A Multi-factor Biometric Based Remote Authentication Using Fuzzy Commitment and Non-invertible Transformation

Thi Ai Thao Nguyen(✉), Dinh Thanh Nguyen, and Tran Khanh Dang

Ho Chi Minh City University of Technology, VNU-HCM,
Ho Chi Minh City, Vietnam
{thaonguyen,dinhthanh,khanh}@cse.hcmut.edu.vn

Abstract. Biometric-based authentication system offers more undeniable benefits to users than traditional authentication system. However, biometric features seem to be very vulnerable - easily affected by different attacks, especially those happening over transmission network. In this work, we have proposed a novel multi-factor biometric based remote authentication protocol. This protocol is not only resistant against attacks on the network but also protects biometric templates stored in the server's database, thanks to the combination of fuzzy commitment and non-invertible transformation technologies. The notable feature of this work as compared to previous biometric based remote authentication protocols is its ability to defend insider attack. The server's administrator is incapable of utilizing information saved in the database by client to impersonate him/her and deceive the system. In addition, the performance of the system is maintained with the support of random orthonormal project, which reduces computational complexity while preserving its accuracy.

Keywords: Remote authentication · Biometric template protection · Biometric authentication · Fuzzy commitment · Orthonormal matrix

1 Introduction

In modern world, services for people's daily needs are being digitalized. E-commerce happens everywhere, in every aspect of life. As e-commerce is being used as widely as of today, an essential need for its long survival, beside quality, is security. The first security method to be mentioned is authentication. Traditional authentication method that most e-commerce providers are using is username/password. However, this method is revealing its natural setbacks. Password cannot identify legal user with an imposter who is able to access to user's password. Besides, the more complicated – more secured a password is, the harder it is for users to remember. That is to say, a "true" password is difficult for people to remember but easy for computer to figure out. Especially, with recent technology development, computer ability is being enhanced; meaning password cracking chance is rising too. For that reason, biometric based authentication method was born; with its advantages, this method is gradually replacing its predecessor. The first advantage to be mentioned is that biometric (such as face, voice, iris, fingerprint, palm-print, gait, signature,…) reflects a specific individual

I. Khalil et al. (Eds.): ICT-EurAsia 2015 and CONFENIS 2015, LNCS 9357, pp. 77–88, 2015.
DOI: 10.1007/978-3-319-24315-3_8

which helps preventing multi-user usage from one account [1]. Moreover, using biometric method is more convenient for users since they do not have to remember or carry it with them.

However, advantages are accompanied with challenges. Usage of method related to biometric requires technology to eliminate interferences happening when the sensor process biometric features. Beside, concerns of security and privacy, especially in remote architecture, are also put on table. The fact that human has a limited number of biometric traits makes users cannot change their biometric over and over like password once it is compromised [2]. Moreover, some sensitive information could be revealed if biometric templates are stored in database server without strong security techniques. In this case, the user's privacy could be violated when the attackers can track their activities by means of cross-matching when a user employs the same biometrics across all applications. Therefore, all the authenticating servers should not be trustworthy to process a user's plaint biometric, and the level of trust of these servers should be discussed more. Last but not least, the network security is also the important component in biometric based remote authentication scheme. When the authentication process is carried out over an insecure network, anyone with their curiosity can approach the biometric information transmitted [3].

The goal of this study is to present an effective approach for preserving privacy in biometric based remote authentication system. Concretely, biometric template stored in database is protected against the leakage private information while preserving the revocability property. Besides preventing the outside attacks, proposed protocol is also resistant to the attacks from inside.

The remaining parts of this paper are organized as follows. In the Sect. 2, related works is briefly reviewed. We show what previous works have done and their limitations. From that point, we present our motivation to fill the gap. In Sect. 3, we introduce the preliminaries and notations used in the proposal. In the next section, our proposed protocol is described in detail. In the Sect. 5, the security analysis is presented to demonstrate for our proposal. Finally, the conclusion and future work are included in the Sect. 6.

