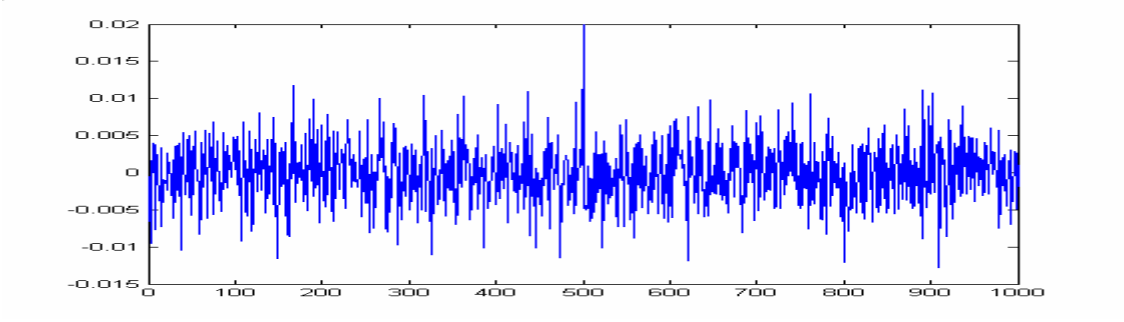
Fig.2 The watermarked image (ω =0.03)

3.1 Performance Test of Two kinds of Methods

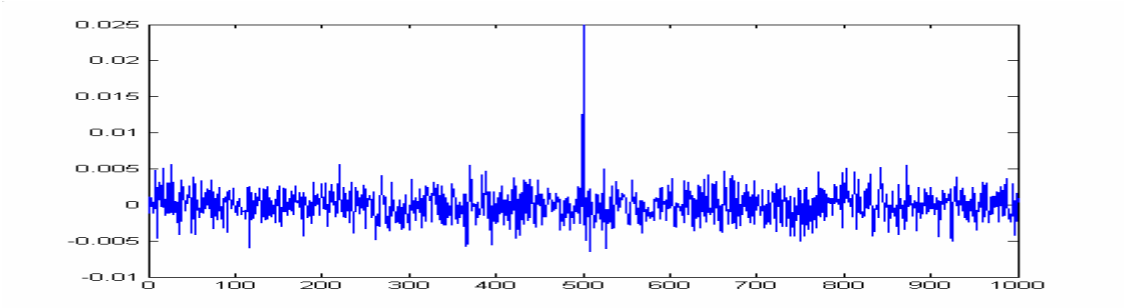
For watermarking detection problem, the normalized correlations are computed by the intensity information of digital image (called Detector 1) and orthogonal projection sequence (called Detector 2) of this image, respectively. For a digital image, the equation (2) is rewritten following as

$$\alpha_{ij} = \sum_{k=0}^{m-1}\sum_{l=0}^{n-1} I(k,l)Walsh(i,k)Walsh(j,l), \qquad i = 0,1,\ldots,m-1;\ \ j = 0,1,\ldots,n-1$$

Fig.3(a) is output result of Detector 1, and Fig.3(b) is output result of Detector 2. We notice that the peak values of two Detectors are created all at output position 500. Therefore, two detectors can detect the watermark successfully. However, by comparing, performance of Detector 2 is better than Detector 1's. Because the threshold value choice range of Detector 2 is bigger than the Detector 1's, which can guarantee the lower false alarm probability.



