Pattern Recognition 48 (2015) 2290–2303

Contents lists available at ScienceDirect

Pattern Recognition

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

Alignment-free row-co-occurrence cancelable palmprint Fuzzy Vault

Lu Leng [a,b], Andrew Beng Jin Teoh [a,*]

[a] School of Electrical and Electronic Engineering, College of Engineering, Yonsei University, Seoul 120749, South Korea
[b] Key Laboratory of Nondestructive Test (Ministry of Education), Nanchang Hangkong University, Nanchang 330063, China

ARTICLE INFO

Article history:
Received 27 October 2014
Accepted 23 January 2015
Available online 3 February 2015

Keywords:
Palmprint fuzzy vault
Row-co-occurrence
2DPalmHash Code
Alignment-free matching
Cancelable palmprint

ABSTRACT

Texture coding approach of palmprint biometric enjoys several merits; however, palmprint texture code suffers from alignment problem during matching, which hinders it from being directly adopted in biometric cryptosystems, such as Fuzzy Vault. On the other hand, Fuzzy Vault itself is plagued by several security and privacy issues if biometric template is left unprotected. In this paper, we proposed two hybrid cancelable palmprint cryptosystems based on palmprint texture code, dubbed row-alone and row-co-occurrence Fuzzy Vaults. To be specific, we blend 2DPalmHash Code (2DPHC), a cancelable biometric scheme, and Fuzzy Vault primitive to jointly protect palmprint templates. In row-alone Fuzzy Vault, we leverage the horizontal displacement tolerance trait of 2DPHC to extract an alignment-free feature set for polynomial projection. We further generalize row-alone Fuzzy Vault to row-co-occurrence Fuzzy Vault to improve the key recovery rate. Besides that, we demonstrate that 2DPHC-based Fuzzy Vault enhances the robustness against several security attacks.

1. Introduction

Palmprint biometric has been widely employed recently thanks to its high accuracy, low cost and wide user acceptance [1]. Unfortunately, the secure and privacy problems that plague many biometrics [2] also present in palmprint biometric:

- Palmprint features are immutable, which implies that palmprint templates cannot be revoked and reissued even if they are compromised.
- With the widespread usage of palmprint systems, palmprint templates are stored diversely in different databases. The security levels of these databases are different. If the palmprint templates in the database with low security level are compromised, the templates stored in other databases are no longer safe.
- Users' privacy information, such as gene deficiency and health condition, is likely to be leaked from original palmprint features.

Therefore, biometric template protection methods, such as cancelable biometric and biometric cryptosystem, are essential to avoid direct disclosure of original palmprint features.

Palmprint features can be extracted by means of geometry-based approaches, subspace-based approaches, statistical approaches and texture coding approaches in general [1]. The discriminative ability of geometry-based features, such as points, lines, is highly subject to the availability of high resolution image [3,4]. Some mathematical transformations, such as wavelets transform, Fourier transform, discrete cosine transform (DCT), are usually adopted by statistical approaches, whereby statistical or representative features in transformed domain are utilized [5–7]. Subspace-based approaches, such as principle component analysis (PCA) and linear discriminant analysis (LDA), do not exploit the inherent features of palmprint biometric, such as lines, orientations, ordinal features, and hence their accuracies are usually unsatisfactory [8,9]. To make matters worse, it is always hard to extract the discriminative features with small training sample set [10].

On the other hand, a class of prominent binary palmprint feature extraction technique, which we coin *texture coding approach*, can be derived from palmprint texture by means of 2D-Gabor filter or texture descriptors. Several instances of palmprint texture codes are PalmCode [11], Fusion Code [12], Competitive Code [13], Ordinal Code [14], Robust Line Orientation Code [15], Binary Orientation Co-occurrence Code [16], Extended Binary Orientation Co-occurrence Code [17], etc. They enjoy several merits, such as parsimony in computation and storage, free from training as well as favorable accuracy performance in large database. Thus it is tempted to develop biometric cryptosystems based on palmprint texture code, which are still absent today.

Unfortunately, palmprint texture codes mainly suffer from alignment-matching problem caused by the displacement of two templates [1]. This problem can be rectified in virtue of the 2D ordered structure of texture codes. One template is usually shifted along horizontal and vertical orientations, and then matched with

[*] Corresponding author. Tel.: +82 2 21235772; fax: +82 2 3132879.
E-mail addresses: lenglu@126.com (L. Leng), bjteoh@yonsei.ac.kr (A.B.J. Teoh).

http://dx.doi.org/10.1016/j.patcog.2015.01.021
0031-3203/© 2015 Elsevier Ltd. All rights reserved.

another template for multiple times. The minimum distance is considered as the final dissimilarity score [11–17].

However, the above solution is not transferable to biometric cryptosystems, such as Fuzzy Vault that requires texture code to be decomposed into several sub-blocks for polynomial projection. This will severely ruin the inherent ordered structure of texture code and void the multiple-translated matching trick used in ordinary palmprint verification systems. In this paper, we demonstrate our solution to this problem along with several other well-known implementation issues on Fuzzy Vault.

1.1. *Related works*

1.1.1. *Biometric template protection*

In general, biometric template protection should meet three basic criteria, namely non-linkage, non-invertibility and recognition/verification performance.