2 Related Works

Over the years, there have been plenty of works which research on preserving privacy in biometric based authentication system. Biometric template protection is one of indispensable part to this research field. In [4], Jain et al. presented a detailed survey of various biometric template protection schemes and discussed their strengths and weaknesses in light of the security and accuracy dilemma. There are two approaches to deal with this issue, including feature transformation and biometric cryptosystem. The first approach identified as feature transform allows users to replace a compromised biometric template while reducing the amount of information revealed. However, some methods of the approach cannot achieve an acceptable performance; others are unrealistic under assumptions from a practical view point [3]. The other approach tries to combine the biometrics and cryptography technique in order to take advantages of both. The schemes employing these methods aim at generating a key, which derived from the biometric tem-plate or bound with the biometric template, and some helper data. Both the biometric template and the key are then discarded, only the helper data is stored in the database for reproducing the biometric or the secret key later. Nevertheless, the biometric cryptosystem seem to lose the revocability property that requires the ability to revoke a compromised template and reissue a new one based on the same biometric data. On this account, some recent studies tend to integrate the advantages of both approaches to enhance only the security but also the performance of the system. The combination of secure sketch and ANN (Artificial Neural Network) was proposed in [5]. The fuzzy Vault was combined with Periodic Function-Based Transformation in [6], or with the non-invertible transformation to conduct a secure online authentication in [7]. The homomorphic cryptosystem was employed in fuzzy commitment scheme to achieve the blind authentication in [8]. In this paper, we try to integrate the ideal of fuzzy commitment and the non-invertible transformation to guarantee the security for user's biometric template.

In recent years, many biometric based remote authentication protocols have been proposed. However, most previous protocols only protect the client side and the transmission channel, neglecting the server side. In [9], the authors utilizes Biometric Encryption Key (BEK) to encrypt Private Key and safeguard Private Key. The BioPKI system proposed in the paper turned around the security of private key, and left the biometric feature out security aspect.

In 2010, Kai Xi et al. proposed a bio-cryptographic security protocol for remote authentication in mobile computing environment. In this protocol, fingerprint was used for verification, and the genuine points were protected by the fuzzy vault technique which inserts randomly a great number of chaff points into the set of genuine points. All elements in the newly created set were given index numbers. The server only stored the index numbers of all genuine points. The communication between client and server was protected a Public Key Infrastructure (PKI) scheme, Elliptic Curve Cryptography (ECC) which offered low computational powers with the same security strength as the RSA. However, the authors focused only on the security of the client side (mobile devices) and the transmission channel. The server was supposed to have higher security strength, so the authors did not care about the attacks on the server or even the attacks from the server. In addition, the authors argued that to prevent replay attack and brute force attack, a biometric-based session key was generated separately from the set of a genuine points; nonetheless, the server only had the list of index numbers of these points so it was unable to generate the key independently as described in [10].

In 2013, Hisham et al. presented another approach that combined steganography and biometric cryptosystem in order to obtain the secure mutual authentication and key exchange between client and server in remote architecture [11]. In this paper, the authors provided some references for proving that hiding biometric data in a cover image based on steganography technique can increase the security of transferring biometric data between unsecure networks [12]. Moreover, in order to protect biometric template stored in the authentication server while preserving the revocability property, the protocol employed the invertible transformation technique using random orthonormal matrices to project biometric feature vectors into other spaces while preserving the original distances. The new approach obtained not only the secure mutual authentication but also the immunity from replay and other remote attacks. However, the authors have not considered the ability that the authentication server itself stoles the data in its own database to impersonate its users in order to conduct the illegal transactions. This attack will be particularly dangerous in case that server is bank. The bank with its dark intention is totally free to impersonate its customers. It abused its privileges to login into customers' accounts, draw all money and leave no guilty evidence. Nonetheless, almost current researches only focus on biometric template protection or how to defend against the attack from outside; they have not spent enough concerns for the attacks from inside yet. More concretely speaking, the ability that the server accesses into the system on behalf of a user and carries out some criminal actions should be taken into account.

In addition, the scalability property needs to be discussed more in the remote authentication architecture. When the number of users and the number of servers is growing, the number of templates which belongs to a user is large, and each server has to remember every user's template. That design makes the system vulnerable and wastes our resources. To guarantee the scalability properties, Fengling et al. presented a biometric based remote authentication which employed the Kerberos protocol [13]. A biometric-Kerberos authentication protocol was suitable for e-commerce applications. The benefit of Kerberos is that expensive session-based user authentication can be separated from cheaper ticket-based resource access. However, the Achilles' heel of the proposed scheme is Key Distributed Center (KDC) – authentication server which is supposed to be trusted. Therefore, there were no techniques protecting the private information of client against the insider attacks.

