Effects of Watermarking on Iris Recognition Performance

Jing Dong
National Lab of Pattern Recognition
Institute of Automation, Chinese Academy of Sciences
Beijing, China

Tieniu Tan
National Lab of Pattern Recognition
Institute of Automation, Chinese Academy of Sciences
Beijing, China

***Abstract*—Protection of biometric data and templates is a crucial issue for the security of biometric systems, and biometric watermarking is introduced for this purpose. However, watermarking introduces extra information into the biometric data (biometric images or biometric feature templates) which leads to certain image distortion. In addition, watermarked images are always subject to the risk of being attacked. Hence, whether and how biometric recognition performance will be affected by biometric watermarking deserves investigation. In this paper, we make a first attempt in such investigations by studying two application scenarios in the context of iris recognition, namely protection of iris templates by hiding them in cover images as watermarks (iris watermarks), and protection of iris images by watermarking them. Experimental results suggest that watermarking iris images does not introduce detectable decreases on iris recognition performance whereas recognition performance drops significantly if iris watermarks suffer from severe attacks.**

***Index Terms*—Biometrics, iris watermarking, iris recognition.**

I. Introduction

The increasing popularity of biometrics [1] offers personal identification systems greater security and convenience than traditional password-based identity authentication systems. Biometric-based personal identification techniques use physiological or behavioral characteristics of an individual (e.g. face, voice, fingerprint, gait, hand geometry, iris, gene, etc.) to establish automatic personal recognition or authentication. Since biometrics characteristics are inherently associated with a particular individual, making them uneasy to be stolen, forgotten, lost or attached, biometric techniques are promoted over worldwide utilization. However, the problem of ensuring the security and integrity of biometric data in networked environments is becoming urgent. Although standard encryption techniques are useful in many ways to assist the security enhancement of biometric systems, there still exist several new types of possible security issues. *Ratha et al.* [2] identified eight basic sources of attacks that are possible in a biometric system, including:

1) Fake biometric at the sensor;
2) Resubmission of old digitally stored biometrics signal (typical replay attack in voice recognition);
3) Override feature extraction;
4) Tampering with the feature representation in network environment;
5) Override matcher;
6) Tampering with stored templates in database;
7) Channel attack between stored templates and the matcher during biometric data or feature template transmission;
8) Decision level override.

Although liveness detection and cryptography techniques could help to prevent fake biometric attack and eliminate the attacks on biometric data exchange, the risk of stealing and tempering biometric information in and out of the biometric system still remains. Cryptography only focuses on methods to make the biometric information meaningless to attackers rather than conceal such information from perception. As we may known, the personal biometric data are usually easy to be collected in public activities. For example, one leaves his fingerprints on every surface he touched and his face image could be captured by every public camera or from his public photo gallery. Even iris image could be captured clearly under a special camera with a long focus lens and high resolution. If the transmission of biometric data is interrupted by the attackers and then tempered or replaced by another, the security of identification system would be compromised.

For the worldwide promotion of networked biometric applications and the security enhancement of biometric systems, security enhancement solutions with introduction of data hiding techniques (e.g. steganography and watermarking) are proposed recently. The goal of steganography is for secret communication by hiding critical information in unsuspected carrier signal. Digital watermarking is a well known technique used to embed proprietary information for multimedia digital rights protection and content tempering authentication. Since watermarking is always regarded as a subset of steganography, watermarking can either be introduced to embed secret biometric data into host signal without suspicion during transmission (hence protect the biometric data), or they can be used for biometric image authentication by embedding ownership information as well as integrity information for database source tracking and biometric image tempering detection. Although watermarking could ensure biometric data protection, the watermarking embedding process would directly cause some image distortions by making certain changes of image pixels for watermark embedding. As biometric recognition system requires only small variations between the input biometric data and registered templates for an successful matching from

978–1–4244–2287–6/08/$25.00

the same person (regardless the data being watermarked or not). Hence, questions of image distortion by data embedding and the effects of watermarking on biometric recognition performance (even after regular watermarking attacks) become critical and deserve further studies. Despite the practical importance of such issues, little has been done. In this paper, we attempt to fill this gap by investigating the effects of watermarking on biometric recognition, especially on iris recognition performance. We consider two application scenarios of iris data protection by means of watermarking. That is, the protection of iris templates by hiding them in cover images as watermarks (iris watermarks), and protection of iris images by watermarking them.

