Pattern Recognition 48 (2015) 458–472

Contents lists available at ScienceDirect

Pattern Recognition

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

Secure biometric template generation for multi-factor authentication

Salman H. Khan [a,*], M. Ali Akbar [b], Farrukh Shahzad [b], Mudassar Farooq [b], Zeashan Khan [c]

[a] School of Computer Science and Software Engineering, The University of Western Australia, Crawley, WA 6009, Australia
[b] Next Generation Intelligent Networks Research Center, Institute of Space Technology, Islamabad 44000, Pakistan
[c] Riphah International University, I-14, Islamabad 44000, Pakistan

ARTICLE INFO

Article history:
Received 12 January 2014
Received in revised form
20 August 2014
Accepted 28 August 2014
Available online 8 September 2014

Keywords:
Two factor authentication
Biometric template protection
Feature transformation
Dynamic signature verification
Biohashing
Random projections
Distance matching

ABSTRACT

In the light of recent security incidents, leading to compromise of services using single factor authentication mechanisms, industry and academia researchers are actively investigating novel multi-factor authentication schemes. Moreover, exposure of unprotected authentication data is a high risk threat for organizations with online presence. The challenge is how to ensure security of multi-factor authentication data without deteriorating the performance of an identity verification system? To solve this problem, we present a novel framework that applies random projections to biometric data (inherence factor), using secure keys derived from passwords (knowledge factor), to generate inherently secure, efficient and revocable/renewable biometric templates for users' verification. We evaluate the security strength of the framework against possible attacks by adversaries. We also undertake a case study of deploying the proposed framework in a two-factor authentication setup that uses users' passwords and dynamic handwritten signatures. Our system preserves the important biometric information even when the user specific password is compromised – a highly desirable feature but not existent in the state-of-the-art transformation techniques. We have evaluated the performance of the framework on three publicly available signature datasets. The results prove that the proposed framework does not undermine the discriminating features of genuine and forged signatures and the verification performance is comparable to that of the state-of-the-art benchmark results.

1. Introduction

The ubiquitous Internet connectivity has led to provision of an ever increasing list of diverse online services ranging from financial transactions to online gaming. With cloud computing on the rise, geographically distant employees of organizations tend to access and share the sensitive organizational resources online. This trend has increased the stakes of user authentication process. An ever increasing need to control the access to sensitive resources, through user authentication process, demands that the data needs to be stored on the server in a secure manner.

The three different types of elements (known as *factors*) that can be used for authentication of a user's identity are the *ownership*, *knowledge* and *inherence* factors. The traditional passwords based approach belongs to the knowledge factor (something user knows) and has been the prevalent method of authentication for the last couple of decades. However, as the recent security incidents have demonstrated, the single-factor authentication (SFA) approach is insufficient [38,12,17]. The threats against poorly protected authentication information are rising exponentially. The major leaks of the period 2012–2013 – include Twitter [38], LinkedIn [21], IEEE.org [12], Dropbox [6] and Yahoo [17] – corroborate the argument. Therefore, there is a requirement for adoption of multi-factor authentication (MFA) schemes (e.g., Dropbox offered two-factor authentication (TFA) in July 2012 [6]). A directive from US Federal Financial Institutions Examination Council (FFIEC) also makes it compulsory for the banks to use MFA in online transactions [14].

Biometrics based identity verification systems are unique from the ownership factor (ATM, National ID Card, badges, etc.) and knowledge factor (password, security questions, PIN number, etc.) based authentication paradigms. Consequently, such systems free the user from concerns like identity lost/theft, illegal distribution, repudiation, expiry dates, bearing the identity all times or remembrance issues [33]. Human biometrics are characteristic of a user (inherence factor) and can be used collectively with passwords for MFA for highly secure systems. The verification performance achieved through the analysis of human biometric traits has reached up to a mature level. However, the security and privacy of biometric templates for storage and communication is still a challenging problem [54]. The possible vulnerabilities in the existing biometric authentication systems have been explored in various recent studies [7,1,19], thus advocating that the security of biometric templates is an open research problem. It must be noted that biometric data needs special attention for its security because

* Corresponding author.
E-mail address: salman.khan@research.uwa.edu.au (S.H. Khan).

http://dx.doi.org/10.1016/j.patcog.2014.08.024
0031-3203/

standard encryption techniques (like RSA, DES and AES) cannot be employed in this case [3]. Mainly, this is due to the reason that template matching cannot be performed in encrypted domain since intra-user variability is not preserved.

The current need is to design security mechanisms that make use of multi-factor authentication in such a way that not only the user privacy is preserved but the biometric authentication is also accurate. A scheme for secure storage of user authentication template can be evaluated over a set of necessary requirements that ensures relatively foolproof template usage, handling and accessibility [26,4]. These requirements are:

- *Security*: The secured template should not leak the original authentication data and the user-specific factors. Privacy of each user should remain intact when data of one user is matched with other users.
- *Performance*: The performance of user authentication system using secure template must not seriously degrade in comparison to its non-secured counterparts. False reject rate (FRR) and false accept rate (FAR) should be as low as possible.
- *Renewability*: The secured template and the user-specific factors must be easily cancellable in an event of compromise. It should be possible to generate a new unique template when the same authentication data is provided.