The contribution of this work is that we propose the biometric-based remote authentication protocol which has the ability to prevent an authentication server from impersonating its clients. In addition, the proposal is resistant to the outside attacks from an insecure network by combining the orthonormal random project with the fuzzy commitment scheme. The mutual authentication and the key agreement are also guaranteed in this protocol.

3 Preliminaries and Notations

3.1 Fuzzy Commitment Scheme

Fuzzy commitment scheme as proposed in [14] belongs to the first class of biometric cryptosystem approach. It is the combination two popular techniques in the areas of Error Correcting Codes (ECC) and cryptography. To understand how fuzzy commitment scheme works, we have to learn about ECC. Formally speaking, ECC plays a central role in the fuzzy commitment scheme. An ECC contains a set of code-words $\mathtt{C}\subseteq\{0,1\}^n$ and a function to map a message to a code-word before it is transmitted along a noisy channel. Given the message space $\mathcal{M} = \{0,1\}^n$, we define the translation function (or encoding function) $g : \mathcal{M} \rightarrow \mathtt{C}$, and the decoding function $f : \{0,1\}^n \rightarrow \mathcal{M}$. Therefore, g is a map from $\mathcal{M}$ to $\mathtt{C}$; however, f is not the inverse map from $\mathtt{C}$ to $\mathcal{M}$ but a map from arbitrary n-bit strings to the nearest code-word in $\mathtt{C}$.

In fuzzy commitment scheme, a biometric data is treated as a corrupted code-word. During registration stage, a client provides biometric template B to server. Server

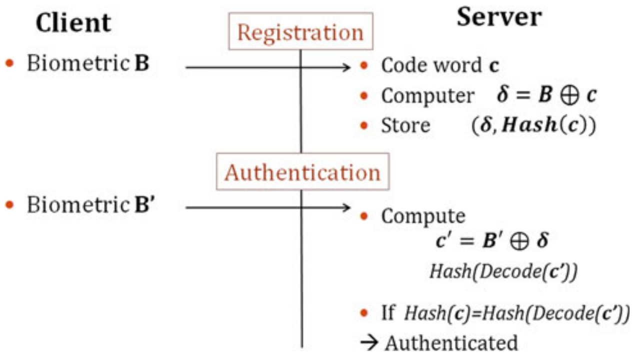

Fig. 1. Fuzzy commitment scheme.

randomly picks a code-word c then calculates $= B \oplus c$, and the hash version of code-word c. Next, server stores the pair of $(\delta, Hash(c))$ into the database. During authentication stage, a new biometric with noise *B'* is distributed to server by the client. From its side, server calculates $c^{'} = B^{'} \oplus \delta$, proceeds decoding *c'*, then compares hash version of the result with $Hash(c)$ previously stored in the database. If the two are matched, client is authenticated. This process is demonstrated in Fig. 1.

3.2 Orthonormal Random Projection

Random Orthonormal Projection (ROP) is a technique that utilizes an orthonormal matrix to project a set of points into other space while preserving the distances between points. In the categorization of template protection schemes proposed by Jain [4], ROP belongs to the non-invertible transformation approach. It meets the revocability requirement by mapping a biometric feature into a secure domain through an orthonormal matrix. The method to effectively deliver orthonormal matrix was introduced in [15]. It can be used to replace traditional method of Gram-Schmidt. Given the biometric feature vector x of size $2n$, orthonormal random matrix A of size $2n \times 2n$, random vector b of size $2n$, we have the transformation $y = Ax + b$.

The orthonormal matrix A of size $2n \times 2n$ owns a diagonal which is a set of n orthonormal matrix of size $n \times n$. The other entries of A are zeros. We present the example of matrix A in (1) where the values $\{\theta_1, \theta_2, \ldots, \theta_n\}$ are the random numbers in the range $[0 : 2\pi]$

$$A = \begin{bmatrix} \cos\theta_1 & \sin\theta_1 & 0 & 0 & 0 & 0 \\ -\sin\theta_1 & \cos\theta_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cos\theta_2 & \sin\theta_2 & 0 & 0 \\ 0 & 0 & -\sin\theta_2 & \cos\theta_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cos\theta_n & \sin\theta_n \\ 0 & 0 & 0 & 0 & -\sin\theta_n & \cos\theta_n \end{bmatrix} \tag{1}$$

By using this technique to produce the orthonormal matrix, there is no need for a complex process such as Gram-Schmidt. Beside its effectiveness in computational complexity, it can also improve the security while guaranteeing intra-class variation. When client is in doubt of his template getting exposed, he only needs to create another orthonormal matrix *A* to gain a new transformed template.

