A NOVEL PARAMETER MANAGEMENT APPROACH FOR REMOTE CANCELABLE BIOMETRICS

Neha Dahiya*

Dr. Chander Kant**

Abstract

Protecting biometric information is key concern in biometric systems, since physical characteristics such as fingerprint, irises, face and vein patterns cannot be changed or revoked like passwords. As a solution to this problem, an authentication model called Cancelable biometrics has been studied, in which the biometric features are transformed by a kind of encryption or one-way function and matched without restoring the original features. In this transformation a user specific parameter or key is used. The security of template formed after transformation depends on the security of parameter used. In this paper, we review several naive models for parameter management. Some of the limitation and overhead in the models is enlightened and to remove it we propose a novel parameter management model based on server-side parameter management and authentication protocols. The proposed parameter management model makes it possible to realize a cancelable biometric authentication system with high usability and security with minimal overhead.

* M.Tech. Student, Department of Computer Science and Applications K.U., Kurukshetra, Haryana, INDIA.

** Assistant Professor, Department of Computer Science and Applications K.U., Kurukshetra, Haryana, INDIA.

I. Introduction

Identifying a person is not a difficult task, biometric verification technology, automatically identifies a person based on his/her physical or behavioural features. These can be used for user authentication in various applications such as physical access control and computer login. In the future, it is expected to be applied to remote user authentication over the network, e.g. for Internet banking, e-commerce, and various cloud services. A typical remote biometric authentication system is based on client server model which consists of an authentication server and client terminals with biometric sensors [1]. The server keeps biometric feature data associated with user IDs, which are known as templates, in a database.

There are some problems here[2]. The first is a security issue: because biometric features such as fingerprint patterns are unchangeable, unlike passwords, they cannot be changed or Revoked even if the templates or feature data are compromised. The second is a privacy issue: biometric information is strongly linked to a person's identity, so some users does not feel safe to reveal their biometric data to the server over the network. Conventional biometric system that works on network uses encryption and cryptography as a security tool and solution to these problems. Encryption done at client side needs decryption at server side for pattern matching at time of authentication. Attacker who aims at this timing or a malicious administrator of the server can acquire the original templates. To solve this problem, some biometric template protection models have been introduced. These models can be broadly classified into two categories, i.e. feature transformation and biometric cryptosystems [3]. The biometric cryptosystems [4], such as ones using fuzzy vault [5], take an approach of extracting stable binary representation from noisy biometrics data (biometric key generation),and using it as a cryptographic key or a password. However, since most biometric key generation methods rely on error correcting code theory, the performance, i.e. the false rejection rate (FRR) and false acceptance rate (FAR), of biometric cryptosystems is limited by the error-correcting capability. Generating a stable key from noisy biometric data with practical performance is a major challenge in this approach. The feature transformation approach was firstly proposed by Ratha, et. al. [6], named Cancelable biometrics.

In Cancelable biometrics,[7], biometric features are transformed and matched in the transformed domain directly without restoring the original feature. The transformation function is determined by a (typically user specific) parameter, which may be a set of multiple parameter

values. The parameter plays a similar role as an encryption key. Even if the transformed template or the parameter is compromised, they can be revoked by changing the parameter and reissuing a transformed template via the new parameter, without changing the original biometric feature. Some methods of Cancelable biometrics have potential to take advantage of sophisticated conventional matchers with practical accuracy. In addition, several transformations are considered to have high security in the sense that it is impossible or computationally hard to restore or guess the original feature from a transformed template without knowing the parameter. In fact, for many methods invert the transformed template when the parameter is known. Though several techniques for one-way transformation are proposed, recent studies reported that some of them have vulnerabilities in the sense that it is easy to find either a close approximation of the original template or a pre-image of the transformed template. [8]-[9]

Finding a feature similar to one of the pre-images of a transformed template sufficient for impersonation is not hard unless the FAR is extremely low. Otherwise, an attacker can perform the following dictionary attack: for each sample from sufficiently large biometric database of real or artificially generated features, the attacker transforms the sample and compares it to the transformed template. This process is repeated until the similarity exceeds the threshold value. The expected trial number of this attack can be estimated by 1/ FAR under the assumption of independent Bernoulli trials with success probability FAR. Note that this attack can be performed offline, i.e. without accessing the server, when both the transformed template and the corresponding parameter are known. Thus, it is much more serious than online dictionary attacks which can be prevented, e.g., by locking the system or alarming after some number of consecutive authentication failures.

