Iris Authentication Using Privatized Advanced Correlation Filter

Siew Chin Chong, Andrew Beng Jin Teoh, and David Chek Ling Ngo

Faculty of Information Science and Technology (FIST), Multimedia University,
Jalan Ayer Keroh Lama, Bukit Beruang, Melaka 75450, Malaysia
{chong.siew.chin, bjteoh, david.ngo}@mmu.edu.my

Abstract. This paper proposes a private biometrics formulation which is based on the concealment of random kernel and the iris images to synthesize a minimum average correlation energy (MACE) filter for iris authentication. Specifically, we multiply training images with the user-specific random kernel in frequency domain before biometric filter is created. The objective of the proposed method is to provide private biometrics realization in iris authentication in which biometric template can be reissued once it was compromised. Meanwhile, the proposed method is able to decrease the computational load, due to the filter size reduction. It also improves the authentication rate significantly compare to the advance correlation based approach [5][6] and comparable to the Daugmant's Iris Code [1].

1 Introduction

Nowadays, security is in critical demand of finding reliable and cost-effective alternatives to passwords, ID cards or PIN due to the increasing of financial losses from computer-based fraud such as computer hacking and identity theft. Biometric solutions address these fundamental problems due to the fact that the biometric data is unique and cannot be transferred. However, the traditional biometrics system does not completely solve the security concerns. One critical issue is the cancelability or replaceability of the biometric template once it is compromised by an attacker.

Some authors like Bolle et. al. [2] and Davida et al. [3] have introduced the terms cancelable biometrics and private biometrics to rectify this issue. These terms are used to denote biometrics data that can be cancelled and replaced, as well as is unique to every application. The cancelability issue of biometrics was also addressed by Andrew et al. [4]. They introduced the freshness into the authenticator via a randomized token. The revocation process is essentially the inner-product of a tokenized pseudo-random pattern and the biometrics information iteratively. Most recently, Savvides et al. [5] proposed a cancelable biometrics scheme which encrypted the training images used to synthesize the correlation filter for biometrics authentication. They demonstrated that convolving the training images with any random convolution kernel prior to building the biometric filter does not change the resulting correlation output peak-to-sidelobe ratios, thus preserving the authentication performance. In other word, their work does not show any improvement in terms of performance.

D. Zhang and A.K. Jain (Eds.): ICB 2006, LNCS 3832, pp. 382 – 388, 2005.

In this paper we propose a private or cancelable biometric formulation method based on Savvides et al. advance correlation filter formulation. We multiply training images with the user-specific random kernel in frequency domain instead of convolving the training images with random kernel in spatial domain that done by Savvides et al. The objectives of the proposed method are three fold: to provide private biometrics realization in iris authentication in which biometric template can be reissued by replacing the random kernel if it was compromised. Secondly, it helps to decrease the computational load during the enrollment as filter size is greatly reduced. In terms of authentication rate, the proposed method shows better performance than the advance correlation based approach.

The outline of the paper is organized as follow: Section 2 briefly explains MACE filter. Section 3 introduces the proposed method. Experiments and results are reported in Section 4. Conclusion is presented in Section 5.

2 Overview of Minimum Average Correlation Energy (MACE) Filter

Kumar et al [6] [7] has proposed many types of advanced correlation filters for biometrics authentication purpose. Minimum average correlation energy (MACE) filter is one of the advanced correlation filters. MACE is designed such as correlation function levels at all points can be reduced except at the origin of the correlation plane and thereby obtained a very sharp correlation peak [8].

During the enrollment stage, multiple training images are being used to form a MACE filter. Let $\mathbf{D}_i$ be a d x d diagonal matrix containing the power spectrum of training image i along its diagonal, and let diagonal matrix $\mathbf{D}$ be the average of all $\mathbf{D}_i$. Also, $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N]$ is a d x N matrix with N training image vectors, $\mathbf{x}$ as its columns. MACE filter is given as follows:

$$\mathbf{h} = \mathbf{D}^{-1}\mathbf{X}(\mathbf{X}^{+}\mathbf{D}^{-1}\mathbf{X})^{-1}\mathbf{u} \tag{1}$$

In general, $\mathbf{u} = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N]^T$ and $\mathbf{u}_i$ is user defined. All $\mathbf{u}_i$ belonging to an authentic class are set to 1; otherwise they are set to 0. The superscript + denotes the complex conjugate transpose. On the other hand, the test image will be cross-correlated with the MACE filter to produce the correlation output in the authentication stage.

