Pattern Recognition 64 (2017) 105–117

Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

Cancellable iris template generation based on Indexing-First-One hashing

Yen-Lung Lai[a], Zhe Jin[a], Andrew Beng Jin Teoh[b,*], Bok-Min Goi[a], Wun-She Yap[a], Tong-Yuen Chai[a], Christian Rathgeb[c]

[a] Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Kuala Lumpur, Malaysia
[b] School of Electrical and Electronic Engineering, College of Engineering, Yonsei University, Seoul, South Korea
[c] Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany

ARTICLE INFO

Keywords:
Iris
Cancellable template
Min-hashing
Jacaard similarity
Security & privacy

ABSTRACT

Eye iris has been widely recognized as one of the strongest biometrics attributed to its high accuracy performance. However, templates in conventional iris recognition systems are unprotected and highly vulnerable to numerous security and privacy attacks. Despite a number of cancellable biometric schemes have been proposed but at the expense of substantially decreased accuracy performance. In this paper, we introduce a new cancellable iris scheme, coined as "Indexing-First-One" (IFO) hashing. IFO hashing is inspired from the Min-hashing that primarily used in text retrieval domain. However, IFO hashing has been further strengthened by two novel mechanisms, namely P-order Hadamard product and modulo threshold function. The IFO hashing scheme strikes the balance between accuracy performance and privacy/security protection. Comprehensive experiments on CASIA-v3 iris benchmark database and rigorous analysis demonstrate decent accuracy performance with respect to its original counterparts yet offer strong resilience against several major security and privacy attacks.

1. Introduction

Conventional identity verification mechanisms rely on memory-based credentials or possession tokens such as passwords, PIN numbers or access cards for system access. Unfortunately, they are easily being forgotten, stolen and lost. On the other hand, biometrics have been introduced as an alternative that exploits the physiological and behavioral characteristics of human being as identity credentials. Typical biometrics are fingerprint, facial image, palm print, iris and etc. Since the biometric traits are inherently associated to individuals, the aforementioned issues are largely relieved. Due to the usability merit, biometrics are increasingly replacing passwords and ID cards in many applications which demand identity management [1].

Among all the biometric traits available today, eye iris is considered as one of the highly reliable biological traits attributed to its discriminability and stability. The iris remains constant throughout the lifetime and not subjected to the environment and genetics factor [2]. Daugman is the first person who devised practical automated iris recognition systems and the inventor of favorite iris representation known as IrisCode [2]. Besides, it has been validated that the entropy of iris patterns is typically much higher than other biometric traits [3]. This infers that the false matches between different IrisCodes are highly unlikely to be happened. Therefore, apart from verification, iris can be very useful for identification task.

For both verification and identification tasks, individual user first has to enroll his/her iris data into the system and the iris data is stored as a template (e.g. IrisCode) in the database. During authentication process, only the right person can be verified or identified successfully through the matching of the IrisCode with the right iris from the genuine user.

Since the IrisCode contains highly discriminatory information of the individual user, the exposure of the IrisCode to an adversary may lead to security breaches such as masquerade attack and replay attack [4–6]. Besides, due to the fact that human iris is permanently associated to each individual, this implies a permanent loss of identity. Moreover, it is possible to cross-match multiple templates by compromising several databases which may result severe user privacy invasion.

The security and privacy issues of iris templates have been a major concern and hence its protection has emerged as a subtopic of biometric technology namely *biometric template protection* (BTP) dedicated to solve the aforementioned challenges. Instead of storing the IrisCode undisguised, BTP is used to generate its protected instances which are more secure to be stored inside the database. Interested readers are referred to comprehensive reviews such as [7–10]. In this paper, we focus on a specific instance of template protection

* Corresponding author.
E-mail address: bjteoh@yonsei.ac.kr (A.B. Jin Teoh).

http://dx.doi.org/10.1016/j.patcog.2016.10.035
Received 22 August 2016; Received in revised form 14 October 2016; Accepted 31 October 2016
Available online 09 November 2016
0031-3203/

technique called cancellable biometrics. Cancellable biometrics distorts the biometric features intentionally by applying certain transformation function during enrollment and authentication. To design a decent cancellable biometrics scheme, the following four criteria have to be satisfied [11,12]:

1. Unlinkability: it should not be able to differentiate whether one or more protected templates are generated from the same source (same user's biometric). This is to prevent cross-matching across different applications.
2. Revocability: it should be computationally infeasible to derive its original counterparts from *multiple* protected templates. This enables new template to be revoked or renewed to replace the old one meanwhile preventing the adversary from obtaining the original template.
3. Non-invertible: it should be computationally infeasible to derive its original counterparts from the protected template and/or the helper data; hence it prevents the abuse of the compromised biometric data and enhances the security of the system.
4. Performance: the accuracy performance of cancellable template must be approximately preserved with respect to its original counterparts.

1.1. Related work

In this section, previous works for iris template protection are revisited and summarized. Ratha et al. [13] first introduce the notion of cancellable biometrics. In their works, they permute the fingerprint minutia in Cartesian and polar domains to generate cancellable template. Apart from that, they devise a surface folding transformation function for minutia points remapping in such a way that the transformed surface is locally non-smooth and globally smooth to achieve non-invertibility yet preserve accuracy performance. In spite their works render satisfactory accuracy performance, the non-invertibility was found weak [14]. However, the work had inspired iris template protection schemes later [15,16]. In general, cancellable biometrics can be classified into biometric salting and non-invertible transformation.