Furthermore, it should also be noted that the many-to-one property, which is typically used as the foundation of onewayness of transformations, inevitably decreases the information content of biometric features and reduces the discrimination ability. Constructing secure one-way transformations for Cancelable biometrics without degrading the performance is still a challenging problem. Nevertheless, it is a mistake to think that it is impossible to construct secure Cancelable biometric systems just because the transformations are not one-way. What is important in Cancelable biometrics is to manage the parameter securely in order not to be

compromised simultaneously with the transformed template. However, little attention has been given so far to the parameter management problem of Cancelable biometrics.

In this paper, we review several naive models for parameter management. Some of the limitation and overhead in the models is enlightened and to remove it we propose a novel parameter management model based on SOS Model combined with concept of partial transformation. The proposed parameter management model makes it possible to realize a Cancelable biometric authentication system with high usability and security with minimal overhead.

II. Parameter management models in cancelable biometrics

In this section, we explain three naive parameter management models [10] based on the following system models: (1) Store on Client (SOC) model, (2) Store on Token (SOT) model and (3) Password Based Parameter Generation (PBPG) model, (4)Store on Server (SOS) model and describe enrolment and authentication protocols for each model.

A. Store on Client

In the SOC model, the parameter is stored and managed in the client such as PCs, mobile terminals and sensor devices. At the time of enrolment, the enrolment client extracts a template from biometric information captured from a user, and transform it by a randomly chosen parameter . The transformed template is sent to the server, and stored in the database associated with the user ID. The parameter is stored in the authentication client associated with the ID. At the time of authentication, the authentication client extracts a feature that is transformed using the parameter stored in the client, and sent to the server. The server decides "match" (acceptance) or "no match" (rejection).

B. Store on Token

In the SOT model, the parameter is stored in hardware token such as a smart card and a USB token, and managed by each user. The protocols are the same as those of the SOC model except that the parameter is stored in hardware token and issued to the user during the enrolment process. At the time of authentication, the parameter is loaded from the token presented by the user. The SOT model can be viewed as two-factor authentication using a hardware token and

biometrics if it is sufficiently hard to impersonate a user without knowing both the biometric feature and the parameter. From another point of view, however, the SOT model reduces the usability of the authentication system because it requires a user to carry a hardware token which are easily lost or forgotten at home.

C. Password-based parameter generation

The PBPG model is similar to well-known password based encryption (PBE) . In this model, the parameter is generated from user's secret knowledge such as a password. Fig.3 shows an overview of the PBPG model. At the time of both enrolment and authentication, the user inputs some secret knowledge such as a password as well as biometric information. The password is fed into a mixing function (e.g., based on a secure hash), to generate a parameter to transform the template or the feature. In the same manner as in the PBE, a random string called a salt can be added to the password to prevent pre-calculated dictionary attacks. As with the SOC model, the PBPG model can also be viewed as two-factor authentication using passwords and biometrics if it is sufficiently hard to impersonate a user without knowing both the biometric feature and the parameter. Note, however, easy-to-remember passwords will not have enough complexity against dictionary attacks to recover the original template from the transformed one. Sufficiently complex passwords are required to secure the template, which would reduce the usability of the authentication system.

D. Store on Server

In SOS model , the authentication system consists of enrolment clients, authentication clients, an authentication server and a parameter management server. The parameter management server stores the parameters of all users, while the authentication server stores the transformed templates, both associated with the user IDs. We assume that the following requirements are fulfilled. The authentication server and the parameter management server are administered separately by different administrators or organizations, and they do not collude with each other. This requirement is necessary because if the parameters and transformed templates are compromised at once, the original templates can be recovered.

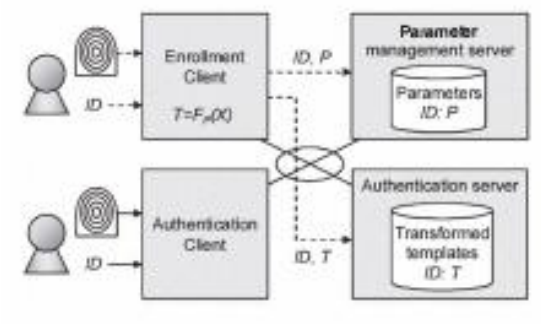

Fig. 1 Store on Server

Three protocols were developed for SOS authentication. In First Protocol, assume the transformation function F* and the parameter space P satisfies the following mathematical conditions:

Cond.l: For any PI, P2 E P, there exists Q E P such that Fp1 (Fp2 (X)) = FQ(X) for any biometric template or feature X (i.e., closure property of parameters under function composition).[12]