3 The Proposed Method

During the enrollment phase, we multiply normalized iris training images, $\mathbf{x}$ with the user-specific random kernel, $\mathbf{R}$ in the frequency domain before biometric filter is created:

$$\mathbf{e}(\mathbf{x}, \mathbf{R}) = \mathbf{R}_{dm}^{T}\mathbf{x}_d \quad \text{where } m < d \tag{2}$$

where d is the original template size and m is the size after the concealment. The concealed patterns are used to synthesize a minimum average correlation energy (MACE) filter. Meanwhile, for the authentication stage, a testing iris image with its

associated random kernel will be also gone through the concealment operation to generate the concealed iris pattern and will then convolute with the trained MACE filter to produce a correlation output. Fig.1 shows the idea of the proposed method.

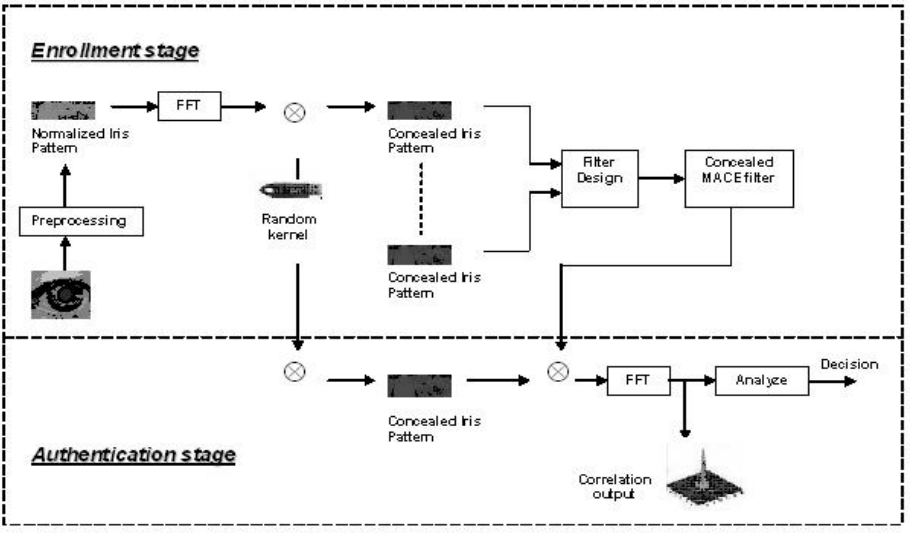


Fig. 1. Block diagram of the proposed method

In practice, random kernel can be generated from a physical device, for example smartcard or USB token. There is a seed which stores in USB token or smartcard microprocessor to generate **R** using a random number generator. Different user will have different seeds for different applications and these seeds are recorded during the enrollment process. A lot of pseudo-random bit/number algorithms are publicly available, such as ANSI X9.17 generator or Micali-Schnorr pseudo-random bit generator [9].

The process flow of the enrollment phase is as follow:

1) Perform Fast Fourier transform (FFT) to each normalized iris patterns, $I \in \Re^{d_1 \times d_2}$.
2) Convert each of the FFTed iris patterns into the column vector, **x** with dimension d (d_1 x d_2) through column-stacking.
3) Then, multiply **x** with random kernel, **R**, thus $\mathbf{e}(\mathbf{x}, \mathbf{R}) = \mathbf{R}_{dm}^{T}\mathbf{x}_d$, where $m \leq d$.
4) Then $\mathbf{E} = [\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_N]$ will be used to synthesize the MACE filter as follow:

$$\mathbf{h} = \mathbf{D}^{-1}\mathbf{E}(\mathbf{E}^{+}\mathbf{D}^{-1}\mathbf{E})^{-1}\mathbf{u} \tag{3}$$

where **D** is a m_1 x m_2 diagonal matrix containing the average power spectrum of all the training images along its diagonal. Also, $\mathbf{u} = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N]^T$ is a N x 1 column vector containing the desired peak values for N training images. The resulting **h** is a column vector with m entries that need to be re-ordered into matrix to form the MACE filter.

From the above description, a concealed iris size, **e** is either equal or less than the **x** original iris template, $m \leq d$; hence the MACE filter size can be greatly trimmed down if m is small. This helps increase the computation speed, especially the calculation of inversion matrix **D** in eq(3).

In order to ascertain how similar a test image to a MACE filter, a corresponding metric is needed. Kumar [6] suggested the Peak-to-Sidelobe Ratio (PSR) as a "summary" of the information in each correlation plane. Thus, the PSR is used to evaluate the degree of similarity of correlation planes. The PSR is defined as follows:

