ELectronics EXpress

IEICE Electronics Express, Vol.2, No.11, 349–355

Tokenised discretisation in iris verification

Chong Siew Chin[a)], **Andrew Teoh B. J., and David Ngo C. L.**

Faculty of Information Science and Technology (FIST), Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia

a) *chong.siew.chin@mmu.edu.my*

Abstract: A novel authentication approach which based on the integration of tokenised pseudo-random numbers and the user's iris biometrics, to generate a user-specific binary bitstring via an iterated inner-product mechanism is proposed. The proposed method, S-Iris encoding, protects against iris fabrication as it can only contribute to the authentication process when both the genuine biometrics template and pseudo-random number are presented. It also enables straightforward revocation via token replacement. Furthermore, S-Iris Encoding reduces length of iris feature to around 5% of its original size yet able to attain an approximately 0% of Equal Error Rate (EER). This approach also shows the effectiveness and accuracy in term of verification rate if compared to the traditional biometrics system or the straightforward use of two authentication schemes in parallel.

Keywords: S-Iris Encoding, two-factor authentication, iris verification

Classification: Science and engineering for electronics

References

[1] R. M. Bolle, J. H. Connel, and N. K. Ratha, "Biometrics Peril and Patches," *Patt. Recogn.*, vol. 35, pp. 2727–2738, 2002.

[2] J. Armington, P. Ho, P. Koznek, and R. Martinez, "Biometric authentication in infrastructure security," *Int. Conf. of Infrastructure Security*, Bristol, UK, 2002.

[3] G. Lisimaque, "Biometrics and smart cards," *Conf. of the Biometric Consortium*, 1999.

[4] P. Ho and J. Armington, "A dual-factor authentication system featuring speaker verification and token technology," *Proc. 4th Int. Conf. on Audio-Video Based Personal Authentication*, UK, pp. 128–136, 2003.

[5] Li Ma, Yunhong Wang, and Tieniu Tan, "Iris Recognition Based on Multichannel Gabor Filtering," *5th Asian Conf. on Computer Vision*, Melbourne, Australia, Jan. 23–25, 2002.

[6] J. G. Daugman, "The Importance of Being Random: Statiscal Principles of Iris Recognition," *Patt. Recogn.*, vol. 36, no. 2, pp. 279–291, 2003.

[7] D. Field, "Relations between the Statistics of Natural Images and the Response Properties of Cortical Cells," *J. Opt. Soc. Am.*, 1987.

[8] Libor Masek, "Recognition of Human Iris Patterns for Biometrics Identification," B.Eng's thesis, University of Western Australia, 2003.

DOI: 10.1587/elex.2.349
Received April 29, 2005
Accepted May 27, 2005
Published June 10, 2005

[9] CASIA Iris Image Database 1.0. From: http://www.sinobiometrics.com

1 Introduction

Nowadays, computer security industry is in demand of finding reliable, accurate and cost-effective alternatives to physical key, passwords, ID cards or PIN due to the increasing of computer-based fraud such as identity theft. Biometrics addresses this problem as an individual's biometrics data is unique and non- repudiation. However, biometrics suffers from specific threats [1], like risk of being compromised by attacker whereby an attacker might use the biometrics data to masquerade as the person. The worst is a biometrics feature cannot be replaced once it was compromised.

Presently, there are several literatures reported the integration of biometrics into the smartcard [2, 3]. However, the only effort being applied in this line is to store the user's template inside a smart card, protected with Administrators Keys, and extracted from the card by the terminal to perform verification. Some are allowed to verify themselves in the card whenever the verification is positive. This is the situation where the two authentication schemes are used in parallel, one based in biometrics data and one based in secret password. Obviously, these configurations are not a remedy for the invasion of privacy problem.

Most recently, Ho and Armington [4] reported a dual-factor authentication system that designed to counteract imposter by pre-recorded speech and the text-to-speech voice cloning technology. Despite of that, no attempt for the False Accept Rate (FAR) - False Reject Rate (FRR) interdependent problem is reported.