3.3 Notations

In the rest of the paper, we will use the following notations:

- B is a biometric feature vector of a client
- M is an orthonormal matrix that a client creates.
- $\mathrm{B_{TC}}$ is a transformed biometric stored in the database as a template.
- H(m) is the hash version of the message m.
- BL is a biometric lock of a client.
- P is a permutation
- Pu & Pr are respectively the public key and the private key of a cryptosystem.
- $\mathrm{E_{PuX}}$(m) is the encryption of the message m using the public key of X.
- $\mathrm{K_A}$ is the authentication key generated randomly by the client.
- $\mathrm{E_{kA}}$(m) is the symmetric encryption of the message m using the secret key K_A.
- S is the mobile serial number provided by the client.
- $\mathrm{S_T}$ is the mobile serial number of the client which is stored in the database.
- C is a client.
- $\mathrm{S_1}$, $\mathrm{S_2}$ are respectively the first server and the second server.

4 Proposal Protocol

4.1 Enrollment Phase

In the enrollment phase, the client employs a random number K_m stored on the his/her device to generate the random orthonormal matrix *M* (based on the technique described in Sect. 3.2). After being extracted, the feature vector *B* is combined with matrix *M* to produce the cancellable version B_{TC} of *B* which is sent to server S_1 after that. In addition, the client also needs to register a secret number *PIN* to server S_1. The hash version of *PIN* is then stored in the database by server S_1. Parallel to that process, the client has to send serial number of his/her mobile device to another server (server S_2). The act of dividing client's information into two different databases is meant to reduce workload for the server; more importantly it serves to limit the control of server over client's private information. The process is illustrated in Fig. 2.

4.2 Authentication Phase

In this phase, we apply the ideal of fuzzy commitment scheme to obtain the secure biometric based remote authentication. Instead of transmitting the plain biometric data

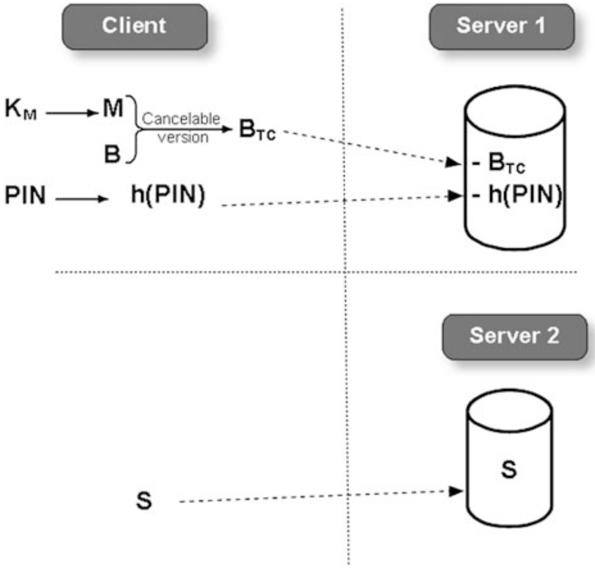

Fig. 2. Enrollment phase.

over the insecure network as the original scheme, client sends a biometric lock (*BL*) or a helper data to a server. At the server side, a biometric lock is combined with the component *Y* related to the client's biometric which is stored in database at the enrollment phase. The result of this combination is the authenticated key. The process is presented by the Fig. 3.

More details of the authentication phase are described in the Fig. 4. The authentication function is undertaken by the second server S_2. Meanwhile, the first server S_1 takes the responsibility for computing the encryption of the authentication key and then sends the result to S_2 to do the next steps.