1.1.1. Salting approach iris template

In biometric salting, independent auxiliary data such as user-specific password or token are combined with biometric data to render a distorted version of the biometric template. An instance of iris salting scheme was proposed by Chong et al. [17] namely S-IrisCode encoding. To be specific, the iris Gabor-feature vector $\boldsymbol{\omega} \in C^n$ was first generated by convoluting the 1-D log-Gabor filter with the normalized iris image that later reshaped into a n-dimensional feature vector·Then, the magnitude of $\boldsymbol{\omega}$, denoted as $\boldsymbol{w}$ was projected into a lower dimensional feature space through iterated inner products with a set of user-specific orthonormal random vectors $\{\boldsymbol{r}_{\perp i} \in \Re^n i = 1,\ldots,m\}$ where $m \leq n$. A quantization process was carried out that computed s_i from$\{\alpha = \langle \boldsymbol{w} \mid \boldsymbol{r}_{\perp i} \rangle i = 1,\ldots,m\}$ with s_i=0 when $\alpha \leq 0$; s_i=1 when $\alpha > 0$. Once compromised, new cancellable template can be regenerated by issuing a new set of random vectors from user-specific token. To improve the accuracy performance, a noise mask $\{s_{iN} | i = 1,\ldots,m\}$ was utilized with s_{iN}=0 when $\alpha < -\sigma and \alpha > \sigma$ otherwise. The noise mask acts as a control bit to determine the validity of the s_i bits by eliminating the weak inner product, thus, improved the correctness in hamming distance matching.

Zuo et al. [16] proposed a salting method which can be applied to either real-valued or binary iris patterns, namely GREY-SALT and BIN-SALT. In GREY-SALT, an artificial pattern was either added or multiplied to iris pattern. For BIN- SALT, XOR operation was applied to the IrisCode and the random binary key pattern. For both GREY-SALT and BIN- SALT, the iris information was concealed with the auxiliary data. Thus, cancellable iris template refreshment was realized by replacing the auxiliary data. However, accuracy performance may significantly deteriorate without pre-alignment process.

Instead of using the whole iris image as in Chong et al. [17], Pillai et al. [18] used sectored random projections for cancellable iris template generation. They remarked that, by projecting the iris image directly via a user-specific random matrix may inevitably lead to performance deterioration due to noises such as eyelashes, specular reflection, and eyelid as well as inhomogeneous quality in different regions of iris image. Thus a linear transformation of good iris regions with the noises corrupted the data. In their work, the iris was partitioned into several sectors, and then the Gabor features of each sector were projected into a lower dimensional space via a user-specific random Gaussian matrix. Lastly, the cancellable template was generated by concatenating the projected outputs from different sectors. Followed by a feature encoding process as in conventional iris recognition system [2,3,19] a cancellable IrisCode can be generated. Their work compressed the original template while preserving the accuracy performance. New templates can be generated by using different random projection matrices.

However, Kong et al. [20] and Lacharme et al. [21] showed that if the same random matrix is applied to different users, the accuracy performance degraded significantly and it is highly likely the cancellable template can be inverted when the user-specific random matrices are disclosed to the attacker (stolen-token scenario). This implies that in general the biometric salting is feasible if and only if the auxiliary data is kept secret.

1.1.2. Non-invertible transformation methods for iris template

Non-invertible transformation is conceptually attractive for template protection schemes [22]. In non-invertible transformation, a one way transformation function is used to transform the iris template in which the transformed iris template is non-invertible and can be securely stored in the database [23]. Zuo et al. [16] proposed two non-invertible transformation methods, namely GREY-COMBO and BIN- COMBO for iris templates. In GREY-COMBO, they shifted the iris image in a row-wise manner via the random offset (random key), then followed by an operation (either addition or multiplication) on two randomly selected rows. In BIN_COMBO, same procedure was performed to IrisCode but with XOR or XNOR operation. In this manner, the original iris data was distorted attributed to the addition/multiplication operation between the two randomly selected row features, hence, fulfilled non-invertibility criterion. In both GREY-COMBO and BIN_COMBO, the shifted rows of the iris template were always in the same orientation regardless rotation, hence it is 'registration free' which implies that no alignment is needed for matching. However, the first method suffered from performance degradation when poor quality iris images was used. Nevertheless, since they used user-specific key, this exposed to the risk of stolen-token as in salting approach.

Hämmerle-Uhl et al. [15] used block remapping method to perform non-invertible transformation. The normalized iris image was first partitioned into several image blocks and randomly permuted with a key. An image block remapping technique was applied to generate cancellable template. In this process, a target image, which is the same size to the source iris image was initialized. Then, different image blocks from the source image were mapped into the target image. Same image block was allowed for multiple times of remapping. The lossy remapping process prevents the reconstruction of original iris image and satisfies the non-invertibility criterion. Despite the scheme did not jeopardize the accuracy performance, Jenisch et al. [24] however demonstrated that 60% of the original iris image can be restored from the stolen template.

Ouda et al. [25,26] proposed a tokenless IrisCode template protection scheme, namely Bio-encoding. They first determined the "consistence bits" from several IrisCodes of each user. The consistence bits refer to the bits that have lower probability to be flipped among several samples collected. The consistence bits, $C \in \{1, 0\}^n$ where n denotes the