In this paper, a novel two factor authentication approach, coined as S-Iris Encoding where direct mixing of tokenised user-specific random numbers and the ID Log-Gabor filtered iris feature through an iterated inner-product to generate a unique binary code per person is proposed. Figure 1 illustrates the progression of S-Iris Encoding.

This formulation is primarily aims to address the invasion of privacy issue of biometrics, such as iris fabrication. This problem can be resolved by

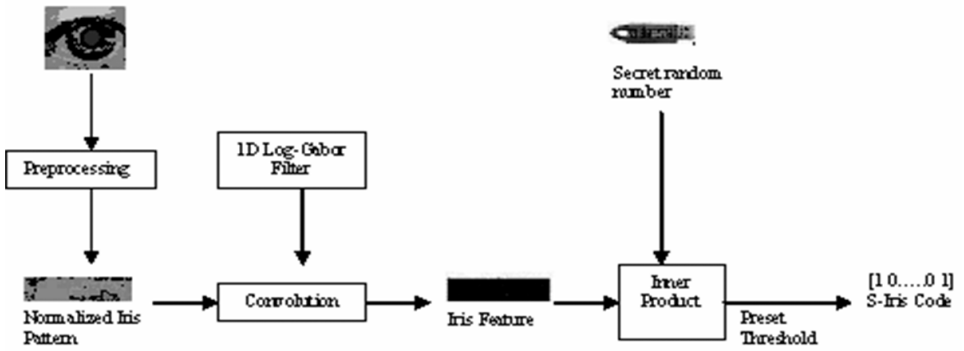

Fig. 1. S-Iris Encoding Progression

DOI: 10.1587/elex.2.349
Received April 29, 2005
Accepted May 27, 2005
Published June 10, 2005

replacing the stolen/lost token so that a new S-Iris code can be generated just as a new credit card can be issued if the old one is compromised. Also, the S-Iris Encoding contributes to the authentication process only when both live-captured iris and user-specific token are presented together by their rightful owner. S-Iris Encoding also reduces length of iris feature to around 5% of its original size yet able to attain an approximately 0% of Equal Error Rate (EER). In addition, S-Iris Encoding shows the effectiveness and accuracy in term of verification rate if compared to the straightforward use of two authentication schemes in parallel, one based in biometrics data and one based in secret password.

2 Iris Feature Encoding

An iris image needs to be processed before using it for the purpose of iris recognition due to the unwanted data in the image such as eyelid, pupil and specular reflections. Therefore, preprocessing is required to segment, normalize iris and to exclude the artifacts. After the preprocessing, the feature encoding is performed on the iris features to extract the underlying user-specific information in an iris pattern for the matching purpose.

2.1 ID Log-Gabor Filters Encoding

Gabor Filters based methods have been widely used as feature extractor in computer vision, especially for texture analysis [5]. Daugman [6] used multi-scale Gabor wavelets to extract phase structure information of the iris texture. However, Field [7] has examined that there is a disadvantage of the Gabor Filter in which the even symmetric filter will have a DC component whenever the bandwidth is larger than one octave. To overcome this disadvantage, an improved version of Gabor Filter known as Log-Gabor Filter, which is Gaussian on a logarithmic scale, can be used to produce zero DC component for any bandwidth. The frequency response of a Log-Gabor Filters is given as:

$$G(f) = \exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\beta/f_0))^2}\right) \tag{1}$$

where f_0 represents the center frequency, and β is the bandwidth of the filters [8].

In our scheme, 1D Log-Gabor Filters are chosen to be the feature extractor. By applying 1D Log-Gabor Filters, a 2D normalized iris pattern is first decomposed into a number of 1D signals, and these 1D signals are convolved with 1D Log- Gabor wavelets [8]. The resultant features are phased quantized to generate a series of real and imaginary numbers and are then encoded into binary iris templates as what commonly practice by the iris biometrics researcher, which follow the Daugman's IrisCode formulation.