In authentication phase, the client sends request to server S_1. This server creates a random number (Nonce – Number used ONCE) N_a, then sends it to the client. Note that all messages between the client and the server over transmission network are protected by asymmetric cryptosystem (PKI – Public Key Infrastructure). In the mean time, the client generates transformed biometric feature B_C from biometric feature *B'*

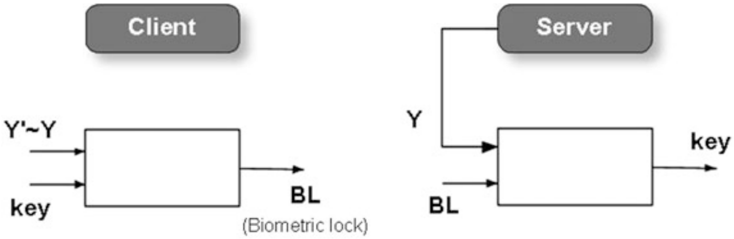

Fig. 3. The fuzzy commitment in the proposal authentication phase.

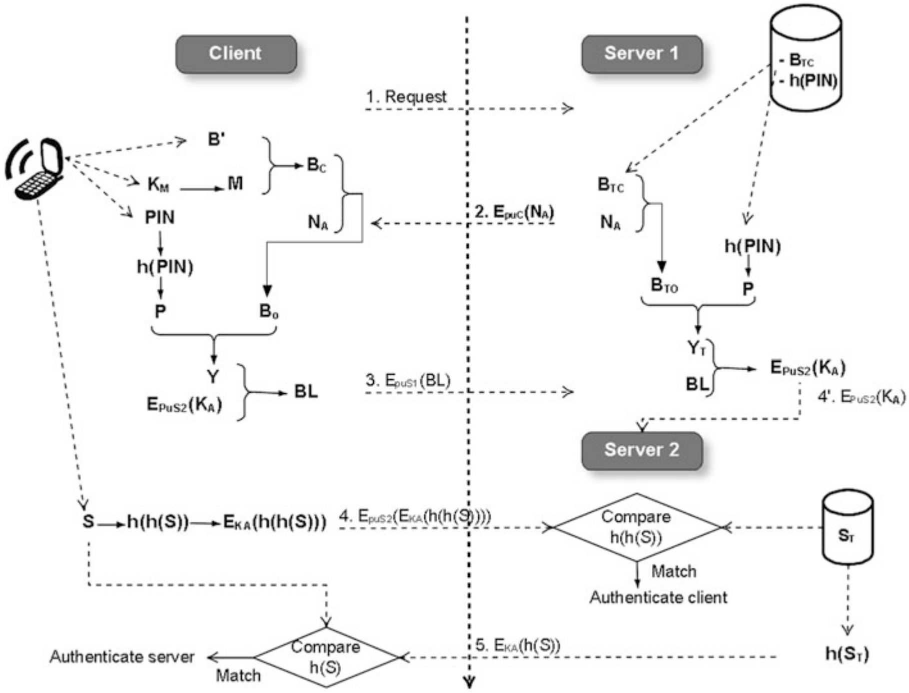

Fig. 4. Authentication phase.

which is extracted in this phase, and orthonormal matrix M from K_M. From the same client, biometric feature B in registration phase and B' in authentication phase cannot be identical due to noises. Calculated B_C combines with N_a to produce another version of transformed biometric – B_O. This step is done to ensure every time the client sends his/her request, a different version of B_O is created to avoid replay attack. This B_O's items are permuted through permutation P which is generated from the hash version of *PIN*. This operation results in *Y*. It is meant to improve security by eliminating the characters of each biometric feature, enabling random distribution of biometric feature's value. Following that, *Y* and the encryption of the authentication key K_A become inputs of the fuzzy commitment process to generate biometric lock *BL* (described in Fig. 3.). Client then sends *BL* to server S_1 for authentication purpose.

At server side, after generating the NONCE N_A, S_1 retrieves the B_{TC} and h(*PIN*) from the database. The one time version of biometric template $\mathrm{B_{TO}}$ is created from the combination between B_{TC} and N_A. Some parts of this process are similar to the process at client side. After B_{TO}, server generate Y_T by shuffling B_{TO} using P which is computed from h(*PIN*). Then, Y_T is used to unlock the *BL* to reproduce the encryption of authentication key K_A.

