International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 2 (2018) pp. 1415-1420

Robust Biometrics-Based Authentication Scheme for Cryptographic Keys Distribution

Kadhim H. Kuban Alibraheemi

Department of Computer Science, College of Education for Pure Sciences, Thi-Qar University, Thi-Qar, Iraq.

Orcid: *0000-0002-4749-8673*

Abstract

The authentication is one of the main objectives of cryptographic systems, through which two parties sharing encrypted communication could authenticate each other. To achieve this goal, many approaches and protocols have been proposed, some of which are based on passwords and others based on smart cards. Those approaches have many drawbacks, including passwords, are prone to forgetfulness, divulged, or hacking as well as smart cards might be lost, stolen, or shared. If these approaches are compared with biometric approaches such as fingerprint and iris, it found that biometric approaches have no such defects; biometric systems have therefore gained considerable attention. This research presents a robust scheme based on the fingerprint biometrics to share confidential key of symmetric cryptography between two parties through the Keys Sharing Center (KSC) as a third party which activated on secure and trusted server. The client/server architecture was used to implement the proposed scheme. The proposed scheme was implemented in a way similar to the e-mail service, so it required the use of the ID account for each user, through which any two parties could share the encrypted confidential key through KSC. The proposed scheme is implemented in local area network. The security and performance are discussed to show that the proposed scheme is highly secure, practical and robust.

Keywords: Key generation, Key recovery, KSC, Authentication, CAPTCHA

INTRODUCTION

Encryption represents a process of converting a particular text (plaintext) into another form called encrypted text (cipher text) in which the original message is hidden. The encrypted message is sent through the different communication channels to the other party, which in turn retrieves the original message by a process called decryption. Both encryption and decryption require the so-called cryptographic key. Most of the systems suffer from the key retention problem. The key is often stored in smart cards, databases, or other means that can be compromised by others or sometimes forgotten even by those authorized to use the encryption system. According to Kirchhoff's principle [1], this states that "the security of an encrypted message must depend on keeping the key secret. It doesn't depend on keeping the encryption algorithm secret". Therefore, the encryption algorithm must be highly complex in order to avoid breaking through analytical methods. There is an additional problem with cryptographic systems, which is the key distribution problem that can be cracked through communication channels. In order to overcome problems related to cryptographic keys, the need to adopt biometrics such as iris, face, fingerprint, etc. have recently been used to generate keys or to link them with the keys to make the cryptographic system more reliable between the two ends of the communication. The use of biometrics has reduced the probability of losing or forgetting the keys or the penetration of the keys and the possibility of copying them as it was with passwords. In addition, biometrics have given higher confidence systems than those using digital keys.Cryptographic systems need an exact key to ensure that clear text is retrieved from encrypted text, while the use of biometrics in generating cryptographic keys cannot be a complete success in this retrieval process due to some of the effects on this biometrics when they are obtained such as noise. The process of integrating cryptographic systems into the process of recognition still faces many challenges. There are some requirements for biometrics-based encryption systems, these requirements are: Revocability, security, performance, and diversity [2].

As previously mentioned, encryption systems suffer from the problem of key distribution because keys must be shared confidentially. The distribution of keys may be in manual ways, either directly between the sender and the receiver or through a third party that delivers the key to the sender and receiver. In encryption systems over the network, manual key distribution is confusing, especially in distributed systems over a wide area network [3]. A better way to distribute keys for both sender and recipient to have a third-party encrypted connection, which in turn delivers the key through encrypted links to both sender and recipient [4]. Many biometric-based authentication approaches are proposed some of these are based on smart cards for multi-server environment [3], others integrated passwords with biometric for multi-server environment, authentication [5]. This paper presents an authentication scheme for cryptographic key distribution based on three factors (identity, password, and biometric).

METHODOLOGY

The idea of this research is inspired by the e-mail service. The e-mail is based on the principle of storage and delivery, where messages are stored in mailbox users to see them at the time

they like. The main component of the proposed system is an application called Key Sharing Center (KSC) which is activated on a trusted server. This application performs the following tasks:

a) Generate a secret key at the request of the first party (sender).

b) Generates all keys needed in secret key generation phase.

c) Encrypt the secret key.

d) Sends the encrypted secret key to the sender.

e) Retrieve the secret key at the request of the second party (receiver).

The process of e-mails exchanging does not require that the two communicating parties to be present at the same time, so the proposed scheme consists of three basic phases. These phases are explained by referring to notations in Table 1 below.