The paper is organized as follows. Section II contains an introduction to iris watermarking application scenarios and studies the effects introduced by these watermarking applications on iris recognition performance. In Section III, we carry out a number of experiments under the two scenarios and make analysis on the experimental results. Discussions and conclusions are presented in Section IV.

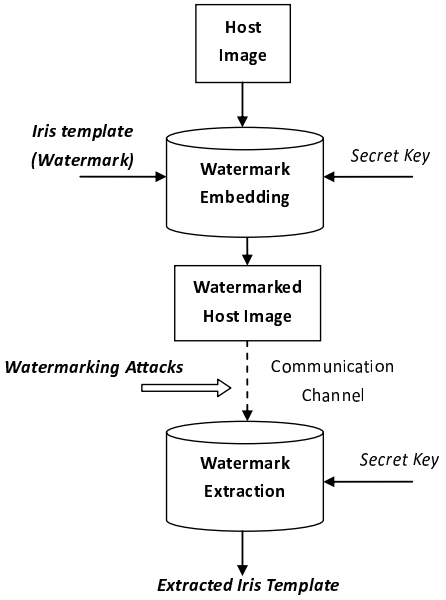


Fig. 1. Diagrams of the application scenario of using iris template as watermark for securing iris template transmission.

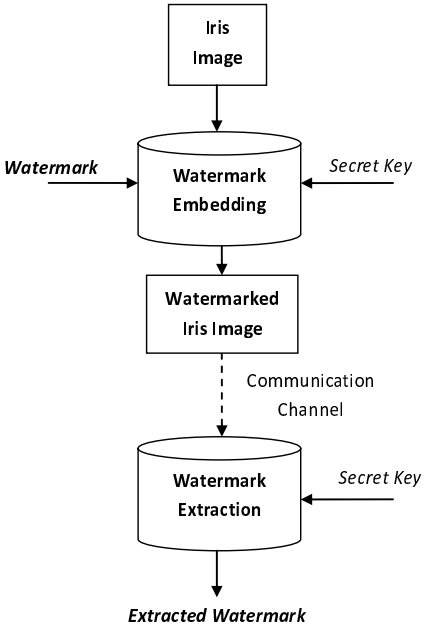


Fig. 2. Diagrams of the application scenario of watermarking iris images for its ownership protection and content authentication.

II. Iris Watermarking

A. Related Work

Digital watermarking [3], or simply watermarking, is defined as embedding imperceptible information (named as watermark) of multimedia data in the host signal. Watermarking, when complemented with encryption, has been demonstrated to be very useful and serves for many purposes, for example, copyright protection, broadcast monitoring, tempering detection and data authentication. According to embedding domain, watermarking techniques can be categorized as spatial domain watermarking techniques [4] and transform domain watermarking [5] [6]. According to embedding purposes, watermarks can be categorized into three types: robust, fragile, and semi-fragile. Robust watermarks [4] are designed to withstand arbitrarily malicious attacks and usually used for copyright protection to declare the rightful ownership. Fragile watermarks [7] are adopted to detect any unauthorized modification for the purpose of authentication. Semi-fragile watermarks [8] are designed for detecting any unauthorized modification, ant at the same time allowing some image processing operations.

In the past few years, several researchers made attempts on biometric data protection with the help of watermarking techniques. *Ratha et al.* [9] proposed a data embedding method, which is applicable to fingerprint images compressed with WSQ wavelet-based scheme. *Pankanti and Yeung* [10] proposed a fragile watermarking method for fingerprint image tampering detection. A watermark image is embedded in the fingerprint image by utilizing a verification key. Their method can locate regions of the image that have been maliciously tampered. They also made some analysis about their watermarking technique about performance loss in fingerprint verification. In the work of [11] [12], two applications of fingerprint watermarking method are presented by *Jain et al*. The first application is related to increasing the security of biometric data exchange, by hiding several fingerprint minutiae data on biometric images. However, only limited hidden data are reported in their experiments. In the second application they authenticate a user based on his face image, along with the fingerprint information hidden in the face image. The data decoding performance in the case of JPEG compression and cropping attacks on host images is

also analyzed. In their second application, the embedding rates are low and only two slight watermarking attacks are studied.