$$PSR = \frac{mean(mask) - mean(sidelobe)}{\sigma(sidelobe)} \tag{4}$$

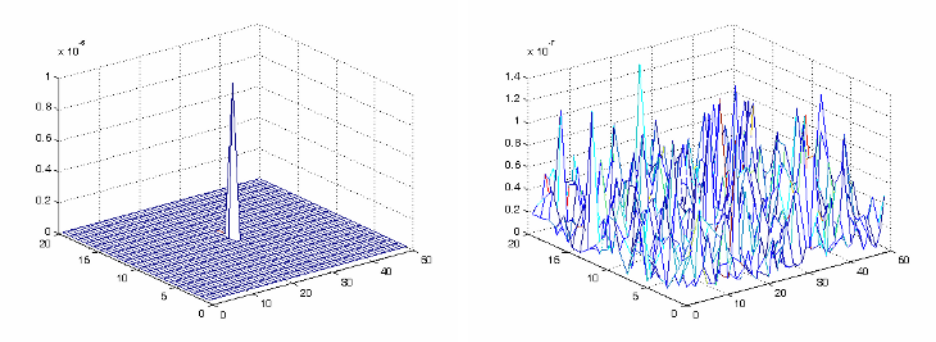
First, the correlation peak is located and the mean value of the central mask (e.g., of size 3 x 3) centered at the peak is determined. The sidelobe region is the annular region between the central mask and a larger square (e.g., of size 10 x 10), also centered at the peak. The mean and standard deviation of the sidelobe are calculated.

4 Experimental Results

The experiments were conducted by using Chinese Academy of Sciences-Institute of Automation (CASIA) Iris image database [10], which consists of 756 grey scale eye images with i=108 individuals and 7 images each. In the experiment, 3 images of each person are randomly selected as training images while other j=4 images are used as testing images. For the False Accept Rate (FAR) test and imposter population distribution, the specific MACE filter of each iris is cross-correlated against all other testing iris images, leading to 46224 imposter attempts $(((i-1)\times j)\times i)$. For the False Reject Rate (FRR) test and genuine population distribution, the specific MACE filter of each iris is cross-correlated against all images of the same iris, leading to 432 genuine attempts $(i \times j)$.

In the experiment, the performance of MACE, the proposed method (RMACE) and Daugmant's Iris Code. (For a detailed study of Daugman's Iris Code see [1]) are examined. During the authentication phase, the filter is cross-correlated with the testing images to generate correlation outputs which will be used for calculating the PSR. Fig. 2 shows the correlation plane of RMACE-20x50, from a person during the authentication phase. As demonstrated by the figure, the correlation output will exhibit a sharp peak for authentics but no such peak for imposters.

As illustrated in Fig. 3 and Table 1, the performance of the original and the proposed method are tested. The proposed method, RMACE is tested with different size of m. For the original MACE filter, its original size is 20x240 and the EER achieved is 14.78%. If compare to RMACE, the authentication of RMACE-m where m = 20x20, 20x40 and 20x50 are far better than MACE. The best authentication rate can attained from RMACE-20x50 in which the EER is 0.0726%. For Daugman's Iris Code, we can see that the EER achieved is 0.43% which is better than MACE but poorer than RMACE-20x50.



(a) (b)

Fig. 2. Correlation plane of RMACE-1000 of a person: (a) Genuine class (b) Imposter class

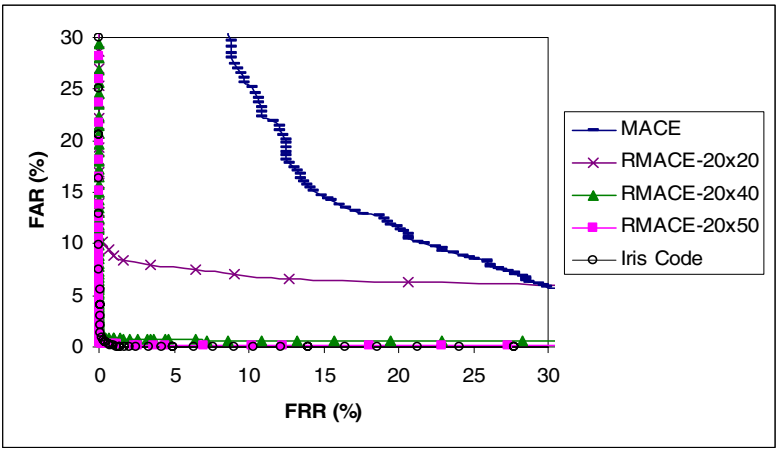


Fig. 3. Receiver operating curve for MACE, RMACE and Iris Code

Table 1. Performance evaluation of genuine class and imposter class of CASIA Iris Image Database using MACE and RMACE tested on different size of concealed template

Method	Concealed template size, *m*	FAR (%)	FAR (%)	EER (%)
MACE	20x240 (=4800)	14.7456	14.8148	14.7802
RMACE	20x20 (=400)	7.4831	6.4815	6.9823
	20x40 (=800)	0.8589	0.9259	0.8924
	20x50 (=1000)	0.0715	0.0729	0.0722
Iris Code	2048 bit binary code	0.4253	0.4409	0.4331

In addition, from the result obtained, it is obviously that the size of the iris templates is greatly reduced if compared to the original MACE methodology and Daugman's Iris Code. MACE's template has 20x240 and Iris Code's template has 2048 bit binary code whereas RMACE can provide the best EER with size 20x50. Among these three methods, our proposed method is able to generate the best EER with smaller template size. Intuitively, smaller size is less accurate in performing authentication task. However, our proposed method shows that the size reduction does not weaken the accuracy in authentication task but somehow improve the authentication rate. Meanwhile, the size reduction also helps to reduce the computational load.