2.2 S-Iris Encoding

During the S-Iris Encoding process, discretisation and binarization of the iris feature, w is carried out via an iterated inner-product of user-specific random

DOI: 10.1587/elex.2.349
Received April 29, 2005
Accepted May 27, 2005
Published June 10, 2005

numbers, $\boldsymbol{r}$, which yield a set of binary bitstring as shown in Eq. (2):

$$\boldsymbol{S}(w, \boldsymbol{r}) = \text{sgn}\left(\sum_k w_k r_k - \mu\right) \text{ and } r = (r_1, r_2, \cdots r_k) \tag{2}$$

where sgn(•) is defined as the signum function and μ is a preset threshold.

In practice, pseudo-random numbers, $\boldsymbol{r}$, can be obtained from a physical device, for example smartcard or USB token. There is a seed which stores in USB token or smartcard microprocessor to generate $\boldsymbol{r}$ using a random number generator. Different user will have different seeds for different applications which are recorded during the enrollment process.

Specifically, the process flow of generating S-Iris code is as follow:

1. Raw iris image: $I \in R^N$, with N is the image dimension.
2. Transformed iris feature which is in vector representation: $w \in R^n$, with n is the dimension of 1D Log-Gabor feature in frequency domain.
3. Token is used to generate a set of n-dimension random vectors, $\{\boldsymbol{r}_i \in R^n | i = 1, \ldots, m\}$ with m is the number of random vectors and their entries follow the Uniform distribution, U[−1 1].
4. Transform the $\{\boldsymbol{r}_i \in R^n | i = 1, \ldots, m\}$ into a set of orthonormal random vectors, $\{\boldsymbol{r}_{\perp i} \in R^n | i = 1, \ldots, m\}$ via Gram-Schmidt orthogonalization.
5. Compute $\{< w|\boldsymbol{r}_{\perp i} > \in R | i = 1, \ldots, m\}$ where $< \cdot|\cdot >$ indicates the inner-product operation.
6. Compute m bits of S-Iris code, $S = (S_1, \ldots, S_m) \in \{0, 1\}^m$ from $S_i = \begin{cases} 0 & if \quad \alpha \leq \mu \\ 1 & if \quad \alpha > \mu \end{cases}$, where μ is a preset threshold and $\alpha =< w|r_{\perp i} >$.

From the above process flow, it has been clearly shown that the bit length of S-Iris code can be either equal or less than the w feature length; hence the bit length of S-Iris can be reduced dramatically. This dimensional reduction may helps to decrease the computation load and increase the processing speed. Normally, smaller dimension iris features leads to lower computational complexity but lower accuracy. However, S-Iris Encoding provides both high accuracy and low computational complexity demands as will be discussed in section 3.

Note that it is highly unlikely that the pseudo-random number set from two different tokens can be closely similar as it is protected by the target collision resistance of Hash function. The major advantage of S-Iris Encoding is that compromising of either iris feature or pseudo-random number is merely useless as only the combination of both can contribute to the recognition process.

DOI: 10.1587/elex.2.349
Received April 29, 2005
Accepted May 27, 2005
Published June 10, 2005

3 Experimental Result

The experiments evaluates on iris images taken from the CASIA eye image database [9], which consists 756 grey scale eye images with 108 individuals and 7 images for each individual. The system performance can be addressed through the FAR, FRR and EER.

For the FAR test, the first image of each iris in the testing set is matched against the first impression of all other irises and the same matching process was repeated for subsequent images, leading to 40446 imposter attempts. For the FRR test, each image of each iris is matched against all other images of the same iris, leading to 2268 genuine attempts. In the experiments, the template size with radial resolution of 20 pixels and angular resolution of 240 pixels was chosen. Here, Hamming Distance employed by Daugman's IrisCode is chosen as a matching metric.

3.1 1-D Log-Gabor Filter Encoding

For feature extraction by using 1D Log-Gabor Filters, optimum selection for several parameters is needed in providing the best verification rate. These parameters include:

- The number of filters, F
- Base wavelength, λ
- Filter bandwidths, β
- Multiplicative factor between center wavelengths of successive filters, ν

In the encoding process, the outputs of each filter should be independent, so that there is no correlation in the encoded template, otherwise the redundancy of filters may occur. For maximum independence, the bandwidths of each filter must not overlap in the frequency domain, and also the center frequency must be spread out. The encoding process generates a binary iris template with 9600 bits.