In view of the aforementioned challenges and requirements, we present our template generation framework that applies random projections to biometric data (inherence factor), using secure keys derived from passwords (knowledge factor), to generate inherently secure, efficient and revocable/renewable biometric templates for user verification. We discuss how compressed sensing can weaken the security of randomly mapped biometric data. We apply an arithmetic hash function to further secure the mapping acquired after random projections. The key distinguishing feature of this novel scheme KRP−AH (Keyed Random Projections and Arithmetic Hashing) is its strength against attacks despite compromise of user specific key. Moreover, this scheme does not require the random subspace mapping to be strictly orthogonal as opposed to schemes that only consider orthogonal random projections for mapping biometric data [31,52]. Since our framework does not use error correcting codes or biohashing, there is no need to restrict real valued biometric signals to binary domain and this also helps in preserving security. The framework performs user authentication by using a bi-stage scheme requiring genuine biometric data and correct user specific key/password.

The rest of the paper is organized as follows. In Section 2, we describe the related work in the area of biometrics security. We formulate the mathematical constructs for the KRP−AH scheme in Section 3. The proposed framework architecture for the TFA utilizing KRP−AH scheme is presented in Section 4. Our scheme uses a novel operation named *Arithmetic Hashing* to strengthen the security of biometric templates. We discuss the security strengths of the framework against different attack scenarios in Section 5. To empirically establish that the generated secure biometric templates are still highly usable for authentication purposes, we evaluate the proposed framework in a TFA setup by using user passwords and dynamic handwritten signatures in Section 6. Unlike the traditional feature transformation techniques [20,35,29,25], our system preserves the important biometric information even when the user specific password is compromised. We have identified a number of local and global features related to dynamic signatures for template generation, and we use both dynamic and static distance measures to match the secure templates. We have evaluated the performance of the framework over three publicly available dynamic handwritten signature datasets. The results show that our proposed framework does not undermine the discriminating features of genuine and forged signatures and the verification performance is at par with the reported benchmark results. Finally, we conclude the paper with an outlook to future work.

2. Related work

The proposed scheme (KRP−AH) focuses on TFA by generating secure templates derived from user-provided password and biometric data. In this section, we discuss the related work in the literature that attempts to solve the problem of securing biometric data based authentication templates. Several schemes have been proposed to protect the biometric templates. These schemes can be broadly classified in to two categories: *Biometric cryptosystems* and *feature transformation schemes* [3]. The general idea is to store and process a variant of the original biometric so that an intruder cannot extract exact biometric data if he/she gets hold of a user's template.

Biometric cryptosystems combine biometrics with standard cryptographic techniques to generate data that can be used as a proof of user's identity. Error correcting codes are usually used to deal with the intra-user variability of templates during enrollment and verification process [30,55]. Biometric cryptosystems show good performance by preserving the inter-user variability [34]. However, these systems pose a difficulty in generating revocable templates that can be easily cancelled and reissued. In feature transformation techniques, instead of storing the original biometric data, transformation functions are applied on them. When the applied transformation is invertible, we call it *salting transform*. In case when an inversion is not possible, we call it *non-invertible transform*. In either case, the transformation is dependent on a randomly generated user specific key. These schemes have good revocability; however, their performance generally decreases with an increase in complexity level of transformation function. In the following discussion, we will discuss a brief overview and shortcomings of existing feature transformation schemes.

Orthonormal random projections are studied in [20] to secure biometric templates. A random multispace quantization technique is proposed in [52] to secure face biometrics by applying orthogonal random projections and biohashing. Similar to biohashing, palmhashing technique is presented in [29] to generate revocable palmcode using Gabor filters. However the security of all these salting transforms is dependent on the security of parameters that define user specific transformation characteristics. As an example, the above-mentioned techniques that employ random projections to map users' data are dependent on user specific key or token. They use key/token as a seed to generate random projections. When this key is compromised, the security gets weak and the intruder can recover original biometric either partially or completely.

The non-invertible transforms are applied in [28,25,56] for template protection of face and finger print biometrics. Maiorana et al. have used a signature transformation technique to secure online signature templates that can be matched via HMM [35]. A universal background model based approach is discussed in [4] for dynamic signatures protection. The problem with these techniques is their relatively low performance levels compared to salting transforms. Moreover, it is difficult to quantify the level of security provided by such techniques [3]. As an example, a revocable transform is applied on finger print templates in [49] which can be cracked by the technique proposed in [47].

Our method is inspired by the work of Feng et al. [13] that uses a hybrid mechanism consisting of random projections, discriminability preserving transform (DPT), and fuzzy commitment scheme to secure face templates. Whilst the hybrid approach successfully combines positives of biometric cryptosystems and feature transformation schemes, it is different from our approach in several ways.