(a). Output result of Detector 1



(b). Output result of Detector 2

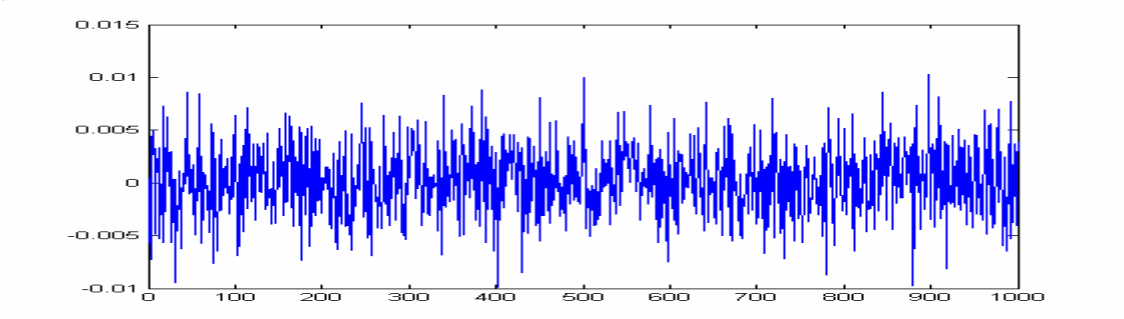
Fig.3. The comparison of the output results of two Detectors

3.2 Test of Anti-Noise Attack

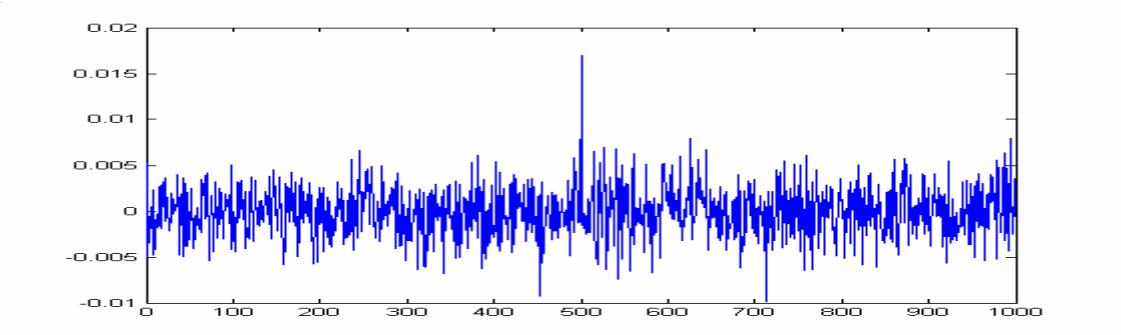
Fig.4(a) is result image generated by zero-mean Gaussian noise with variance 0.01 adding to Fig.2.

(a). The watermarked image attacked by the Gaussian noise

We detect W_{500} to Fig.4(a) to use two detectors respectively, and the Fig.4(b) and (c) are their output results.



(b). Output result of Detector 1



(c). Output result of Detector 2

Fig.4 The comparison of the output results of two Detectors

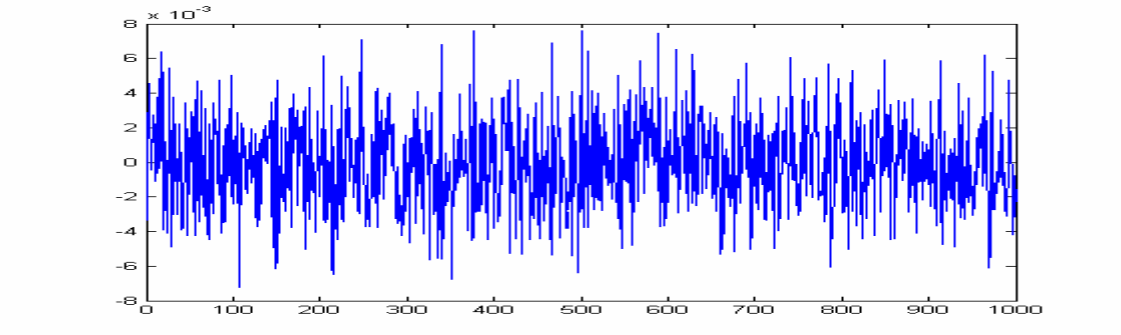
From the Fig.4(b) and (c) we know that Detector 1 can't detect W_{500} correctly, and Detector 2 can generate a higher the peak value in 500 position. This show that Detector 2 is not sensitive to noise, and it has the very strong anti-noise ability. This is because the projection characteristic of digital image is integral characteristic of this image, and integral calculus of digital image has the smooth function, therefore Detector 2 has the anti-noise attack ability.