B. Application Scenarios

Since there are only few works about biometric data protection by watermarking and they only focus on fingerprint data, no revelent research about iris data protection has been reported yet to the best of our knowledge. Inspired by the work of fingerprint watermarking, in this paper, we make a first attempt to investigate applications about iris watermarking and make some analysis on the influences which caused by watermarking applications to iris recognition performance. There are two application scenarios about iris watermarking. The first is taking iris template as watermark (see Fig. 1) and the other is watermarking iris images (see Fig. 2). The first application is actually evoked by secure iris template transmission between the central database and local iris matcher. The basic idea of this application is to embed iris template (feature set for iris recognition) in host images using watermarking algorithms. The iris templates are regarded as watermarks in this scenario. The host image could be any image available to the encoder with certain capacity since its only function is to carry the embedded data. As a result, the watermarked images are sent to the communication channel which also could suffer from certain watermarking attacks during the transmission. However, as the watermarking attacks can directly cause the distortion of host images and also affect the embedded iris templates, the embedded iris watermarks can be changed to some extent after being extracted. The second application aims at iris database ownership protection as well as iris image tempering detection. The iris database owner could embed proprietary information into iris images using either robust watermarking fragile watermarking. However, whatever watermarking algorithm is taken, the distortion of iris image itself caused by watermark embedding is there. Consequently the corresponding distortion would also be introduced to the iris features, which are generated from iris images for recognition.

Hence, whatever application scenario is taken, variations of iris data either by watermarking attacks or by watermarking embedding process will be introduced. Truly, the impacts brought by watermark embedding and watermarking attacks would be diverse by different watermarking algorithms and different watermarking attacks. However, whether and how these impacts will affect iris recognition accuracy deserves investigation. As we all know, there is an important module in iris recognition called iris matching. During the matching process, the input iris data (usually a feature set extracted from iris image) are required to compare with all the registered iris templates. If the matching score between input template A and registered template B is higher than certain threshold T, A and B are identified from the same eye. Hence, if the variation caused by iris watermarking is within the range of certain threshold, it would not significantly affect the iris recognition performance, and vice versa. Whether and how the recognition performance is affected by watermarking embedding or attacks deserves studies. In the rest of this paper, we investigate the influence introduced by iris watermarking and make some analysis of their effects on iris recognition performance respectively.

C. Watermarking Algorithm

We consider the quantization index modulation (QIM) method proposed by *Chen et al.* [13] as the watermarking algorithm in both application scenarios. The QIM watermarking algorithm is a well known watermarking algorithm and it is based on dither modulation and uniform scalar quantization. This watermarking algorithm could achieve provably better rate-distortion-robustness trade-offs than previously proposed classes of watermarking methods such as spread spectrum and low-bit(s) modulation against worst-case square-error distortion-constrained intentional attacks, which may be encountered in a number of copyright, authentication, and covert communication multimedia applications. There are two important parameters in the QIM embedding scheme. The watermark embedding rate depends on a threshold t and the choice of quantization step q would affect on watermarked image distortion intensity. The smaller the t is, the higher the embedding rate. The larger the q is, the worse the distortion. Both of the parameters can result in a change of PSNR (peak signal-to-noise ratio of image), which is usually considered as an important performance index of watermarking algorithm. Basically, the security of iris watermarking and the robustness of iris watermark depends on the security and robustness of the watermarking algorithm. However in this paper, our main purpose is to study the effects of watermarking applications on iris recognition in general means rather than to compare which watermarking algorithm is better for iris watermarking. Hence, the QIM embedding algorithm is employed in our study.

