Journal of Engineering and Applied Sciences 12 (Special Issue 9): 8657-8660, 2017
ISSN: 1816-949X

Symmetric Key Generation using Integrated System of Multi-Modal Biometrics and User-Password

Sreenivas Reddy Chitla, S. Pooja and Mayank Shukla
Department of Information and Communication Technology,
Manipal Institute of Technology (MIT), Manipal, Karnataka, India

Abstract: Encryption is an important aspect in data storage in today's life. The necessity of securing highly classified data like military data, bank transactions, personal data, etc. is a must and for that multi layered security becomes extremely important. Symmetric or asymmetric key can be used for the process of encryption and decryption. Symmetric key uses the same secret key for encryption of text and decryption of ciphered text. There are existing systems where with the help of biometric feature such as fingerprint is used to secure the data. The existing systems have only one layer of security. The proposed system has three layers of security. In order to retrieve the secret key, user has to provide his/her fingerprint followed by password given by the user and lastly iris image of the user. Thus, providing two additional layers of security, the data becomes more classified as even if the fingerprint is lifted by an attacker to retrieve the secret key, he must get hold of password which only the user is aware of and iris pattern of the user which is impossible to retrieve.

Key words: Minutia, encryption, iris, fingerprint, secret, classified, security

INTRODUCTION

Development in information and technology is increasing day by day. The necessity of storing the information of every client is important. Confidentiality in accessing and securing the data plays a major role in determining company's capability to secure the information. Better the protection, safer the data. The techniques used in the system to secure the data are biometric based key generation and user's password. The biometric features considered here are fingerprint and the iris of the enrolled user. The biometric feature is chosen here because of its universal presence and unique property. But now a days to obtain fingerprint of an individual is still a tedious job but not impossible to get. So, in this proposed research two additional layers of protection are added by combining the fingerprint of the user with his password and followed by his iris scan. This is more secure compared to just fingerprint encryption because there is no way of knowing the password and the iris pattern. The password shall not be known to anybody until and unless mentioned by user. The fingerprint encryption acts as a first layer protection. This is made more complex and secure by making use of user's password.

A number of existing work can be found on biometric cryptosystem based on either fingerprint, iris or using multimodal biometric. Jain *et al*. (1997) has proposed a work that describes the working methodology of an on-line fingerprint verification system. It has two stages of operation, they are: minutia points extraction and minutia points matching. A revised version of an algorithm for minutia points extraction was put forward by Ratha *et al.* (1995) which is much better and reliable. Minutia matching is done based on the alignment an elastic matching algorithm has been developed. With the help of this algorithm mapping between minutiae points found in the input image and the stored template can be matched without processing to an exhaustive search and has the ability to take care of nonlinear deformations and dealing with inexact pose transformations between fingerprints scans. Barman *et al*. (2014) has proposed a work that describes a cryptographic key which is generated using the fingerprint. The fingerprint image is modified and binary key string is generated. This key is used to encrypt a message. During decryption process, the user inputs his fingerprint once again and decrypts the encrypted message. Euclidean distance computation model is used to generate the key of 128 bit long using minutia points extracted from fingerprint image. Bhattacharyya *et al.* (2008) has proposed a research that describes iris feature extraction system. With the help of properly located sensors, the biometric data in numerical format, i.e., the iris images are automatically acquired by the system. Iris images typical input format is colored but it is processed to get a gray scaled image. Iris effective

Corresponding Author: Sreenivas Reddy Chitla, Department of Information and Communication Technology,
Manipal Institute of Technology (MIT), Manipal, Karnataka, India

region is detected using the feature extraction algorithm and then features are extracted. Existing works on fingerprint (Li and Hu, 2016), integrated biometric feature with user-password (Pooja and Saritha, 2016), multi-biometric cryptosystem (Dandawate and Inamdar, 2015) exist but the proposed model includes multimodal biometric with user-password protection layer.