Basically in this protocol, the parameter management server chooses Q E P randomly and generates a one-time parameter R = QoP based on the original parameter P associated with the ID. The R is sent back to the client, and Q is sent to the authentication server. The client extracts a feature data Y from the biometric information, transform it to V = FR(Y) using the onetime parameter R, and send it to the authentication server. The authentication server generates a one-time template U = FQ(T) and matches it to V to decide acceptance or rejection

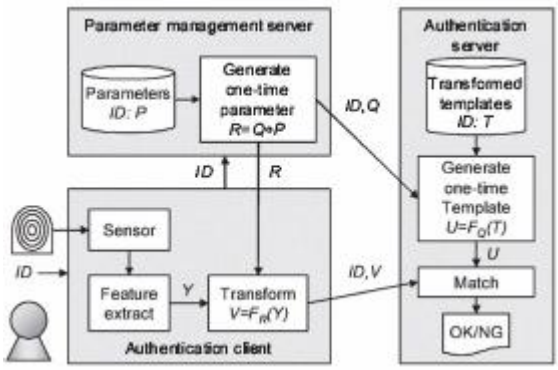

Fig. 2 Protocol 1

Second Protocol, assume the following condition for F* and P.

Cond.2: For any P E P, there exists Q E P such that FQ(Fp(X)) = X for any X (i.e., existence of an inverse element).

In this protocol, the client chooses a one-time parameter Q E P randomly and sends it to the parameter management server. Then the client extracts a feature data Y from the biometric information, transform it to V = F Q (Y) using the one-time parameter Q, and send it to the authentication server. The parameter management server generates a differential parameter D = Q 0 p-l based on the original parameter P associated with the ID, and send it to the authentication server. The authentication server generates a one-time template U = FD(T) (= FQ(Fp-l(Fp(X))) = FQ(X)) and matches it to V = FQ(Y) to decide acceptance or rejection.

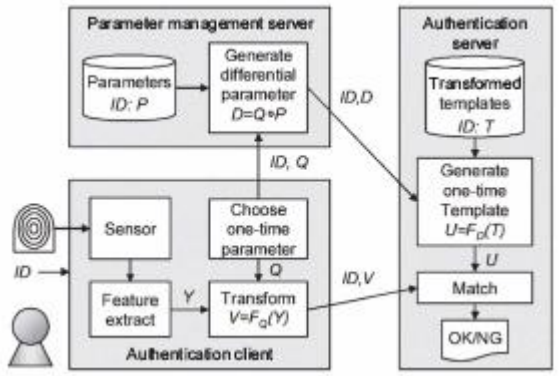

Fig. 3 Protocol 2

While Third Protocol, assume the following condition for F* and P, instead of the Cond.l and Cond.2

Cond.3: For any PI, P2 E P, Fp1 (Fp2(X)) = Fp2(Fp1 (X)) holds for any X (Le., commutative property for function composition).

In this protocol , the client chooses a one-time parameter Q E P randomly and send it to the authentication server. Then the client extracts a feature data Y from the biometric information, transform it to V = FQ(Y), and send it to the parameter management server. The parameter management server transforms V to W =Fp(V) using the parameter P associated with the 10, and

send W to the authentication server. The authentication server generates a one-time template U = FQ(T) and matches it to W to decide acceptance or rejection.

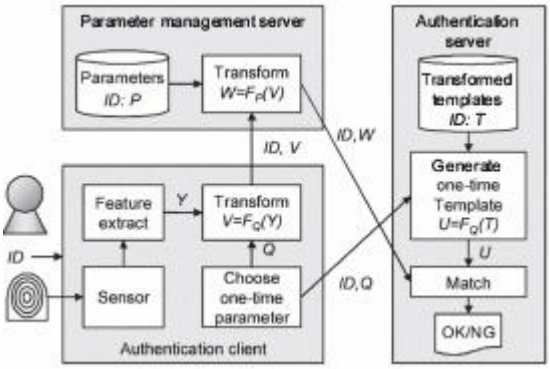

Fig. 4 Protocol 3

III. Proposed Work

Storing the parameter on server was right decision but the authentication protocols have overhead of repeated transformation both at client and both the server. To create, store and manage one time template and on time parameter was also overhead on the system and also original template has to undergo transformation each time authentication is done. To solve this issue a novel parameter management model based on Store on Sever (SOS) model is being proposed.