Fig. 4 shows the PSRs of RMACE-20x50 for the first 400 comparisons of genuine and imposter class. A clear separation is found between the genuine and the imposter plots. This implies that RMACE can recognize the genuine and imposter perfectly.

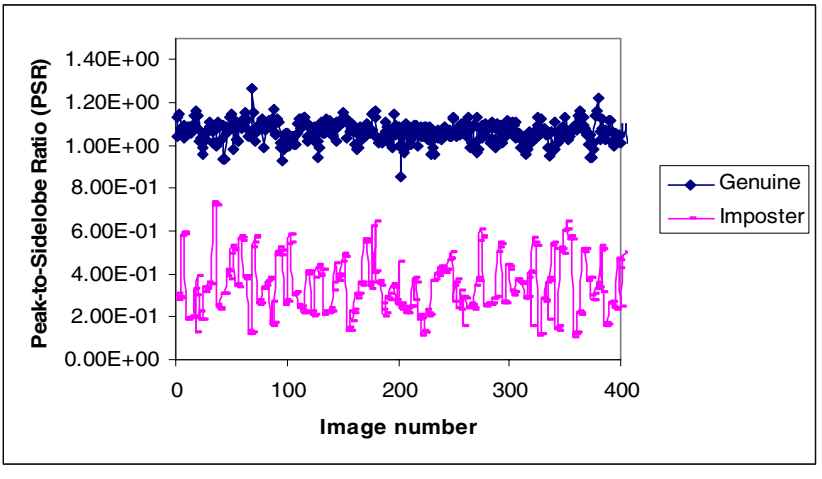


Fig. 4. PSR plots using RMACE-1000 for the first 400 comparisons of Genuine and Imposter class

5 Conclusion and Future Works

In this paper, a promising method for private iris authentication is presented. The privatization of biometrics is done based on the concealment of random kernel and the iris images to synthesize a minimum average correlation energy (MACE) filter for the iris authentication. Specifically, we multiply training images with the user-specific random kernel in frequency domain before biometric filter is created. Therefore, new private biometrics filter can be easily reissued if his/her possession has been lost/stolen.

In terms of authentication rate, it improves the performance significantly compare to the advance correlation based approach and comparable to the

Daugmant's Iris Code. Besides that, the filter synthesizing speed during the enrollment is notably increased due to the size reduction of the concealed iris template.

The research presented here will be further investigated by considering more challenging conditions such as noise contaminated, rotated and random occlusion iris images. Besides, it is interesting to look at the theoretical aspect on the proposed method.

References

1. J.G Daugman,: Recognizing Persons by their Iris Patterns In Biometrics: Personal Identification in Networked Society. Kluwer, (1998) 103-121.
2. R. M. Bolle, J. H. Connel and N. K. Ratha.: Biometric Perils and Patches. Pattern Recognition, Vol. 35, (2002) 2727 2738.
3. Davida, G., Frankel, Y., & Matt, B. J.: On enabling secure applications through off-line biometric identification. Proceeding Symposium on Privacy and Security, (1998) 148-157
4. Andrew Teoh Beng Jin, David Ngo Chek Ling and Alwyn Goh.: An Integrated Dual Factor Verification Based On The Face Data And Tokenised Random Number. LNCS, Springer-Verlag, 3072, (2004)117-123.
5. Marios Savvides, B.V.K. Vijaya Kumar and P.K. Khosla.: Cancelable Biometric Filters For Face Recogntion. Proc. of the 17th International Conference on Pattern Recognition (ICPR'04), (2004).
6. B. V. K. Vijaya Kumar, Marios Savvides, Chunyan Xie, Krithika Venkataramani, Jason Thornton and Abhijit Mahalanobis.: Biometric Authentication With Correlation filters. Applied Optics, Vol. 43, No.2, (2004) 391-402.
7. B.V.K Vijaya Kumar, M. Savvides, K. Venkataramani, C. Xie.: Spatial frequency domain image processing for biometric recognition. Proc. of Int. Conf. On Image Processing (ICIP), Vol.1, (2002) 55-56.
8. A.Mahalanobis, B.V.K Vijaya Kumar, and D.Casasent.: Minimum average correlation filters. Appl, Opt 26, (1987) 3633-3640.
9. A.Menezes, P.V. Oorschot, S. Vanstone.: Handbook of Applied Cryptography. CRC Press, Boca Raton, (1996).
10. CASIA Iris Image Database, Version 1.0. From: http://www.sinobiometrics.com