There are wide uses of the proposed application such as authentication which restricts everyone except the user who has encrypted the message and he is the only one to decrypt it. In secure network communications such as in the case of military where in the messages sent and received should remain secure. So, by encrypting those messages, it can be made sure that they are only seen by authorized personnel. Another field where in encryption is of utmost importance is disk encryption. The practice of encrypting the entire hard disk of the user allows user to avoid leaving any traces of unprotected data on the disk. The methodology followed here is firstly a key is generated using user's fingerprint which is 128 bit long. Moving on, another 32 bit key is generated by user's password which is converted into 128 bit key by using customized mapping techniques. As mentioned before, we have two layers of protection that is fingerprint and user-password. At this point, a third layer of protection is added by scanning iris pattern of the user. A 128 bit key is generated using the iris pattern which is further combined with the key generated by the previous layers. The data is encrypted using the final key and can only be decrypted using the right fingerprint, password and iris pattern.

MATERIALS AND METHODS

The application requires three user-details to perform encryption. They are fingerprint of the user, user-password and the iris scan of the user. From the input of user's fingerprint, minutia points are extracted, these points include terminations and bifurcations. With the help of these points and using Euclidian distance calculation, a unique 128 bit key is generated. Now, a 4-digit user-password is entered. With the help of certain computations, explained below, a unique 128 bit key is generated from the user-password. Now, both the keys are combined by using a logical XOR operation which generates entirely a new 128 bit key. Lastly, user's iris is scanned. The scan is modified suitably to create its canny edge image. Minutia point feature extraction concept is applied on this image. From the canny edge image, a 128 bit key gets generated. This key is now combined with the newly generated key from the combination of the previous layers. XOR operation is used again to combine both the keys and further a new final 128 bit key gets generated which can be used for encryption/decryption.

The encryption process: The encryption process of the proposed system is illustrated diagrammatically using Fig. 1:

- Fingerprint of the user is taken as an input
- The image is binarized and undergoes thinning process
- Minutia points are extracted in the form of (x, y) coordinates
- Distance between each and every minutia point is calculated and stored in a vector
- $V_{mf} = \{d_1, d_2, d_3, ..., d_n\}$
- Now, unique distances are analyzed from the vector V_{mf} and are placed into a vector
- $U_{mf} = \{d_{u1}, d_{u2}, d_{u3}, ..., d_{un}\}$ with their indexes being same as they were in the vector V_{mf}

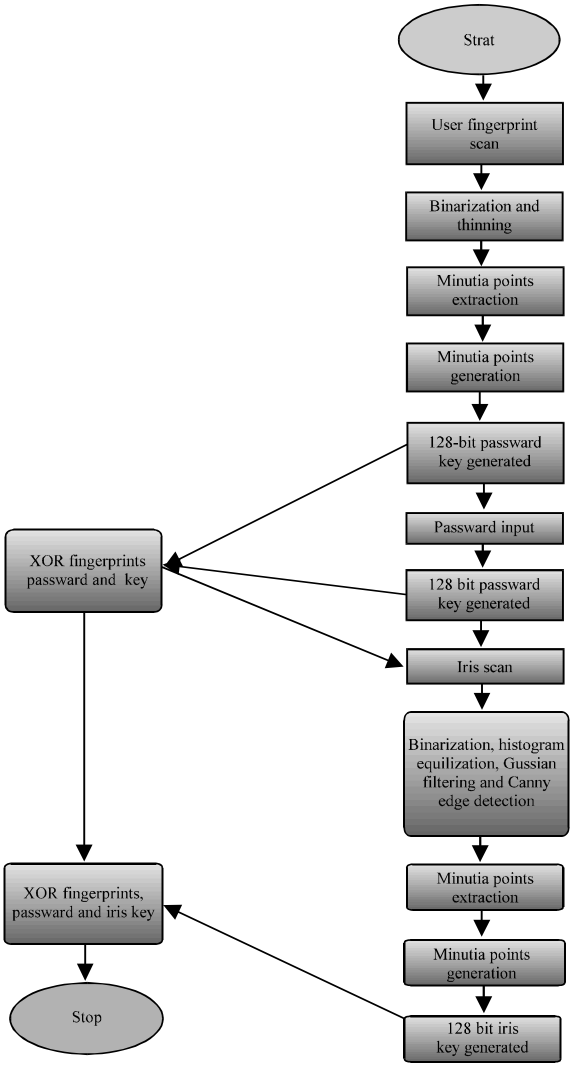
Strat
User fingerprint scan
Binarization and thinning
Minutia points extraction
Minutia points generation
128-bit passward key generated
Passward input
128 bit passward key generated
Iris scan
Binarization, histogram equilization, Gussian filtering and Canny edge detection
Minutia points extraction
Minutia points generation
128 bit iris key generated
XOR fingerprints passward and key
XOR fingerprints, passward and iris key
Stop