In this protocol, we assume the following condition for F* and P,

Cond *: For any P, there exist p1 and p2 such that p1+p2=P. And Fp2(Fp1 (X)) = Fp(X) holds for any X .

In our proposed scheme, Parameter (P) is randomly divided into two sub parameters (P1, P2).Transformation of the feature extracted during authentication is a two step process. Partial transformation using parameter P1 is done on authentication client and rest transformation using the parameter P2 is done on parameter management server.

We assume that the following requirements are fulfilled.

- The authentication server and the parameter management server are administered separately by different administrators or organizations, and they do not collude with each other. This

requirement is necessary because if the parameters and transformed templates are compromised at once, the original templates can be recovered.

- The communication channel between each pair of entities of the system (e.g., between an authentication client and the parameter management server, between the authentication server and the parameter management server, and so on) is encrypted independently, e.g. by SSL.[11] Thus, for example, the parameter management server cannot eavesdrop the communication between an authentication client and the authentication server. This requirement is necessary to prevent recovery of the original biometric features or templates from the transmitted data over the channel.
- The enrolment clients are securely managed and trustworthy.
- The authentication clients are tamper evident so that users or operators can easily find unauthorized alternations, e.g. by security seals to detect physical tampering and cryptographic signatures to detect logical tampering.

Fig. 6 shows an overview of the SOS model with partial transformation.

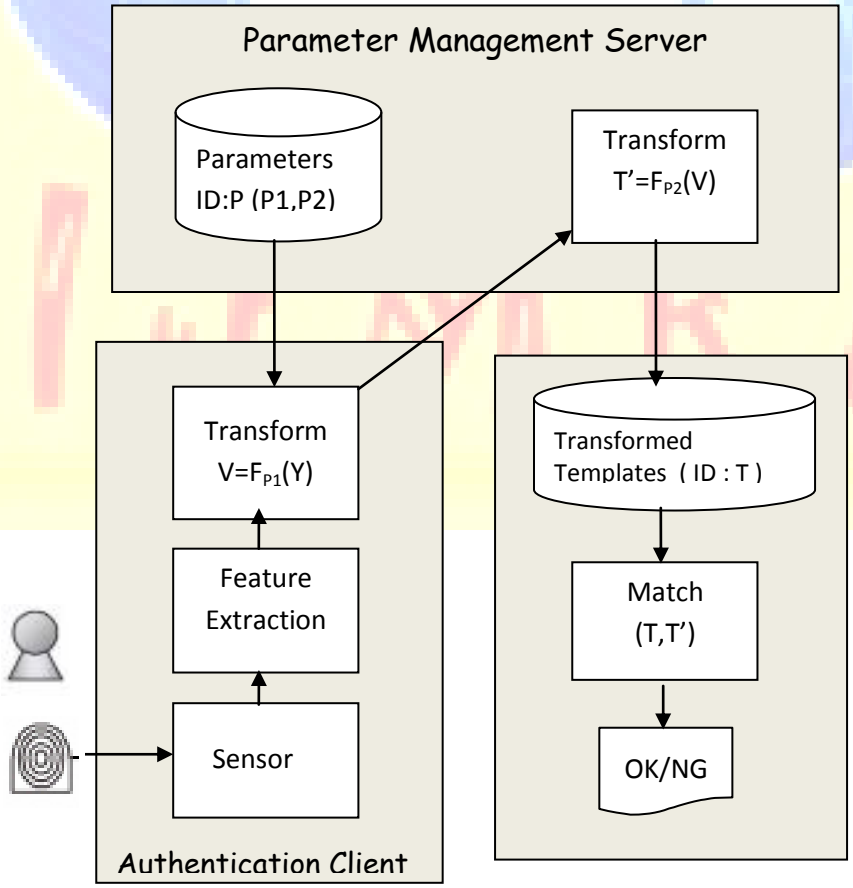

Fig. 6 Store on server with partial Transormation

The enrolment protocol for the proposed model is as follows.

1. A user presents his/her biometric information and inputs the user ID to an enrolment client.
2. The enrolment client chooses a parameter P randomly and sends it to the parameter management server.
3. The parameter management server stores the parameter P associated with the ID.
4. The enrolment client extracts a template X from the biometric information, transform it to T = Fp (X) using the parameter P, and send it to the authentication server.
5. The authentication server stores the transformed template T associated with the ID.
6. The original template X is cleaned up from the enrolment terminal.

The authentication protocol for the proposed model is as follows.

