Pattern Recognition 47 (2014) 3019–3033

Contents lists available at ScienceDirect

Pattern Recognition

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

Masquerade attack on transform-based binary-template protection based on perceptron learning

Yi C. Feng, Meng-Hui Lim, Pong C. Yuen*

Department of Computer Science, Hong Kong Baptist University, Kowloon Tong, Kowloon, Hong Kong

ARTICLE INFO

Article history:
Received 29 August 2013
Received in revised form
24 February 2014
Accepted 6 March 2014
Available online 15 March 2014

Keywords:
Masquerade attack
Binary
Template protection
Perceptron learning

ABSTRACT

With the increasing deployment of biometric systems, security of the biometric systems has become an essential issue to which serious attention has to be given. To prevent unauthorized access to a biometric system, protection has to be provided to the enrolled biometric templates so that if the database is compromised, the stored information will not enable any adversary to impersonate the victim in gaining an illegal access. In the past decade, transform-based template protection that stores binary one-way-transformed templates (e.g. Biohash) has appeared being one of the benchmark template protection techniques. While the security of such approach lies in the non-invertibility of the transform (e.g. given a transformed binary template, deriving the corresponding face image is infeasible), we will prove in this paper that, irrespective of whether the algorithm of transform-based approach is revealed, a synthetic face image can be constructed from the binary template and the stolen token (storing projection and discretization parameters) to obtain a highly-probable positive authentication response. Our proposed masquerade attack algorithms are mainly composed of a combination of perceptron learning and customized hill climbing algorithms. Experimental results show that our attack algorithms achieve very promising results where the best setting of our attack achieves 100% and 98.3% rank one recognition rates for the CMU PIE and FRGC databases correspondingly when the binarization algorithm (transformation plus discretization) is known; and 85.29% and 46.57% rank one recognition rates for the CMU PIE and FRGC databases correspondingly when the binarization algorithm is unknown.

1. Introduction

Widespread deployment of biometric system in various applications has given rise to public concerns over security of biometric templates. Potential attacks on biometric templates have been presented and summarized in [20]. Since compromise of users' biometric information is permanently irrevocable and irreplaceable, the enrollment biometric template used for query matching must not be stored in the clear without any protection.

To mitigate such a privacy threat, a variety of template protection schemes have been designed [29] and a set of criteria and metrics have been defined for standardizing evaluation of these template protection algorithms [31]. Most template protection schemes convert real-valued templates into binary [9,20,21,27,28,32–34] due to the following reasons: (1) Biometric system that outputs binary biometric representation can be simply integrated with existing cryptographic mechanisms which only accepts binary input. (2) Binary biometric representation enables verification/identification to be performed at an improved matching speed. (3) Binary biometric representation requires low storage capacity. These binary template protection schemes can generally be divided into three categories, namely a biometric cryptosystem [9,21,34], a transform-based approach [20,27,28,32,33] and a hybrid approach [14]. Instead of storing the enrolled biometric information, the biometric cryptosystem stores auxiliary information in the database, such that maliciously deriving information about the target biometrics or the binary template from such auxiliary information is infeasible. For instance, a fuzzy commitment scheme [21] stores a binary offset between a uniform binding key and the binary template. This auxiliary information is retrieved during query and is used to recover the binding key when the queried and enrolled biometric measurements are sufficiently similar. On the other hand, upon feature extraction, the transform-based approach applies a random orthogonal projection on the biometric features to ensure the non-invertibility of the transformed template. Then, the transformed template is discretized into a binary bit string and stored in the database. Henceforth, we term this two-stage transformation and discretization process as a "binarization" process. During query, the transformed binary template is retrieved for matching in order to authenticate/identify an identity. Due to high security level of

* Corresponding author. Tel.: +852 3411 2387.
E-mail addresses: ycfeng@comp.hkbu.edu.hk (Y.C. Feng), menghuilim@comp.hkbu.edu.hk (M.-H. Lim), pcyuen@comp.hkbu.edu.hk (P.C. Yuen).

http://dx.doi.org/10.1016/j.patcog.2014.03.003
0031-3203/© 2014 Elsevier Ltd. All rights reserved.

biometric cryptosystem and decent cancelability of the transform-based approach, the hybrid approach combines both approaches to enjoy these advantages.