(1). *Non-linkage* requires that multiple uncorrelated cancelable biometric templates can be generated from a single original biometric. Furthermore, users can change their cancelable biometric templates freely if their templates are compromised.
(2). *Non-invertibility* prevents the leakage of users' private information from original biometric.
(3). *Recognition/verification performance* requires that the accuracy of cancelable biometric can be comparable to its unprotected biometric counterpart.

Biometric template protection methods can be briefly categorized into cancelable biometric, biometric cryptosystem and hybrid method [18]. Cancelable biometric transforms the original feature to its protected version with specific functions [19]. Biometric cryptosystem attempts to utilize biometric features as authenticators for cryptographic application rather than using conventional credentials, such as passwords, tokens [20]. Unfortunately, none of the single method can address all the requirements of template protection, so it is natural to consider the hybrid of cancelable biometric and biometric cryptosystem [21].

1.1.2. *Palmprint template protection*

The existing methods of palmprint template protection are described as follows.

1.1.2.1. Cancelable palmprint. Cancelable palmprint can be briefly classified into invertible and non-invertible approaches. The former attempts to protect palmprint features via cryptographic solution. Random field shift [22] and encrypted palmprint [23,24] are two representative instances of this technique; while the latter employs non-invertible functions to protect palmprint features. To name a few, they are Cancelable PalmCode [25], PalmHashing [26], cancelable palmprint codes [27,28].

Invertible cancelable palmprints do not meet non-invertibility requirement, which are less useful in practice. However, the non-invertibility requirement likely triggers discriminative deterioration on the features.

Besides the tradeoff between security and accuracy, alignment is another difficulty of cancelable palmprint matching. In [22,29], the original templates are pre-aligned before cancelable template generation. However, for the security and privacy, none original biometric templates should be stored, it is unpractical to pre-align the enrolled and query original templates [30,31]. Thus it is significant to develop alignment or alignment-free methods for the matching of cancelable palmprint codes [32].

1.1.2.2. Palmprint cryptosystem. The merging of biometric and cryptography attempts to deploy biometric as the authenticator of cryptographic applications, in which biometric features are claimed to be protected. Cryptographic systems request that both encryption–decryption keys be identical [33]; however, due to intra-class variance, it is difficult to extract the identical biometric features as the key from the enrolled and query biometric templates [34].

To reconcile this contradiction, key-binding technique was proposed to extract identical biometric features as the encryption–decryption keys, whereby biometric template and secret key were bound with some mechanisms and stored in a form of concealed template. The concealed template should neither leak key information nor biometrics. Due to the error tolerance ability of key binding schemes, the secret key can be retrieved with query biometric features that are close enough to enrolled features. Fuzzy Commitment [35] and Fuzzy Vault [36,37] are two typical key-binding schemes.

In [38], Wu et al. applied a hash function to protect palmprint key that is extracted by Bose–Chaudhuri–Hocquenghem (BCH) error correction code (ECC). However, the palmprint key is unchangeable. The parity bits for error correction stored in the database are likely to leak the information of original palmprint features. The same authors developed another palmprint cryptosystem based on Fuzzy Commitment [39]; unfortunately, the palmprint feature is insecure once both concealed template and key are disclosed.

In [40], a palmprint Fuzzy Vault constructed from DCT features was proposed. Each genuine DCT feature was concealed by two chaff points, that is, each small fuzzy vault contained one genuine point and two chaff points. The matchings of the small Fuzzy Vaults were performed sequentially. In the experiments, the database was small. Although the successive matching of the small Fuzzy Vaults improves accuracy, the security is seriously deteriorated. The success probability of brute force attack on each small Fuzzy Vault is pretty high, i.e., 1/3. Moreover, the DCT features are not protected.

The features extracted by the subspace methods, such as PCA, LDA, can be used for palmprint verification. In [41], Verma and Bharathan developed a palmprint Fuzzy Vault based on PCA features. The database in their experiments was also very small. In [42], Liu et al. proposed a multi-dimensional Fuzzy Vault, in which the intra-class variances of LDA palmprint features were suppressed by a general subspace error-tolerant mechanism. However, subspace trainings incur high computation cost especially for large databases.

1.1.2.3. Hybrid palmprint template protection. Hybrid methods were employed in face template [43], fingerprint template [44,45], etc. For palmprint protection, Leng and Zhang developed cancelable dual-key-binding cryptosystem to enhance the security and privacy of palmprint template [46]. Firstly, the palmprint features were replaced with cancelable features. Secondly, the key generation was controlled by both cancelable palmprint key and variable factor. Recently, Liu et al. [47] combined random projection that enables the cancelability of the genuine points in Fuzzy Vault to protect the original palmprint features extracted by subspace methods.

1.1.3. *Attacks against Fuzzy Vault*

Fuzzy Vault is one of the popular bio-cryptosystems initially introduced by Juels and Sudan [36,37], which was evolved from Shamir's secret sharing scheme for binding cryptographic keys. The security of this scheme largely depends upon the polynomial reconstruction problem. Therefore, several major attacks against Fuzzy Vault have been identified in the literatures as follows [48–51].