At step fourth, client retrieves the mobile serial number *S*, hashes it twice to have h (h(*S*)), encrypts the result by the authentication key, and encrypts once more time by the public key of the server S_2 before sending to S_2. Together with this step, at the step

4', server S_1 sends the encryption of the authentication key using public key of server S_2 to S_2. S_2 uses its private key to obtain the authentication key K_A. Server S_2 uses its private key as well as the newly achieved K_A to decrypt the message from the client. If the decryption process is successful, it also means the biometric the client provided matches with the transformed biometric template stored in the database of server S_1. The result of this decryption is compared with the double hashed version of S_T stored in the database of S_2. If they are matched, the client is authenticated; otherwise, the authentication is failed.

For the mutual authentication purpose, the protocol is not stopped here. After successful authentication, server S_2 computes h(S_T), then encrypts it with the authentication key K_A before sending the result back to the client. The client decrypts the message. If the decryption is successful, he/she can be sure that the authentication server also possesses the same key. The client carries out the comparison between the h (S) of client and the h(S_T) of the server. If they are match, the server is authenticated. The client can feel secure about the authentication server which he/she communicated with. Once the mutual authentication is successfully accomplished, K_A is used to protect the communication between the client and the server.

5 Security Analysis

The protocol indicates that the authenticity of the client needs following factors:

- Client's biometric data
- The number used once N_A
- The token that holds the key K_M to generate the random orthonormal matrix
- The *PIN*
- The mobile serial number S.

The multi-factor authentication enhances security since the ability that an attacker steals client's authentication information to enter the system is reduced. In this section, we analyze in detail how the proposal protocol is robust against some main attacks.

5.1 Biometric Template Attack

The original biometric is protected by the non-invertible transformation function. Server keeps the transformed version, but it is impossible for server to infer the client's original biometric from this template. Using orthonormal matrix as a non-invertible function ensures the revocability of biometric template. In case the client is in doubt that his/her biometric template is compromised, he/she only needs to alter parameter K_M to produce new orthonormal matrix, then registers the new transformed biometric template to the server. This process is similar to that of changing password in traditional authentication system.

Another useful factor helps against biometric template attack is the permutation. A one-time version of the transformed biometric feature B_O is re-ordered by a permutation P. This operation is meant to improve security by eliminating the characters of each biometric feature, enabling random distribution of biometric feature's value. This, eventually, weakens the ability of attacker to infer the value of biometric feature.

5.2 Replay Attack

Replay attack happens when attackers reuse old information to impersonate either client or server with the aim to deceive the other side. This attack is prevented by using N_A and session key K_A which are used only once. The system only collapses once the attackers steal private key. In that case the attacker is able to obtain the 3rd message in authentication phase (see Fig. 4) to calculate *BL.* After that, the attacker reuses the *BL* to deceive server in a new session. The proposed protocol is immune from this type of attack as the *BL* generated every time the clients request contains new N_A produced by the server. In the event of attacker using old *BL*, the authentication process cannot calculate exact authentication key K_A.

More concretely speaking, in authentication phase, the transformed biometric features, BC at client side and BTC at server side, are combined with the same number NA by a simple addition operation. This action creates a one-time version of the transformed biometric feature; therefore, attacker cannot reuse the old transformed biometric feature to delude the server. Thanks to that, the security of the entire protocol is strengthened without scarifying the accuracy. The accuracy is maintained because addition operation does not modify intra-class variation of the biometric features, which results in unchanged distance between transformed biometric feature & its original. In other words, the error rate stabilizes while security is strengthened.

5.3 Man-in-the-Middle Attack

MITM (Man-in-the-middle) attack considers as an active eavesdropping, attackers make an independent connection and replays messages between client and server in order to impersonate one side to delude the other side. Concretely speaking, the communication in this case is controlled by attacker while client or server still believes that they are talking to each other over a private connection.

MITM attack happens when the attacker catches the messages between client and server then impersonates one side to communicate with the other side. In our proposed protocol, this type of attack cannot occur since the protocol presents mutual authentication requirement, not only does it requires the server to authenticate its right client but also enables the client to perform its own process to confirm requested server.