3.3 Test of Anti-Rotation Attack

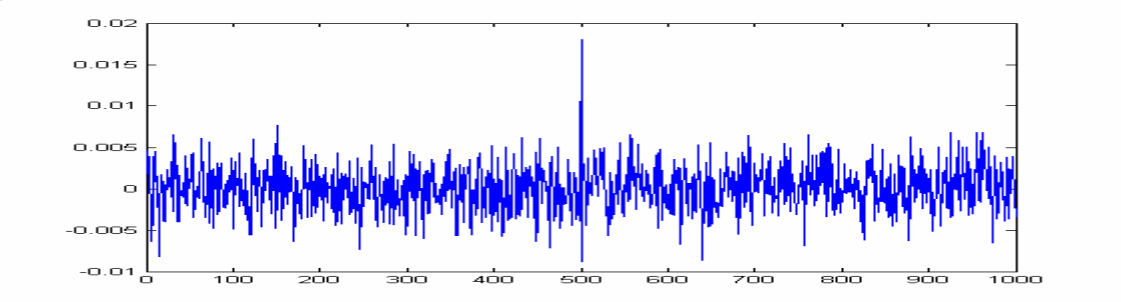
Fig.5(a) is a result image when Fig.2 is rotated 5 degrees.

(a). This is an image by rotating Fig.2 according to 5 degrees

We detect W_{500} to Fig.5(a) to use two detectors respectively, and the Fig.5(b) and (c) are their output results.



(b). Output result of Detector 1



(c). Output result of Detector 2

Fig.5 The comparison of the output results of two Detectors

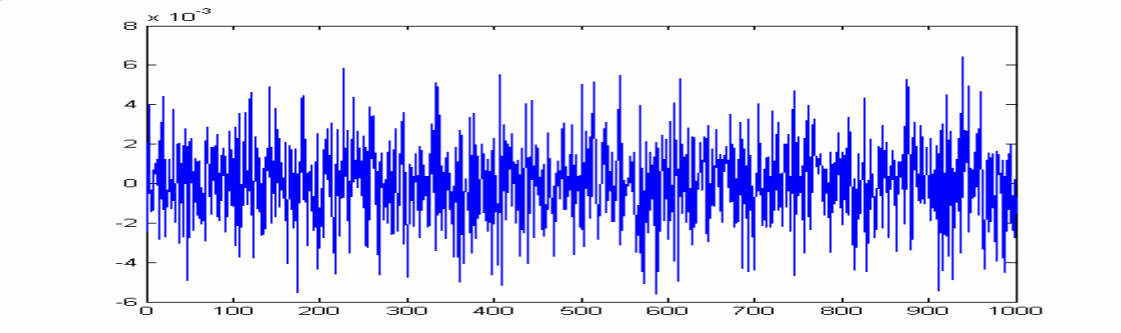
From the Fig.5(b) and (c) we know that Detector 1 can't detect W_{500} correctly, and Detector 2 can generate a higher the peak value in 500 position. This show that Detector 2 is not sensitive to rotation, it has the very strong anti-rotation ability. This is because the projection characteristic of digital image is internal characteristic of this image, and its existence don't depend on the pixel position. Therefore Detector 2 is not sensitive to rotation attack.

3.4 Test of Anti-Translation Attack

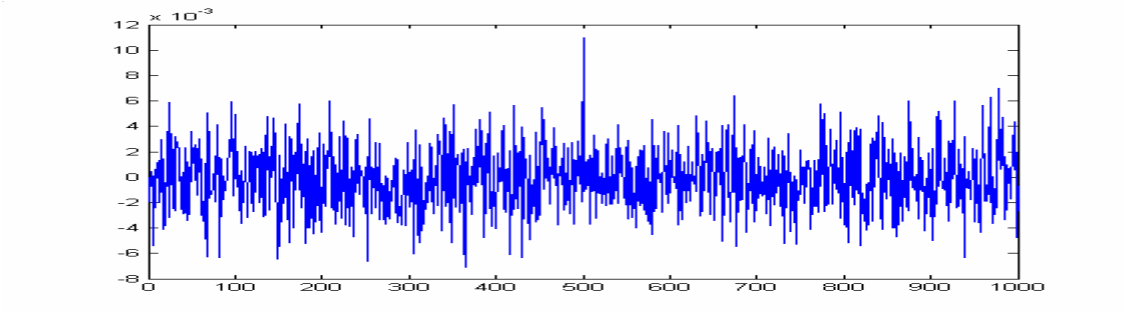
Fig.6(a) is a result image when Fig.2 is translated 3 pixel rightwards and downward respectively.