Fig. 1: Flowchart of proposed encryption process

- Indexes which contain values are replaced with 1 and the indexes which were empty are given a value 0 and this happens till 128th index
- Thus, generating a 128 bit key from the fingerprint.
- Now, the user enters a 4 digit password
- Each digit is converted into an 8 bit binary number
- These converted digits are rearranged and duplicated in a custom pattern to form a 128 bit key
- The two 128 bit generated keys undergo XOR operation and a new key is generated
- In this final layer of protection, iris of the user is scanned
- The image is binarized and undergoes histogram equalization process
- Gaussian filtering is applied over the image and then Canny edge detection process is carried out
- Minutia points are extracted in the form of (x, y) coordinates from the canny edge image
- Distance between each and every minutia point is calculated and stored in a vector
- $V_{mi} = \{d_1, d_2, d_3, ..., d_n\}$
- Now, unique distances are analyzed in vector V_{mi} and are placed into a vector
- $U_{mi} = \{d_{u1}, d_{u2}, d_{u3}, ..., d_{un}\}$ with their indexes being same as they were in V_{mi}
- Indexes which contain values are replaced with 1 and the indexes which were empty are given a value 0 and this happens till 128th index
- Thus, generating a 128 bit key from the iris scan
- The previously generated key by the combination of first two layers of protection and the key generated from the iris scan undergo XOR operation and a new final 128 bit key is generated
- This key is stored in a file custom named by the user and he has to remember it
- The key stored is used for encryption

The decryption process: The decryption process of the proposed system is illustrated using Fig. 2:

- The user enters the filename
- The iris of the user is scanned
- The image undergoes the following operations mentioned in the encryption process which are binarization, histogram equalization, Gaussian filtering and canny edge detection
- The minutia points are extracted and after computation, a 128 bit key gets generated
- The key generated is XORed with the final key that was stored in the file at the end of encryption process and a new 128 bit key (K_1) is obtained
- In the next step, fingerprint of the user is scanned

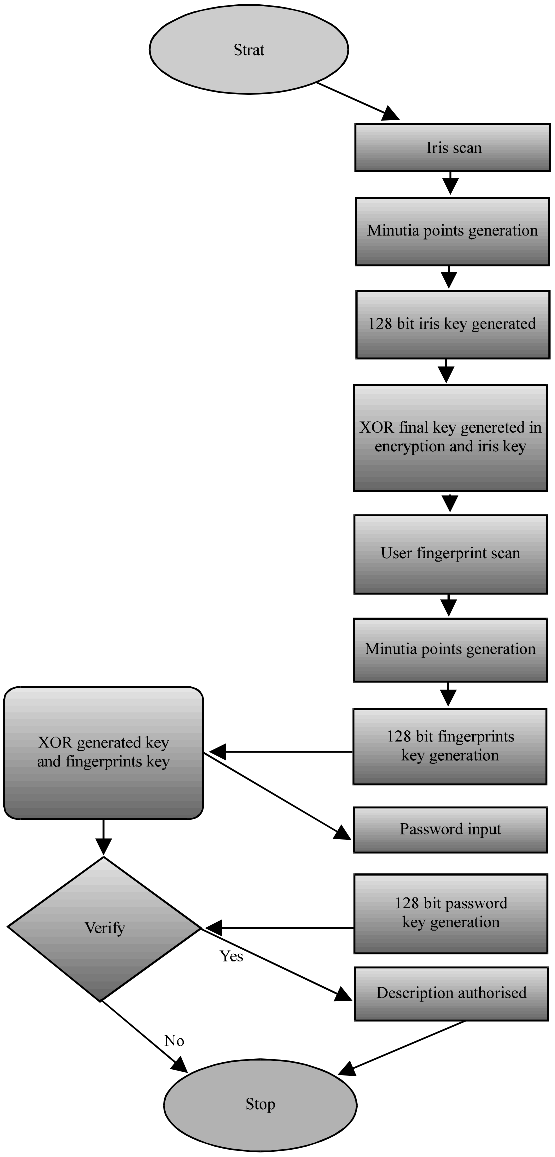
Strat
Iris scan
Minutia points generation
128 bit iris key generated
XOR final key genereted in encryption and iris key
User fingerprint scan
Minutia points generation
128 bit fingerprints key generation
XOR generated key and fingerprints key
Password input
128 bit password key generation
Verify
Yes
No
Description authorised
Stop