III. Experimental Results

A. Database

We run all our experiments on the difficult *ICE-Right* iris database [14], [15]. The ICE v1.0 is released by the National Institute of Standards and Technology (NIST) for "Iris Challenge Evaluation" in 2005. It includes two subsets: ICE-Left and ICE-Right. ICE-Left contains 1527 iris images from 119 left eyes while ICE-Right contains 1426 iris images from 124 right eyes. Most of the subjects are occidental, and some of its images are of poor quality due to de-focus, occluded by eyelids, interlace corrupted and oblique view-angle. All images from our database are 8-bit intensity images with a resolution of 640×480.

Also, in our experiments the ordinal measure (OM) filters [16] are adopted to encode the iris texture from the database as templates (feature set) for iris recognition.

B. Effect of Iris Watermark Attacks on Iris Recognition

In this experiment, we consider iris templates as watermarks and embed them to natural images. We use the 'Lena' image (256×256) as the host image and generate 1426 iris templates from our database using the feature extraction algorithm of [17] as watermarks. Each of the watermarks is with the size of 1K bits. During the watermark encoding process, we utilize the QIM watermarking algorithm [13]with t = 0.5 and q = 35 to embed iris watermarks. Under watermarking encoding process, iris watermark with the size of 1KB is entirely embedded into each 'Lena' image with the average PSNR larger than 37. Then we get 1426 watermarked 'Lena' images. Next, we utilize the following eleven types of watermarking attacks on these watermarked host images separately and form totally 11 groups of attacked watermarked images:

#1: Scaling with factor = 2;
#2: Scaling with factor = 4;
#3: Scaling with factor = 0.25;
#4: Scaling with factor = 0.5;
#5: Spatial low-pass filtering with size 3×3;
#6: Median filtering with size 3×3;
#7: Median filtering with size 1×3;
#8: Cropping 10%;
#9: Cropping 25%;
#10: Gaussian noise with N=0.0005;
#11: JPEG compression with quality factor 50%;

During watermark decoding process, we extracted the iris watermarks from the 11 groups of attacked 'Lena' images and get 11 sets of attacked iris watermarks. Then the changed rates by bits between each of iris watermarks before and after being attacked are calculated and listed in Tab. I. Moreover, biometric recognition performance is usually measured by generating receiver operating characteristic (ROC) curves. The ROC curves plot the tradeoff between false accept rate(FAR) and false reject rate (FRR). It is common to list specific points on such tradeoff curves, such as the FRR when decision threshold causes an FAR of 10^{-3} and the point at which the two error rates are equal (FRR = FAR = EER,the equal error rate). The obtained ROC curves of tests on iris recognition performance before and after corresponding attacks are shown in Fig. 3 and the values of EER and FRR when FAR fixed to 10^{-3} are listed in Tab. I.

From Tab. I and Fig. 3, we notice the watermarking attacks #1, #2 and #10 do not significantly affect the performance of iris recognition. Also, these three attacks produce lower error rates between the watermarks before and after being attacked compared with other kinds of attacks (only 5.32%, 6.51% and 12.58% respectively). Moreover, for those attacks which produce a severe error on the extracted watermark data after being attacked, for example, the median filtering attacks, the

TABLE I
EFFECT OF WATERMARKING ATTACKS ON IRIS WATERMARKS FOR RECOGNITION PERFORMANCE

Attacks	**Avg. changed rate before and after attacks(%)**	**EER**	**FRR @ FAR = 10^{-3}**
#1	5.32	0.0051	0.0048
#2	6.51	0.0068	0.0071
#3	19.95	0.0692	0.105
#4	37.14	0.0735	0.110
#5	52.37	0.0702	0.107
#6	41.00	0.0753	0.121
#7	36.59	0.0761	0.120
#8	36.47	0.0617	0.103
#9	44.75	0.0725	0.109
#10	12.58	0.0038	0.004
#11	20.26	0.0180	0.043
Baseline	0	0.0023	0.0025