5.4 Insider Attack

This type of attack happens when the administrator of authentication server exploits client's data stored in the database to legalize his authentication process on behalf of the client. The proposed protocol is capable of reducing the risk from insider attack by splitting authentication server into two different servers. Each server has its own function and data. Server S_1 stores transformed biometric template and some supporting information to generate authentication key. Authentication function is carried out by server S_2. To perform this function, server S_2 has to receive authentication key calculated by server S_1 and authentication information provided by the client. Consequently, server S_2 can only store authentication information (client's mobile serial number) to proceed authenticating client (described in Sect. 4.2). At the same time, such information is used by client to reversibly authenticate server.

6 Conclusion

In this paper, we have presented an unsusceptible biometric based remote authentication protocol to most of sophisticated attacks over an open network. The proposed protocol combines client's biometric with the other authentication factors to achieve the high level of security. Thanks to the combination of fuzzy commitment and non-invertible transformation technologies as well as a mutual challenge/response, the protocol is resistant to some main attacks to biometric-based authentication system such as biometric template attack, replay attack, man-in-the-middle attack. The remarkable point of this work is that we solved the problem at the unsecure server. We reduce the ability that the administrator utilizes the client's authentication information saved in the database to impersonate him/her and cheat the system. By using the random orthonormal project instead of traditional orthonormal project, the computational complexity is reduced while the accuracy is remained.

Acknowledgements. This research is funded by Vietnam National University - Ho Chi Minh City (VNU-HCM) under grant number TNCS-2014-KHMT-06. We also want to show a great appreciation to each member of D-STAR Lab (www.dstar.edu.vn) for their enthusiastic supports and helpful advices during the time we have carried out this research.

References

1. Jain, A.K., Ross, A.: Multibiometric systems. Commun. ACM **47**(1), 34–40 (2004)
2. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. **2011**(1), 1–25 (2011)
3. Upmanyu, M., et al.: Blind authentication: a secure crypto-biometric verification protocol. IEEE Trans. Inf. Forensics Secur. **5**(2), 255–268 (2010)
4. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Signal Process. **2008**, 1–17 (2008)
5. Huynh, V.Q.P., et al.: A combination of ANN and secure sketch for generating strong biometric key. J. Sci. Technol. Vietnamese Acad. Sci. Technol. **51**(4B), 30–39 (2013)
6. Le, T.T.B., Dang, T.K., Truong, Q.C., Nguyen, T.A.T.: Protecting biometric features by periodic function-based transformation and fuzzy vault. In: Hameurlain, A., Küng, J., Wagner, R., Thoai, N., Dang, T.K. (eds.) TLDKS XVI. LNCS, vol. 8960, pp. 57–70. Springer, Heidelberg (2015)
7. Lifang, W., Songlong, Y.: A face based fuzzy vault scheme for secure online authentication. In: Second International Symposium on Data, Privacy and E-Commerce (ISDPE) (2010)

8. Failla, P., Sutcu, Y., Barni, M.: eSketch: a privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics. In: Proceedings of the 12th ACM Workshop on Multimedia and Security, pp. 241–246. ACM, Roma (2010)
9. Nguyen, T.H.L., Nguyen, T.T.H.: An approach to protect private key using fingerprint biometric encryption key in BioPKI based security system. In: The 10th International Conference on Control, Automation, Robotics and Vision, ICARCV (2008)
10. Xi, K., et al.: A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment. Secur. Commun. Netw. **4**(5), 487–499 (2011)
11. Al-Assam, H., Rashid, R., Jassim, S.: Combining steganography and biometric cryptosystems for secure mutual authentication and key exchange. In: The 8th International Conference for Internet Technology and Secured Transactions (ICITST 2013) (2013)
12. Jain, A.K., Uludag, U.: Hiding biometric data. IEEE Trans. Pattern Anal. Mach. Intell. **25** (11), 1494–1498 (2003)
13. Fengling, H., Alkhathami, M., Van Schyndel, R.: Biometric-Kerberos authentication scheme for secure mobile computing services. In: The 6th International Congress on Image and Signal Processing (CISP 2013) (2013)
14. Juels, A. Wattenberg, M.: A fuzzy commitment scheme. In: Proceedings of the 6th ACM Conference on Computer and Communications Security, pp. 28–36. ACM, Kent Ridge Digital Labs, Singapore (1999)
15. Al-Assam, H., Sellahewa, H., Jassim, S.: A lightweight approach for biometric template protection. In: Proceedings of SPIE (2009)