Fig. 2: Flowchart of proposed decryption process

- The fingerprint image undergoes the following operation mentioned in the encryption process which are binarization and thinning
- The minutia points are extracted and a 128 bit key is generated
- The above key is XORed with the key K_1 and a new key (K_2) which is 128 bit is obtained
- Finally, the user inputs the 4 digit password
- 128 bit key (K_3) is obtained using the methods exactly mentioned in the Encryption process
- Now, the keys K_2 and K_3 are compared if the value is same, the decryption process is authorized because it is being decrypted by the right user or else the decryption fails

Table 1: Proposed system experimental analysis

Metrics	FVC2002 DB2 fingerprint	UBIRIS.v1 iris
GAR (%)	92	92
FAR (%)	0	0
FTCR	2	2

RESULTS AND DISCUSSION

For feature extraction from minutia points, FVC2002-DB2 (Maio *et al*., 2002) fingerprint database is used which contains 800 images with 10 images of each fingerprint. For the proposed model, manually selected high resolution images are taken. UBIRIS.v1 iris database is used for the iris feature extraction. It has over 1877 images collected from 241 eyes. The performance computation of the system is done using metrics such as false acceptance rate, genuine acceptance rate, failure to capture ate. These are computed to ensure that with IRIS feature involved, proposed work should not lose any precision in GAR. Table 1 illustrates the results computed during computation done.

CONCLUSION

The proposed application has three-layers of protection which includes biometric features such as fingerprint and iris along with user entered password. User password is included because even if an imposter gets hold of biometric feature, until and unless the genuine user shares the user password, the imposter cannot get into the system. Without all the details, it is not possible to generate the key and the decryption process shall never occur. Thus, data is secured using a strong encryption process and hence the key is generated using three layers of protection and reliving the user about the doubt of unauthorized access of the data. The limitations of the system are manual input of high resolution iris and fingerprint image for the enrollment process involved for encryption and decryption process which are taken from databases provided online. The proposed system is evaluated using the parameters FAR, FTCR, GAR to measure the accuracy of system in mapping the biometric to the correspondinguser. Since, there is involvement of multimodal biometric features it's difficult for an imposter to get access because even 1 bit change affects the key generated.

REFERENCES

Barman, S., S. Chattopadhyay and D. Samanta, 2014. Fingerprint based symmetric cryptography. Proceedings of the International Conference on High Performance Computing and Applications (ICHPCA), December 22-24, 2014, IEEE, Bhubaneswar, India, ISBN:978-1-4799-5959-4, pp: 1-6.

Bhattacharyya, D., P. Das, S.K. Bandyopadhyay and T.H. Kim, 2008. IRIS texture analysis and feature extraction for biometric pattern recognition. Int. J.Database Theory Appl., 1: 53-60.

Dandawate, Y.H. and S.R. Inamdar, 2015. Fusion based multimodal biometric cryptosystem. Proceedings of the International Conference on Industrial Instrumentation and Control (ICIC), May 28-30, 2015, IEEE, Pune, India, ISBN:978-1-4799-7166-4, pp: 1484-1489.

Jain, A., L. Hong and R. Bolle, 1997. On-line fingerprint verification. IEEE Trans. Pattern Anal. Mach. Intell., 19: 302-314.

Li, C. and J. Hu, 2016. A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures. IEEE. Trans. Inf. Forensics Secur., 11: 543-555.

Maio, D., D. Maltoni, R. Cappelli, J.L. Wayman and A.K. Jain, 2002. FVC2002: Second fingerprint verification competition. Proceedings of the 16th International Conference on Pattern Recognition Vol. 3, August 11-15, 2002, IEEE, Quebec City, Quebec, Canada, ISBN:0-7695-1695-X, pp: 811-814.

Pooja, S. and R. Saritha, 2016. Enhanced fingerprint system with user password. Proceedings of the International Conference on Circuits, Control, Communication and Computing, October 4-6, 2016, MS Ramiah Institute of Technology, Bangalore, India, pp: 1-6.

Ratha, N.K., S.Y. Chen and A.K. Jain, 1995. Adaptive flow orientation-based feature extraction in fingerprint images. Pattern Recognition, 28: 1657-1672.