Table 1. Notations

Symbol	Description
U_i	The i^{th} user
ID_i	Identity of U_i
PW_i	Password of U_i
KSC	Keys Sharing Center
T_i	Biometric template of U_i
T_i'	New biometric template of U_i
Key_{ij}	Secret key shared between U_i and U_j
AK_{ij}	Auxiliary key associated with Key_{ij}
$E(x)_k$	Encrypt x under key k.
$D(x)_k$	Decrypt x under key k.
H(.)	A secure one way hash function
X||y	Data x concatenates with data y
KeyGen(x)	Key generation algorithm
M	Plain message
M'	Encrypted message

i. Enrolment Phase: This phase requires a unique user ID and password and only one of his fingerprints. The fingerprint features are extracted; these features are used to generate a biometric template for this user. Figure 1 shows the steps of enrolment stage

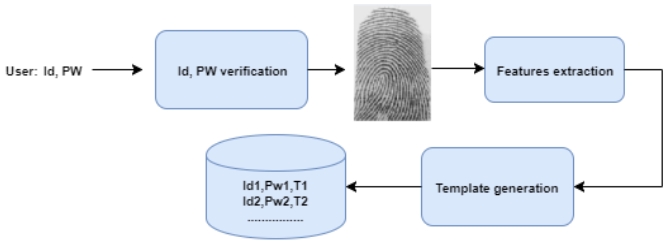

Figure 1: Block diagram of enrolment phase

KSC encrypts the biometric template before storing it in its database using its secret key after modifying it using a party's password to which specific template belongs.

ii. Secret Key Generation Phase: The secret key is generated at the request of the first party (sender) through his connection to the key sharing center using his ID and password. After verifying these two parameters, KSC tells the sender to imprint his fingerprint on a sensor in order to acquire and construct new biometric template, then compare the new template with the old one stored in the database, if this template truly matches the old one; then KSC accept the sender's request and generate the secret key otherwise KSC reject this request and terminate the connection with the sender. Figure 2 shows the secret key generation stage. Full details of this phase will explain in section 2.1

iii. Secret Key Recovery Phase: The secret key is retrieved at the request of the second party (receiver). This phase is similar to the second phase in its biometric-based authentication process. Full details of this phase will explain in section 2.2.

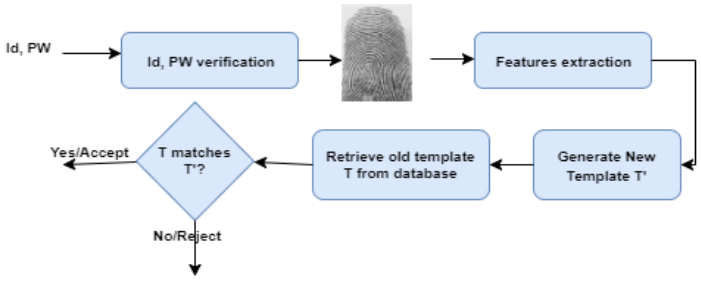

Figure 2: Block diagram of verification process

Key Generation Process

1. User A interact KSC to generate a secret key Key_{AB} to share it with user B. User A supplies his ID_A, PW_A and ID_B.
2. After KSC verifies all parameters supplied by user A, KSC tells user A to imprint his fingerprint on a sensor in order to acquire and construct new biometric template T'_A.
3. KSC searches the database using ID_A and ID_B to retrieve a copy of T_A and T_B respectively.

4. KSC verifies the matching process between T_A with T'_A. If T_A matches T'_A, then KSC accepts the request of user A to generate Key_{AB} otherwise KSC rejects this request and terminate the connection with user A.
5. After KSC verified that user A is an authorized user, KSC generates two keys, one from T'_A as primary key A_{pk} to the user A, another from T_B as primary key B_{pk} to the user B by using the following equations :

$$A_{pk} = \text{KeyGen}(T'_A) \quad (1)$$

$$B_{pk} = \text{KeyGen}(T_B) \quad (2)$$

6. KSC generates another two keys; first key is a unique one-time pad Auxiliary Key AK_{AB} using an independent random number generator, the second key is the secret key Key_{AB} using equation 3.

