Available online at www.sciencedirect.com
SCIENCE DIRECT
Computer Vision and Image Understanding 102 (2006) 169–177
Computer Vision and Image Understanding
www.elsevier.com/locate/cviu

High security Iris verification system based on random secret integration

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

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

Received 29 October 2004; accepted 11 January 2006
Available online 9 March 2006

Abstract

A dual-factor authentication methodology coined as S-Iris Encoding is proposed based on the iterated inner-products between the secret pseudo-random number and the iris feature, and with thresholding to produce a unique compact binary code per person. A thresholding method is devised to exclude the weak inner-product during the encoding process, and thus contribute to the improvement of performance. S-Iris Encoding is primary formulated based on the cancelable biometrics principle to protect against biometrics fabrication. The problem could be rectified by S-Iris code through the token replacement so that a new code can be generated instantly just as a new credit card number can be issued if the old one is compromised. Besides that, S-Iris code is non-invertible and can only contribute to the authentication process when both genuine biometrics template and token are presented. By applying S-Iris Encoding with weak inner-product exclusion, the original iris feature length can be greatly reduced to around 4% of the original size and a 0% of equal error rate (EER) can be attained in CASIA Iris image database.

Keywords: S-Iris Encoding; Two-factor authentication; Cancelable biometrics; Iris verification; Weak inner-product exclusion

1. Introduction

In recent years, with the continuous increasing demand for security and the development of information technology, intelligent personal identification based on biometrics has become a very active topic in both research and practical applications. Currently, many authentication mechanisms are based on users' PIN, passwords, ID cards or physical key to allow them to access into secure zones or to log into a computer. Problem with these methods is that the users need to remember lots of different PIN and passwords or carry the token, which is very inconvenient and insecure.

Thus, biometrics has become another alternative for secure authentication. Biometrics authentication utilizes psychological and physical characteristics that define us as an individual [1]. Biometrics information cannot be shared or transferred. Of all the biometrics technologies used for human authentication today, it is generally conceded that iris recognition is the most accurate. Since the iris is an overt body, iris recognition systems can be non-invasive to their users, which is a very important factor for practical applications [2].

Although biometrics is a powerful tool against repudiation, it still suffers from some inherent biometrics specific threats [3]. There is risk of being compromised by attacker where an attacker might use the biometrics information to masquerade as the person. The worst is a biometrics feature cannot be replaced once it is compromised. Recently, there is substantial research going on to find solutions on this problem. Bolle et. al. [3] has introduced the terms *cancelable biometrics* of which referred to an intentional distortion of a biometrics signal based on a chosen transform. The biometrics signal is distorted in the same fashion at each presentation, that is, during enrollment and for every subsequent authentication. With this approach, every instance of enrollment can use a different transform thus rendering cross-matching impossible. Furthermore, if one

* Corresponding author. Fax: +6062318840.
E-mail addresses: chong.siew.chin@mmu.edu.my (C.S. Chin), bjteoh@mmu.edu.my (A.T.B. Jin), david.ngo@mmu.edu.my (D.N.C. Ling).

1077-3142/$ - see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.cviu.2006.01.002

variant of the biometrics is compromised, then the transformation can simply be changed to create a new variant for re-enrollment. Since then [4] has listed three principal objectives of designing a *cancelable biometrics*:

1. Same cancelable template cannot be used in two different applications.
2. Once the biometrics template has been compromised, a new template can be reissued.
3. The template is non-invertible.

The first attempt towards this direction was done by Davida et al. [5]. They proposed information hiding hash functions as one way to protect the sensitive user template. In this approach instead of storing the template T or the corresponding binary code or key C directly, an information hiding signature and hash $X = H(C)$ is stored. There is no security requirement imposed on the hash function or on the error correcting codes. During verification the acquired biometric code C' is reduced to the canonical representation C using the user specific error correcting code. The user is authenticated if the signature and hash generated are identical. Juels et al. [6,7] generalized and improved Davida et al., scheme through a modification in error-correcting codes, and is hence reduced the code size and achieved higher resilience. However, the techniques did not address the first two requirements that above mentioned. Soutar et al. [8] described a different approach for generating a cancelable biometrics from fingerprints using optical computing techniques. During enrollment stage, a correlation pattern, c_0 was derived from a set of training images. The correlation pattern was then hashed with a cryptographic key to produce an identification code, I_0. During verification, another pattern, c_1 was generated from the new fingerprint image and hashed with the same cryptographic key to produce identification code, I_1. If I_0 and I_1 were similar, then the match was successful. However, the method does not carry rigorous security guarantees and the resulting false acceptance rate (FAR) and false reject rate (FRR) are unknown. The authors also assume that the input and database templates fingerprint images are completely aligned. It is unrealistic to acquire fingerprint images from a finger without any misalignment, even with a very constrained image acquisition system.

Tuyls et al. [9,10] assume that a noise-free template X of a biometric identifier is available at the enrollment time and use this to enroll a secret S to generate a helper data W. Assume that each dimension of the template is quantized at q resolution levels. In each dimension, the process of obtaining W is equivalent to finding residuals that must be added to X to fit to odd or even grid quantum depending upon whether the corresponding S bit is zero or one. At decryption time, the (noise-prone) biometric template Y is used to decrypt to obtain a decrypted message S', which is approximately the same as S. It is hoped that the relatively few errors in S' can be corrected using error-correction techniques. The proposed technique assumes that the biometric representations are completely aligned and that noise in each dimension is relatively small compared to the quantization Q. Most recently, Savvides et al. [11] 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.

In this paper, a cancelable biometrics formulation, which coined as S-Iris Encoding is proposed. S-Iris Encoding combines two authentication factors (iris feature + tokenised pseudo-random number) via iterated inner-product and thresholding to render a set of cancelable binary bit string. Through the S-Iris Encoding formulation, biometrics fabrication issue can be resolved by replacing the 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, S-Iris code only can contribute to the authentication process only when both the live-captured biometrics and user-specific token are presented together by their rightful owner. The inversion of S-Iris code to obtain iris feature is also impossible due to the factoring inner-product of iris feature and pseudo-random number is an intractable problem. Therefore S-Iris Encoding conforms to the above listed three cancelable biometrics criteria. S-Iris Encoding also has significant functional advantages over conventional biometrics, such as providing near zero error rate (EER). Furthermore, weak inner-product exclusion mechanism is introduced to enhance S-Iris Encoding verification performance in the sense that the numerically small value of inner-products is expelled during the verification process. By applying S-Iris Encoding with weak inner-product exclusion, the original iris feature length can be greatly reduced to around 4% of the original size and a 0% of equal error rate (EER) can be attained.

The outline of the paper is as follow: Section 2 describes the overview of S-Iris Encoding progression and its usage in the practical scenario. Sections 3–5 discuss the preprocessing, feature extraction and encoding of iris using the proposed methodology. Section 6 provides the security analysis of S-Iris Encoding. Experiments and results are reported in Section 7. Conclusion is drawn in Section 8.

2. Overview of S-Iris Encoding

The S-Iris Encoding process is started with the transformation of iris image into a lower and more discriminative representation domain through 1D Log-Gabor Filtering. The filtered iris features is then combined with the specific secret pseudo-random number through the iterated