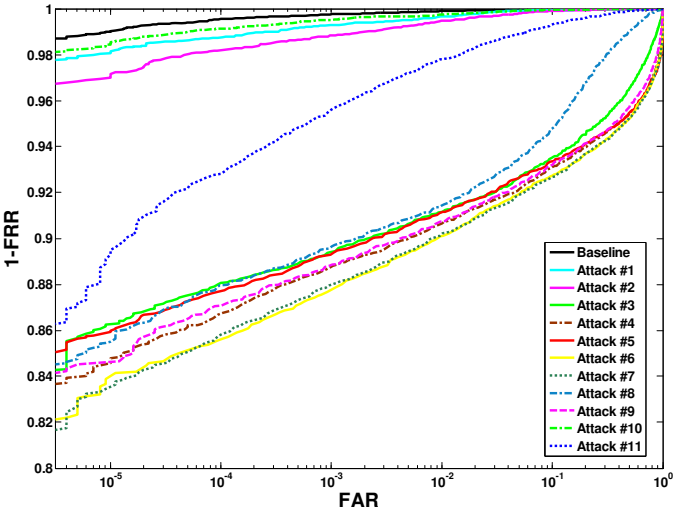


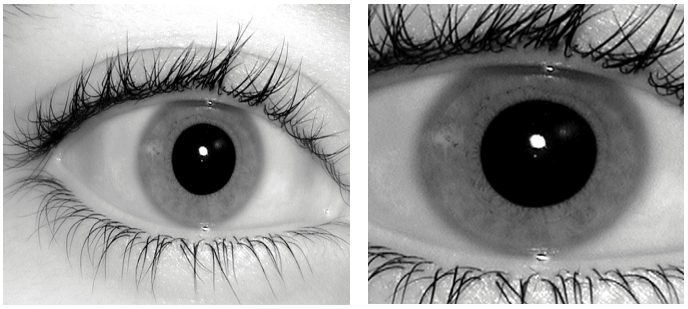
Fig. 3. The obtained ROC curves of tests on recognition performances before (black curve) and after the 11 kinds of attacks on NIST ICE-Right iris database.

recognition accuracy drops significantly on the ROC curves. These results are also consistent with the performance of most watermarking algorithms, which are not very robust to the filtering attacks, as well as some cropping attacks. Clearly, if the robustness of watermarking algorithm improves, so dose the recognition accuracy of the extracted iris templates.

C. Effect of Watermarking Iris Images on Iris Recognition

In this experiment, we embed data into iris images. We again use the QIM watermarking algorithm to embed watermarks (here are randomly generated bit streams) into all 1426 iris images from our database. In order to see the effect of watermark embedding on iris data rather than on other areas of eye images of our database, we preprocess all images and generate from each one a new cropped image of 320×320 pixels with the iris centered in it, as shown in Fig. 4.

As we mentioned, there are two parameters in the QIM watermarking algorithm. Parameter t is responsible for embedding capacity while parameter q determines the



(a) (b)

Fig. 4. (a) A sample iris image with a resolution of 640 × 480 from NIST ICE-right database. (b)Cropped 320 × 320 pixels for watermarking of the sample iris image.

TABLE II
WATERMARK EMBEDDING CAPACITY AND THE CORRESPONDING PSNR OF EACH GALLERY GENERATED UNDER THE 8 PAIRS OF WATERMARKING PARAMETERS, ALONG WITH THEIR EER AND FRR FROM THE ROC CURVES.

(*t*, *q*)	Avg. Embedding rate	Avg. PSNR	EER	FRR @ FAR = 10^{-3}
(0.1, 22)	0.98 *bpp*	37.25	0.0305	0.0037
(0.1, 15)	0.98 *bpp*	40.47	0.0208	0.0031
(0.1, 8)	0.98 *bpp*	45.83	0.0229	0.0025
(0.1, 3)	0.98 *bpp*	53.94	0.0210	0.0025
(0.3, 10)	0.88 *bpp*	44.02	0.0024	0.0028
(1, 10)	0.72 *bpp*	44.42	0.0024	0.0029
(5, 10)	0.42 *bpp*	42.78	0.0017	0.0023
(9, 10)	0.24 *bpp*	50.39	0.0019	0.0024
Baseline	0 *bpp*	N/A	0.0021	0.0024

embedding intensity. The PSNR of a watermarked image would be altered by the change of each parameter. In our experiments, we choose totally 8 pairs of parameters for watermark embedding and the value of these parameters are listed in Tab.II along with their embedding rates and PSNRs by average of each gallery. These pairs of parameters could reflect the different effects of embedding rate and embedding intensity on iris recognition performance, see Fig. 5 and Fig. 6 respectively. The obtained ROC curves and tabulations are presented in Fig. 5 and Fig. 6, along with their EER and FAR in Tab. II.