The results of fine-tuning various parameters of iris feature extraction are presented in Table 1. The optimum value of 1D Log-Gabor Filters parameters can be achieved with bandwidth $\beta = 0.5$, number of filter $= 1$, center wavelength $\lambda = 12$ and multiplicative factor $= 1$. The mentioned set of optimum filter parameters provides optimum EER, which is 2.59%.

3.2 S-Iris Encoding

In this section, comparisons are made between 1D Log-Gabor extracted iris feature (LG) and the S-Iris Code (SLG) by utilized the optimum parameters obtained from section 3.1. The magnitude of complex feature vectors that resulted from the convolution of 1D Log-Gabor filters with iris image, is used to generate SLG, instead of the phase information that sensitive to the inner-product process.

DOI: 10.1587/elex.2.349
Received April 29, 2005
Accepted May 27, 2005
Published June 10, 2005

Table I. Different filter parameters tested on CASIA Iris Image database.

F	λ	ν	β	FAR (%)	FRR (%)	EER (%)
1	4	1	0.5	0.0148	26.4550	13.2349
1	8	1	0.5	0.2052	5.6437	2.9245
1	12	1	0.5	1.4315	3.7478	2.5900
1	14	1	0.5	2.8853	3.3510	3.1182
1	16	1	0.5	2.9916	3.4832	3.2374
1	18	1	0.5	3.3576	3.3951	3.3764
2	12	1	0.5	1.8741	3.7919	2.8330
2	12	2	0.5	2.6554	3.2187	2.9371
1	12	1	0.3	4.6976	3.5273	4.1126
2	12	2	0.3	3.5479	4.8942	4.2211

Table II illustrates the performance comparison by using LG and SLG for different bit length. In the experiments, various bit length, $m = 100$, 150, 200, 300 and 350 are used for SLG. The results show that SLG is able to achieve an approximately zero EER with the bit length 350 bits. Extremely low EER of 0.0025% reveals the robustness of SLG in the verification task. Other bit lengths of SLG gives the EER not more than 1% whilst LG gives the poorest EER of 2.59%. This implies that SLG is more superior in terms of accuracy if compared to LG. Besides that, SLG greatly reduces the bit length of iris template to around 5% of the original feature length 9600 bits. The experiments conclude that SLG has better performance than LG from the aspect of accuracy, computational speed and dimension reduction.

Table II. FAR, FRR and EER for CASIA Iris Image Database tested on different bit length based on different methodologies.

Methodology	Bit Length, m	FAR (%)	FRR (%)	EER (%)
LG	9600	1.4315	3.7478	2.5900
SLG-m	100	0.6231	0.9700	0.7965
	150	0.5242	0.4850	0.5046
	200	0.0816	0.0882	0.0849
	300	0.0396	0.0441	0.0419
	350	0.0049	0.0000	0.0025

4 Conclusion

A novel dual factor authentication approach, S-Iris Encoding, incorporating the pseudo-random number and user specific iris features extracted from 1D Log-Gabor Filters through an iterated inner product has been presented. This proposed methodology has significantly increased the security and protection of a user in applications. It helps in preventing biometric fabrication.

DOI: 10.1587/elex.2.349
Received April 29, 2005
Accepted May 27, 2005
Published June 10, 2005

It also has significant functional advantages over solely biometrics or token usage, which can be shown by the result in achieving a 0.0025% $\approx$ 0% EER. This might avoid the suffering from increased occurrence of FRR when eliminate the FAR.

Another major advantage of this proposed methodology is new iris template of a person can be reissued if his/her template is lost or being stolen. The secret random number can be generated again and combined with the specific iris feature.

In addition, the iris feature length can be greatly reduced to around 5% of the original size as reported in the experiment. The dimensional reduction not only promises the uniqueness of iris feature, but also increases the simplicity and efficiency in verification task.

Ultimately, this approach proves the effectiveness and accuracy in term of verification rate if compared to the traditional biometrics system or the straightforward use of two authentication schemes in parallel.

DOI: 10.1587/elex.2.349
Received April 29, 2005
Accepted May 27, 2005
Published June 10, 2005