1. A user presents his/her biometric information and inputs the user ID to an authentication client.
2. The authentication client sends the ID to the parameter management server.
3. The parameter management server sends the parameter p1 to the client.
4. The client extracts a feature data Y from the biometric information, transform it to V = Fp1(Y) using the parameter p1, and send it to the Parameter management server.
5. The Parameter management server, Transform it to T'=Fp2(V) using parameter p2,and send it to authentication server.
6. The authentication server matches the transformed template T to the transformed feature T', and decides whether to accept or reject the user.
7. The original feature Y and the transformed one T' are cleaned up from the system.

IV. Comparison of authentication protocols for parameter management

The SOS scheme can be applied for any application requiring usability, i.e. without smart cards or passwords, and availability from any authentication client, such as a kiosk terminal, a

shared office PC, and an amusement facility. Now, considering the SOS scheme, the authentication protocols are studied. Earlier protocols in SOS authentication put overhead of one time template and one time parameter, which is removed in proposed approach. Parameter management server maintains parameter and parameter once stored as whole does not move out from it that makes it less prone to communication attacks. Earlier authentication protocols put extra work load on Authentication server, but in proposed scheme authentication server has to just match the templates and give result. Repeated Transformation of original template is also not needed which increase the security and reduce the work load on the authentication server.

Generating a parameter in protocol 2 and a differential parameter in protocol 3 was a tedious task. Therefore, in proposed scheme this work load is removed by just splitting the parameter (P) into two (P1,P2) satisfying cond* mentioned above. This makes transformation during authentication a two step process. Partial transformation using parameter P1 is done on authentication client and rest transformation using the parameter P2 is done on parameter management server.

V. Conclusion

Parameter management is a critical issue for Cancelable biometrics to ensure security and privacy of biometric information. In this paper, we firstly reviewed several naive schemes for parameter management: the Store on Client (SOC), Store on Token (SOT) and Password-Based Parameter Generation (PBPG). All these schemes, however, have limitations in usability; the SOC scheme limits the available authentication clients, the SOT scheme requires a user to carry a hardware token, and the PBPG scheme requires a user to remember a password. Another parameter management scheme, i.e., the Store on Server (SOS), with high usability and security was studied. In this scheme, the parameters are stored in a parameter management server administered separately from the authentication server which manages the transformed templates. However, authentication protocol for the SOS scheme has vulnerability that the parameters are easily compromised from authentication clients. Some protocols where one-time parameters and one-time templates, which are valid during an authentication session only, are used to transform the biometric feature. This increases the overhead of transformation and parameter generation. To deal with this problem we proposed a naive parameter management model based on SOS.

Concept of partial transformation was used in it that reduces the overhead of parameter generation and repeated template transformation. Finally we compared the parameter management schemes and discussed the advantages and disadvantages. The results will be a guide to the design of Cancelable biometric authentication systems.

VI. References

[1] P. Reid, Biometrics for Network Security. Prentice Hall PTR, 2003.

[2] Chander Kant, Rajender Nath, Sheetal Chaudhary" Challenges in Biometrics: proceeding of the International Conference on Emerging trends in Computer Science & IT organized by ALFALAH school of Engineering & Tech, Faridabad, PP69-77, 23 Apr 2008

[3] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP Journal on Advances in Signal Processing, 2008.

[4] U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosysterns: Issues and challenges," Proc. IEEE, vol. 92, no. 6, pp. 948-960,2004.

[5] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. on Information Forensics and Security, vol. 2, pp. 744-757, 2007.

[6] N. K. Ratha, 1. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometric-based authentication systems," IBM System Journal, vol. 40, no. 3, 200 I.

[7] Chander Kant, Rajender Nath, " Protection of Database Template using Cancelable Biometrics" proceeding of the IEEE Advanced Computing Conference, organized by Thapar University Patiala,6-7 March,2009

[8]M. Braithwaite, U. C. von Seelen, J. Cambier, J. Daugman, R. Glass, R. Moore, and I. Scott, "Application-specific biometric templates," in AutoID02, 2002, pp. 167-171

[9] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," in Media Forensics and Security '/0, 2010.

[10] K. Takahashi and S. Hirata, "Parameter management schemes for Cancelable biometrics", In IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM2011), 2011.

[11] K. Takahashi, "Unconditionally Provably Secure Cancelable Biometrics Based on a Quotient Polynomial Ring", In International Joint Conference on Biometrics 2011 (IJCB2011), 2011.

[12] S. Z. Li and A. K. Jain, Eds., Encyclopedia of Biometrics. Springer US, 2009.