The black ROC curve in both Fig. 5 and Fig. 6 is the baseline, which is the original ROC curves generated from the un-watermarked database. The blue, green, mauve and red ROC curves in Fig. 5 show recognition performance of the first four tests with a fixed embedding parameter$t$. Almost no recognition performance loss relative to the baseline (black) ROC curve is detectable by the four watermark embedding schemes. Indeed there is even a small benefit from watermark embedding, shown in blue and red ROC curves. The mauve ROC curves show that under a sever watermarking embedding process (with embedding rate 0.98 *bpp* and PSNR 37.25 by average), only 0.13 % recognition performance decrease in terms of FRR and about 3% decrease in terms of EER are produced. A similar observation is obtained in Fig. 6,

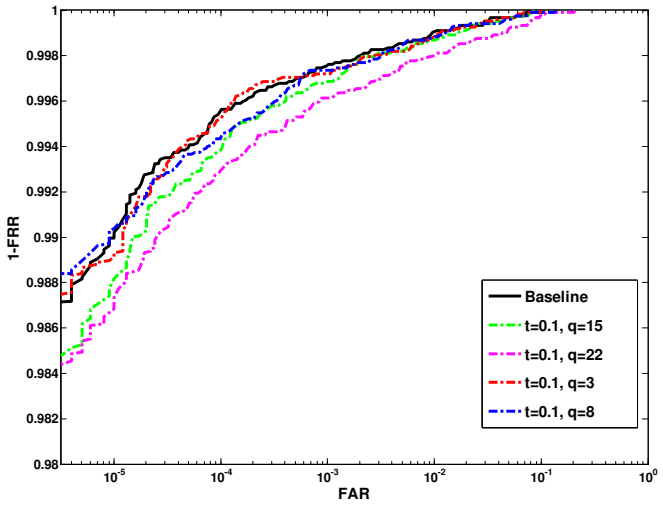


Fig. 5. The ROC curves for iris recognition by watermarking iris images with a fixed embedding threshold t and four different quantization steps q.

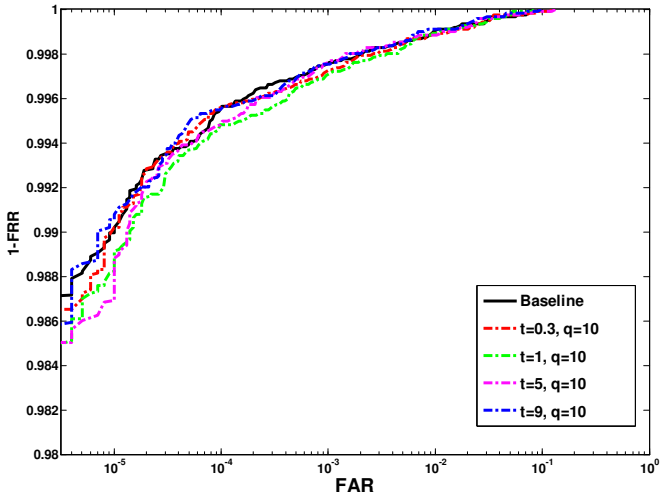


Fig. 6. The obtained ROC curves for iris recognition by watermarking iris images with a fixed quantization step q and four different embedding thresholds t.

in which the blue,green, mauve and red ROC curves show recognition performance of the last four tests with a fixed embedding quantization step q. Almost no significant loss of the recognition performance is noticed in terms of EER as well as FRR. The small benefit for recognition performance may be introduced by the embedding process, which happens to serve as denoising process for iris template generation.

IV. CONCLUSION

In this paper, we have studied the effects on iris recognition performance of iris watermarking. Using iris template as watermark ensures the iris template transmission while watermarking iris images could help to protect the database ownership as well as to detect iris image tempering. However, the influence of watermarking attacks to iris watermark and the influence of watermarking embedding in iris image are

different for iris recognition performance. In the first scenario, the watermarking attacks which lead to severe changes to iris watermarks cause a decrease on recognition performance. However, the attacks which the embedding algorithm is robust to would not significantly affect recognition performance. The watermark embedding in the second scenario hardly affects iris recognition performance.