(a). This is an image which is obtained by translating Fig.2

We detect W_{500} to Fig.6(a) to use two detectors respectively, and the Fig.6(b) and (c) are their output results.



(b). Output result of Detector 1



(c). Output result of Detector 2

Fig.6 The comparison of the output results of two Detectors

From the Fig.6(b) and (c) we know that Detector 1 can't detect W_{500} correctly, are Detector 2 can generate a higher the peak value in 500 position. This show that Detector 2 is not sensitive to translation, it has the very strong anti-translation ability. Its reason is the same with Detector 2 has the very strong anti-rotation ability.

3.5 Test of Anti-Other Attack

For two detectors, the other attacks, such as filtering, JPEG compression *etc*, are tested. By these experiments we know that, for these attacks, two detectors can't detect W_{500} correctly. This show that performance of Detector 2 isn't more superior than Detector 1's in the aspects of resisting filtering and JPEG compression *etc*.

4 Conclusion

In this paper, the blind watermark detection is realized partly by orthogonal projection sequence of digital image. By experiment we find that the blind watermark detector, the normalized correlation value is calculated by orthogonal projection sequence of digital image, has the good robustness to Gaussian noise attack, rotation attack, and translation attack. It points out a new way for designing the better blind watermark detector.

References

[1] M.D. Swanson, M. Kobayashi, and A.H. Tewfik. "Multimedia data-embedding and watermarking technologies", *Proceedings of the IEEE*, 86(6), 1064-1087, June 1998.

[2] F. Hartung, and M. Kutter. "Multimedia watermarking techniques", *Proceedings of the IEEE*, 87(7), 1079-1107, July 1999.

[3] Stirmark Package, http://www.cl.com.uk/~fapp2/watermarking/stirmark

[4] Q. Sun, J. Wu, R. Deng. "Recovering modified watermarked image with reference to original image", *In Proceedings of SPIE: Security and Watermarking of Multimedia Contents*, (3657), Jan 1999, San Jose

[5] J.J.K.O Ruanaidh and T. Pun. "Rotation, scale and translation invariant spread spectrum digital image watermarking", *Signal Processing*, (66), 303-317, 1998.

[6] M. Alghoniemy, A. Tewfik. "Image watermarking by moment invariants", *In Proceedings of ICIP*, 2000.

[7] R. Caldelli, M. Barni, F. Bartolini, A. Piva. "Geometric-invariant robust watermarking through constellation matching in the frequency domain", *In Proceedings of ICIP*, 2000.

[8] J.S.F. Hartung, B. Girod. "Spread spectrum watermarking: Malicious attacks and counter-attacks", *In Proceedings of SPIE*: *Security and Watermarking of Multimedia Contents*, (3657), Jan 1999, San Jose

[9] M. K. Hu. "Visual Pattern Recognition by Moment Invariants". *IRE Trans. Information Theory*, IT-8, 1962, 179-187

[10] Ron N. Bracewell. *The Fourier Transform and Its Applications*, New York: McGraw-Hill Book Company, 1965.

[11] I.J.Cox., J.Killian, F.Thomson, and T.Shamoon. “Secure Spread Spectrum Watermarking for Multimedia”. *IEEE Transaction on Image Processing*, (6): 1673-1687, 1997.

[12] P. Moulin and E. Delp. “A mathematical approach to watermarking and data hiding”. In Proc. *IEEE ICIP* 2001, Thessaloniki, Greece, Oct. 2001.

[13] Tzafestas, S.G. *Walsh Functions in Signal and Systems Analysis and Design.* New York: Van Nostrand Reinhold, 1985.