The transform-based approach is commonly adopted in both biometric verification and identification systems. This stems from the fact that the transform-based approach stores binary template and thus being able to produce matching scores as a system output via comparing the query template with the stored template. A well-known example of transform-based approach is Biohash [32], in which the extracted features $\mathbf{x}_i$ of the ith user $(i=1,2,\dots,n_{stolen})$ are first projected onto a new domain via

$$z_p=\mathbf{w}_p^T\mathbf{x}_i\ (p=1,2,\dots,n_{bin}) \tag{1}$$

where $\mathbf{w}_p$ is the pth orthogonal projection vector and z_p represents the pth component of the transformed template. Based on a threshold t_p, z_p is then discretized into a binary bit via

$$B_p(\mathbf{x}_i)=\begin{cases}1: z_p=\mathbf{w}_p^T\mathbf{x}_i+t_p>0\\ 0: z_p=\mathbf{w}_p^T\mathbf{x}_i+t_p\le 0\end{cases}\quad (p=1,2,\dots,n_{bin}) \tag{2}$$

where $B_p(\cdot)$ for $p=1,2,\dots,n_{bin}$ represents a one-way binarization function. A concatenation of $B_p(\mathbf{x}_i)$ over p forms the n_{bin}-bit final binary template that is commonly stored in the database. In practice, the projection vectors and the discretization thresholds $\{\mathbf{w}_p,t_p|p=1,2,\dots,n_{bin}\}$ are usually stored in a smart card or a token which is given to the user during enrollment. Alternatively, a system may only store projection vectors $\mathbf{w}_p$ in a token/smart card and employ a single discretization threshold t for all users and all feature components (e.g. through appropriate normalization). This paper considers the former.

While the transform-based approach offers cancelability in nature, the security of transform-based approach lies in the non-invertibility of the transformation. In the case of security breach of the system, it is believed that the stolen binary template does not leak any information about the biometric information. Therefore, it should be computationally hard for any illegitimate user to retrieve the authentic biometric data so as to masquerade a user in an authentication session.

In this paper, we rebut such a presumption by demonstrating how the security of a biometric system that adopts a transform-based binary template protection approach can be penetrated if the stored template is disclosed to the adversary. More specifically, by adopting face biometric as a subject of study due to its universal and non-intrusive characteristics, we develop perceptron-learning-based masquerade attacks to construct a synthetic face image and impersonate the target user in gaining illegal access to the system. While the fabricated face image could be quite different from the actual one, it is highly probable the transformed binary template would resemble the target binary template in the database.

Table 1 lists out the existing masquerade attacks in comparison to our attack. Essentially, our masquerade attacks can be distinguished from the existing attacks in three aspects:

(1) Our masquerade attack in the second scenario can be adopted against general transform-based template protection schemes [14,25,32,33]; while the listed existing attacks are only applicable to a specific type of biometric scheme.

(2) In both scenarios, the iterative processing in the generation of synthetic face image in our masquerade attacks can be carried out completely offline. Hence, the excessive queries led by the offline iterative hill climbing process of the masquerade attack will not only be restricted by the maximum number of trials allowed in a system access session, but also will not generate any online attack pattern that would result in a security breach alert. This makes our attacks far more feasible than masquerade attacks that requires online iterative processing.

(3) Unlike two existing attacks [22,26] against Biohash, we do not make the following less-realistic assumptions in our masquerade attacks:

   (a) *The binarization parameters (e.g. orthogonal projection matrix* **W** *and discretization threshold* t_p*) are always revealed under the stolen token scenario.*
   In actuality, security tokens (and smart cards) are mostly tamper-resistant [38,39], which strictly prevents adversaries from retrieving any information from the stolen token. As such, elements in the projection matrices can rarely be obtained, even if the adversary is in possession of the token and feature extractor. Evidently, in such a case, the existing attacks [22,26] cannot be applied without complete knowledge of the binarization parameters.

   (b) *The binarization algorithm is always known when the system is compromised.*
   As there are increasing flavors of discretization algorithms being proposed from time to time [4–6,23], a system designer may not follow the single-bit discretization process in the original transform-based approach. Instead, he may adopt a more effective multi-bits discretization method with [5,6,23] or without [4,32] bit allocation procedures in order to achieve better recognition performance. Furthermore, the discretization algorithm is often protected by some means such that even if the system is compromised, retrieval of the relevant algorithm code will not be feasible. Hence, in such situations, it could be

Table 1
Existing masquerade attacks.

Target scheme	Synthetic image construction for masquerade attack	Iterative processing
IrisCode [8]	Genetic algorithm [15]	Online
Minutia-based fingerprint authentication [24]	Hill-climbing [35]	Online
	Minutiae-prototype positioning and iterative pattern growing with necessary pre- and post-processing [3]	Online
Biohash [32]	Solve a constrained minimization of distance between the estimated feature vector and an unrelated feature vector [26]	N/A
	Multiply the pseudo-inverse of the transformation matrix by the discrete output vector [22]	N/A
	Perceptron-learning with hill-climbing (Scenario 1 of our attack)	Offline
General transform-based template protection (e.g., Biohash [32], Multi-stage Biohash [33], Descriptor Binarization [25] and Discriminability Preserving [14])	MLP modeling with customized hill-climbing (Scenario 2 of our attack)	Offline