$$Key_{AB} = \text{KeyGen}(T_A) \quad (3)$$

7. KSC modifies A_{pk} and B_{pk} to get modified keys A_{mk} and B_{mk} for user A and user B respectively, using the prior transformation process agreement with two parties.
8. KSC generates a unique CAPTCHA code CC_A (Completely Automated Public Turing test to tell Computers and Human Apart) and tells user A to enter this code.
9. KSC sends A_{pk} along with CC_A to user A.
10. KSC encrypts Key_{AB} under A_{mk} and under B_{mk}
11. KSC sends $E(Key_{AB})_{Amk} \| E(Key_{AB})_{Bmk}$ along with CC_A and AK_{AB} to user A.
12. User A decrypt $E(Key_{AB})$ A_{mk} under his secret key A_{mk} to extract the secret key Key_{AB}, then user A encrypt the plain message M (usually random number) under Key_{AB} to get encrypted message M' which is needed to transmit to user B as a verification message using the following equation:

$$M' = E(M)_{Key_{AB}} \quad (4)$$

13. User A sends $M' \| E(Key_{AB})_{Bmk}$ to KSC, then KSC will release this message to user B when authenticate with him in key recovery stage.
14. KSC stores $M' \| E(Key_{AB})_{Bmk}$, and AK_{AB} in its database and sends just AK_{AB} and ID_A to user B to notify him there is a new secret key to be shared with user A.
15. To keep the database updated, KSC stores T'_A instead of T_A.

Key Recovery Process

1. User B interact KSC to recover the secret key Key_{AB} that sent from user A. User B supplies his ID_B, PW_B , ID_A, and AK_{AB}.
2. After KSC verifies all parameters supplied by user B, KSC tells user B to imprint his fingerprint on a sensor in order to acquire and construct new biometric template T'_B.
3. KSC searches the database using ID_B to retrieve a copy of T_B.
4. KSC verifies the matching process between T_B and T'_B. If T_B matches T'_B, then KSC accepts the request of user B to recover Key_{AB} otherwise KSC reject this request and terminate the connection with user B.
5. KSC generates a unique CAPTCHA code CC_B and tells user B to enter this code.
6. KSC generates B_{pk} using equation (2) and sends it along with CC_B to user B.
7. KSC searches the database using AK_{AB} to retrieve $M' \| E(Key_{AB})_{Bmk}$ and sends it to user B.
8. User B decrypt $E(Key_{AB})$ B_{mk} under his secret key B_{mk} to extract the secret key Key_{AB} using the following equation:

$$Key_{AB} = D(E(Key_{AB})_{Bmk})_{Bmk} \quad (5)$$

9. Finally user B decrypts M' under B_{mk} to extract the plain message M using equation 6.

$$M = D(M')_{Bmk} \quad (6)$$

10. User B encrypts (M-1) under Key_{AB} and send it to user A.
11. Finally and after completing the two phases; key generation phase and key recovery phase, KSC permanently deletes all keys generated during these two phases.

FEATURES EXTRACTION AND TEMPLATE GENERATION

Features Extraction

Two types of minutiae points are considered in the proposed scheme, namely ridge ending and ridge bifurcation points and these points are the main fingerprint features. The features extraction process as shown in Figure 3 has passed through the following stages.

a. Fingerprint Image Preprocessing

i. **Fingerprint Image Enhancement**: based on Short Time Fourier Transforms (STFT) analysis [6].

ii. **Fingerprint Image Binarization**: A global binarization based on Otsu thresholding method [7] is performed to binarize the fingerprint image.

iii. **Fingerprint Image Segmentation:** Only a

Region of Interest (ROI) is useful to be recognized for each fingerprint image. The first step is block direction estimation and direction variety check. The second is

implementing two morphological operations called 'OPEN' and 'CLOSE'

b. Minutiae Extraction

Minutiae are extracted by the following steps.

i. **Fingerprint Ridge Thinning**: Thinning is the process of reducing the thickness of each line of patterns to just a single pixel width. This is done using a morphological operation used in [8].

ii. **Minutiae Marking**: After the fingerprint ridge thinning, marking minutiae points is the next important step. As the number of minutiae detected is more the probability of accurate result increases.

c. False Minutiae Removing: All the earlier stages occasionally introduce some artifacts which later lead to spurious minutiae. So false minutiae can be removed according to the distances between them [9].

After implementing this procedure, each extracted minutiae will have position and direction, (x,y) and (θ) respectively.

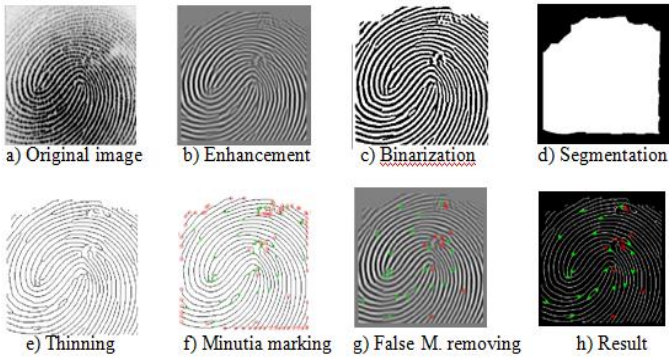

Figure 3: Minutiae extraction stages

Template Generation

Let the minutiae points are represented by a vector M = (M_1, M_2, M_3, …, M_n). M_i = {*xi, yi*} where *i* = 1 to *n*. To construct the template T, consider two vectors; vector V1 contains all the x coordinate values and vector V2 contains all the y coordinate values of a vector M.