The work presented in this paper is just a preliminary but desirable study about iris recognition aiming at the analysis of what effects will be introduced by iris watermarking applications. Although not all circumstances are investigated in this paper, the obtained experimental results have shown that the effect of watermark embedding to iris images does not bring a significant decrease of iris recognition performance, which provides a reasonable suggestion to promote the iris watermarking application in this scenario. The effects of watermarking attacks to iris templates as watermarks could still maintain a reasonable recognition accuracy as long as the watermark extraction accuracy is high enough. Besides, for those attacks which most robust watermarking algorithm could not conquer yet, our results are also negative. Moreover, in order to avoid the suspicion of watermarking attacks on iris template transmission, we still could consider using steganography to conceal the iris template during transmission.

ACKNOWLEDGMENT

The authors would like to thank *Prof. Ying Wang* and *Dr. Jun Xiao* for sharing their implementation of QIM watermarking algorithm. They also acknowledge *Zhaofeng He* and *Wenting Chao* for their assistance and helpful discussions.

REFERENCES

[1] A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal identification in networked society," *Norwell, MA: Kluwer*, 1999.

[2] N. Ratha, J. Connell, and R. Bolle, "An analysis of minutiae matching strength," *Proc. Third Intl. Conf. Audio- and Video-Based Biometric Person Authentication*, pp. 223–228, June 2001.

[3] I. Cox and M. Miller, "A review of watermarking and the importance of perceptual watermarking," *Proceedings of Electronic Imaging*, 1997.

[4] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Processing*, vol. 66(3), p. 385C403, 1998.

[5] J. Huang and Y. Shi, "Embedding image watermarks in dc components," *IEEE Trans. CSVT 10 (6)*, p. 974C979, 2000.

[6] I. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process 6 (12)*, p. 1673C1687, 1997.

[7] G. Caronni, "Assuring ownership rights for digital images," *Proceedings of Reliable IT Systems,VIS95*, p. 251C263, 1995.

[8] Q. Sun and S. Chang, "Semi-fragile image authentication using generic wavelet domain features and ecc," *Proceedings of IEEE International Conference on Image Processing*, p. 901C904, 2002.

[9] N. Ratha, J. Connell, and R. Bolle, "Secure data hiding in wavelet compressed fingerprint images," *Proc. ACM Multimedia*, pp. 127–130, 2000.

[10] S.Yang and I. Verbauwhede, "Secure fuzzy vault based fingerprint verification system," *13th Asilomar Conference on Signals, Systems, and Computers*, vol. 1, p. 577C581, 2004.

[11] A.K.Jain and U.Uludag, "Hiding biomtric data," *IEEE Trans. on Pattern analysis and machine intelligence*, vol. 25, no. 11, pp. 1494–1498, 2003.

[12] A. Jain and U. Uludag, "Hiding fingerprint minutiae in images," *Workshop on Automatic Identification Advanced Technologies*, pp. 97–102, 2002.

[13] B. Chen and G. W. Wornell, "Quantization index modulation methods for digital watermarking and information embedding of multimedia," *Journal of VLSI Signal Processing 27*, p. 7C33, 2001.

[14] "Iris challenge evaluation (ice)," *http://iris.nist.gov/ICE/*.

[15] X. M. Liu, K. W. Bowyer, and P. J. Flynn, "Experiments with an improved iris segmentation algorithm," *Proc. Fourth IEEE Workshop Automatic Identification Advanced Technologies (AutoID)*, 2005.

[16] Z. Sun, T. Tan, and Y. Wang, "Robust encoding of local ordinal measures: A general framework of iris recognition," *Proc. ECCV2004 Int'l Workshop Biometric Authentication*, pp. 270–282, 2004.

[17] J. Daugman, "How iris recognition works," *IEEE Trans. Circuits Syst. Video Technol*, vol. 14, no. 1, p. 21C30, 2004.