$V1=[x_1x_2x_3\ldots x_n]$; $|V1|=n$ (7)

$V2=[y_1y_2y_3\ldots y_n]$; $|V2|=n$ (8)

Concatenating the two vectors V1 and V2 to get a template T

$T=[x_1x_2x_3x_ny_1y_2y_3\ldots y_n]$ $|T|=2n$ (9)

For example, referring to Fig. 3.f, consider the values of V1, V2, and T as follows:

V1=[115 155 112 139 131 226 21 176 142 85 97 71 43 110 129 173 145 207 126 50 90]

V2=[36 59 67 80 89 121 128 128 142 148 156 176 205 211 219 89 121 129 156 195 208]

T= [115 155 112 139 131 226 21 176 142 85 97 71 43 110 129 173 145 207 126 50 90 36 59 67 80 89 121 128 128 142 148 156 176 205 211 219 89 121 129 156 195 208]

Then KSC modifies its secret key using the password of the person to whom that template belongs and uses this modified key to encrypt the template T before storing it in its database.

EXPERIMENTAL RESULTS AND ANALYSIS

In the experiment, fingerprint images from FVC2004 database are used as input fingerprints of two parties, the sender and receiver. The system was implemented in a very easy way where ten persons are registered at KSC each person with eight fingerprints. One fingerprint is used in the registration along with the ID and password. Each person supplied with his other remaining seven fingerprints to be used later in the generation and retrieval of the secret key. The fingerprint features extraction and template generation as explained in section 3.1.

Proposed System Requirements and Architecture

The proposed system was built on a client/server architecture using Apache 2.4.9 as a Web server, MySQL version 5.512 as a database server, and PHP language version 5.6 to establish the connection between clients with KSC database. A local area network is connected and the key sharing center is activated on a network server. An authorized person can be registered at KSC through his/her ID, password, and fingerprint. Also, each person registered in the center knows about the other person's accounts. Here we used the same method used in exchanging e-mails. The two parties are not required to be connected to the KSC at the same time; therefore the proposed work is divided into three stages, which are; enrolment stage, key generation stage, and key recovery stage.

Algorithms and Software Used

In this work AES model ECB of 256 bits is used as an encryption/decryption algorithm and a secure hash function SHA-256 bits is used as one way function for key generation. Also an independent random number generator is used to generate an auxiliary key. MATLAB R2013a is used in the fingerprint images processing in all its stages.

EXPERIMENTAL RESULTS

The proposed method was implemented using MATLAB R2013a. It was tested using FV2004 dataset. The size of fingerprint images was 256×256. One fingerprint is takes as input for each authorized person to generate his permanent key. The impostor key is generated from the remaining fingerprints in the same database, including fingerprints of the same person. The average of False Acceptance Ratio (FAR) is 0.062 and the average of False Rejection Ratio (FRR) is 0.1 while the average of True Acceptance Ratio (TAR) is 90%. The three metrics are computed with threshold equal 0.36. Since an ID and password were used for each authorized user, the focus was on the last scale TAR because the matching process becomes one to one and it was not necessary to

compare a person's fingerprint whose password and identity were identical to those in the database with other fingerprints. To check the robustness of the genuine key, two experiments are implemented, in the first experiment where many impostor keys are generated from other fingerprints and compared them with the genuine key. It is found that the impostors are not able to generate a key similar to the genuine key. The average Levenshtein distance of genuine key with impostor's keys is 71% of the length of genuine key. In the second experiment two fingerprints of the same person are taken with recognition rate 98.9, one fingerprint is used to generate a permanent key to this person and the other fingerprint is used to generate the impostor key, it found that the Levenshtein distance between two keys about 92%.It means that the impostor is needed to guess at least 92% bits (i.e., 235 bits out of 256 bits key length) in an average case to break the genuine permanent key.

The communications between two parties in either two phases; key generation and key recovery phase proved to be more active and with error free. Table 2 shows the execution time to the proposed scheme.

Table 2. Time execution of the proposed method

Stage	Elapsed Time in Millisecond
Pre-processing and Image Enhancement	281
Feature extraction & Template generation	1019
Matching	289
Recognition	16
Key generation	3
Total	1608

Security Analysis

In this section the security of the proposed method is analyzed with respect to the biometric key, the secret key sharing, the privacy of the fingerprint, and finally modifying the primary keys A_{pk} , B_{pk} to get the permanent keys (modified keys) A_{mk} and B_{mk} of the two parties A and B respectively.

a. Security of Biometric-Based Key

All the keys that are generated except the auxiliary key are derived from the fingerprint data to ensure the unity of these keys from two directions; firstly the keys are derived from biometric data and secondly using a one-way function to ensure that it is impossible to return from the output key to the original biometric data. The key generation process was done by verifying that the first party is an authorized where new fingerprint of him is acquired in order to construct a new biometric template to compare it with those in the database; therefore a primary key was generated and then updated to be a permanent key (modified key) for that party. The secret key has been generated from the first party fingerprint template and encrypted under A_{mk} and B_{mk}. KSC will be send the secret key to user A and store a copy of this key in its database to release it later to user B when KSC authenticate with this user during the key recovery stage.

b. Sharing the Secret Key

The secret key was generated from the fingerprint data and was encrypted with two keys derived from biometric template, thus making it so difficult for the attacker to retrieve the original biometric data from secret key. Also, after sending the secret key to the first party, his first biometric template is deleted and stores his new biometric template instead. The CAPTCHA code is used to make sure the first party was still on the line and that the fingerprint was not through its image.

c. Privacy of Fingerprint Data

In either two stages; key generation stage and key recovery stage, the authorized user is not aware of his fingerprint data nor in the method of extraction its features. Also, no authorized user can deduce his biometric template from the keys used.

d. Permanent Keys

The key sharing center shares a transformation parameter with each party to extract or derived his permanent key from the primary key. KSC uses the password of the party to make diversity to his primary key before taking it as input to the key generation algorithm and then construct his permanent key.

CONCLUSIONS

Most of the systems suffer from the key retention problem. The key is often stored in smart cards, databases, or other means that can be compromised by others or sometimes forgotten even by those authorized to use the encryption system. There is an additional problem with cryptographic systems, which is the key distribution problem that can be cracked through communication channels. In order to overcome problems related to cryptographic keys, the need to adopt biometrics such as iris, face, fingerprint, etc. have recently been used to generate keys or to link them with the keys to make the cryptographic system more reliable between the two ends of the communication. The use of biometrics has reduced the probability of losing or forgetting the keys or the penetration of the keys and the possibility of copying them as it was with passwords. In addition, biometrics has given higher confidence systems than those using digital keys. Integration of biometric data to the KSC makes it stronger and easier to maintain the privacy of the secret key. In the proposed scheme, communicating parties are not required to memorize a permanent key as the key is associated with their biometrics. Because the proposed scheme implemented in a way similar to e-mail exchanging both the identity and password are required to facilitate the communication with KSC and among all parties (for simplicity the communicating parties may use their email accounts as their identities to enroll in KSC). The proposed biometric based KSC can easily be implemented with other biometrics like iris, retina, face,

voice, etc. the experimental results proved that the proposed scheme is highly secure, practical, and robust.

REFERENCES

[1] Kerckhoffs, auguste, "La cryptographie Militaire", journal des Sciences Militaires, 161-191, January-February, 1883.
[2] V. N. Boddeti, F. Su and V. Kumar "A Biometric Key-Binding and Template Protection Using Correlation Filters," *Lecture Notes in Computer Science,* pp. 926–936, 2009.
[3] Debiao He, and Ding Wang, "Robust Biometrics-Based Authentication Scheme for Multi server Environment", IEEE SYSTEMS JOURNAL, 2014.
[4] Yashaswini J, "Key Distribution for Symmetric Key Cryptography: A Review", IJIRCCE, Vol. 3, Issue 5, May 2015.
[5] Xuelei Li∗ , Qiaoyan Wen, et al," A biometric-based Password Authentication with key Exchange Scheme using Mobile Device for Multi-Server Environment", Appl. Math. Inf. Sci. **9**, No. 3, 1123-1137 (2015).
[6] Sharat Chikkerur, Alexander N. , et al, "Fingerprint enhancement using STFT analysis", The Journal of Pattern Recognition Society, USA, 40 (198 – 211), (2007).
[7] Otsu, N., "A Threshold Selection Method from Gray-Level Histograms," *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 9, No. 1, pp. 62-66, 1979.
[8] Lam, L., Seong-Whan Lee, et al, "Thinning Methodologies-A Comprehensive Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 14, No. 9, September 1992.
[9] Manvjeet Kaur, Mukhwinder Singh, et al, "Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology 22, 2008.