

Data Transmission Using Multi-Factor Authentication over Wireless Communication Channel

Zachaeus K. Adeyemo*, Temitope A. Lasisi, Isaac A. Akanbi, Amole A. Olatide

Electronic and Electrical Engineering Department, Ladoke Akintola University of Technology, Ogbomoso, Nigeria

Abstract Data transmission through the internet over the worst channel is increasing everyday due to its convenience. However, hackers interrupt the integrity and availability of the data being transmitted. Conventional method used to combat these challenges such as one-factor authentication is prone to hacking because of its weakest in validating the identity of a person. Therefore, this paper investigates the security of the data being transmitted over the wireless communication channel using two-factor authentication. The transmitted data is first encrypted using Advanced Encryption Standard (AES) after which the finger veins of 123 volunteers consisting of 83 males and 40 females are integrated into the encrypted data. This is transmitted using a secret key and finger vein enrollment. The data is then filtered, modulated and transmitted through the wireless channel. The received data is demodulated, decrypted using the same key after the finger vein authentication. The performance of the technique is evaluated using Response Time, False Acceptance Rate (FAR) and False Rejection Rate (FRR). The results show that high level of accuracy and small response time are obtained. The significance of this work is seen in criminal identification, autonomous vending, institutions of learning, hospitals and automated banking.

Keywords Two-Factor Authentication, Symmetric Cryptography, Finger Vein, Database, Encryption

1. Introduction

Wireless system is prone to transmission problem and hacking. Many of the unauthorized accesses in wireless transmission are due to low level of security of the network. The level of security in organizations and establishments such as universities, industries which depend on internet should be very high to preserve the data from hacking. This process of using security code, key or password is known as one-factor authentication and is vulnerable to hacking because it is a default one-factor authentication. Authentication is the process of identifying a person who has been registered or enrolled as a true user.

Two-factor authentication is a combination of two features of authentication which may be password and biometric technologies such as retina, finger prints, face and palm vein recognitions. The two features of authentication can be encryption and any of biometric features. Encryption is the process of encoding the data in such a way that unauthorized person will not be able to read it, that is, no one will not be able to understand the coded signal being transmitted. The data is decrypted to restore the data. Encryption of data is being analyzed by cryptographic algorithms where there is a known key by the authorized user to decrypt the data.

Cryptography is the science of using mathematics to encrypt and decrypt data. It enables storage of sensitive data to be preserved for intended recipient [1-6]. In other word, cryptography is associated with scrambling of plaintext either ordinary text or clear text into ciphertext (encryption) and then back again (decryption). There are two types of cryptographic algorithms namely: secret key cryptography known as symmetric key cryptography where the same key is used for both encryption and decryption and secondly, public key cryptography which is also known as asymmetric cryptography where two different keys are used with one for encryption and the other one for decryption [7].

Biometrics is a technology of measuring and statistically analyzing biological or physiological traits. More generally, a biometric is a feature measured from a human that can be used for recognition, user authentication and verification purposes. This is based on the privilege of having features that are unique and exclusive to individual by the human body. Most popular biometric includes fingerprints, iris, retina, face, hand, voice and signature. Biometric techniques for personal identification have been attracting attention because one factor authentication such as keys, passwords, and PIN numbers have problems in terms of theft, loss and on the user's memory [8-10].

Some of the conventional biometric techniques such as the ear, iris, retina and fingerprint recognitions have associated problem like deterioration of the epidermis of the fingers, finger surface particles, human body and surgical operation effects which reduce the recognition accuracy. The finger

* Corresponding author:

zkadeyemo@lautech.edu.ng (Zachaeus K. Adeyemo)

Published online at <http://journal.sapub.org/ajis>

Copyright © 2015 Scientific & Academic Publishing. All Rights Reserved

vein which is the second layer of authentication is considered with cryptography in this paper because of its universality, uniqueness, and no adverse effects on human body.

In this paper, two-factor authentication which consists of Advanced Encryption Standard under symmetric cryptography and finger vein is considered to improve the level of security over any one-factor authentication. The investigation is carried out over wireless communication channel. The system model developed consists of a transmitter, wireless channel and the receiver. The transmitter consists of the data to be transmitted, encrypted using symmetric cryptography, after which the finger vein data is binarised, embedded, modulated and properly filtered before sending over the wireless channel to the receiver which also consists of other signal processing techniques for demodulation, filtration, authentication and decryption using the secret key to obtain the original data. The system model is evaluated using False Acceptance Rate (FAR) and False Rejection Rate (FRR) which are functions of match ratio and response time. The system has high level of security due to its high accuracy and small response time.

2. System Model

The system model consists of a transmitter with many signal processing techniques such as encryptor, finger vein database, Recognition algorithm, modulator and filter, then

the wireless channel, and the receiver which has demodulator, filter, finger vein authentication and decryptor to retrieve the original transmitted data. The transmitted data is first encrypted using Advanced Encryption Standard (AES) algorithm. After which the finger veins of 123 volunteers consisting of 83 males and 40 females are embedded into the encrypted data. This forms the secured data to be transmitted over wireless channel using a secret key and finger vein enrolment. The secured data is filtered, modulated and transmitted. The received data is demodulated, decrypted with the same key after the finger vein authentication is applied to receive the original transmitted data. Figure 1 shows the system model developed for the investigation. The performance of the system is evaluated using FAR and FRR which are functions of match ratio and response time. Figure 2 depicts the flowchart of the technique used for the process.

2.1. Method of Simulation

The cryptography scheme that is used for the first layer authentication is the Advanced Encryption Standard (AES) while the finger vein recognition is used as the second layer authentication. The two layer authentications are integrated and simulated using MATLAB communication and signal processing toolboxes. The system used for the analysis has 4GB RAM, Windows 8, Core i3 @ 2.4 GHz with MATLAB version of 8.1.0.604 (R2013a).

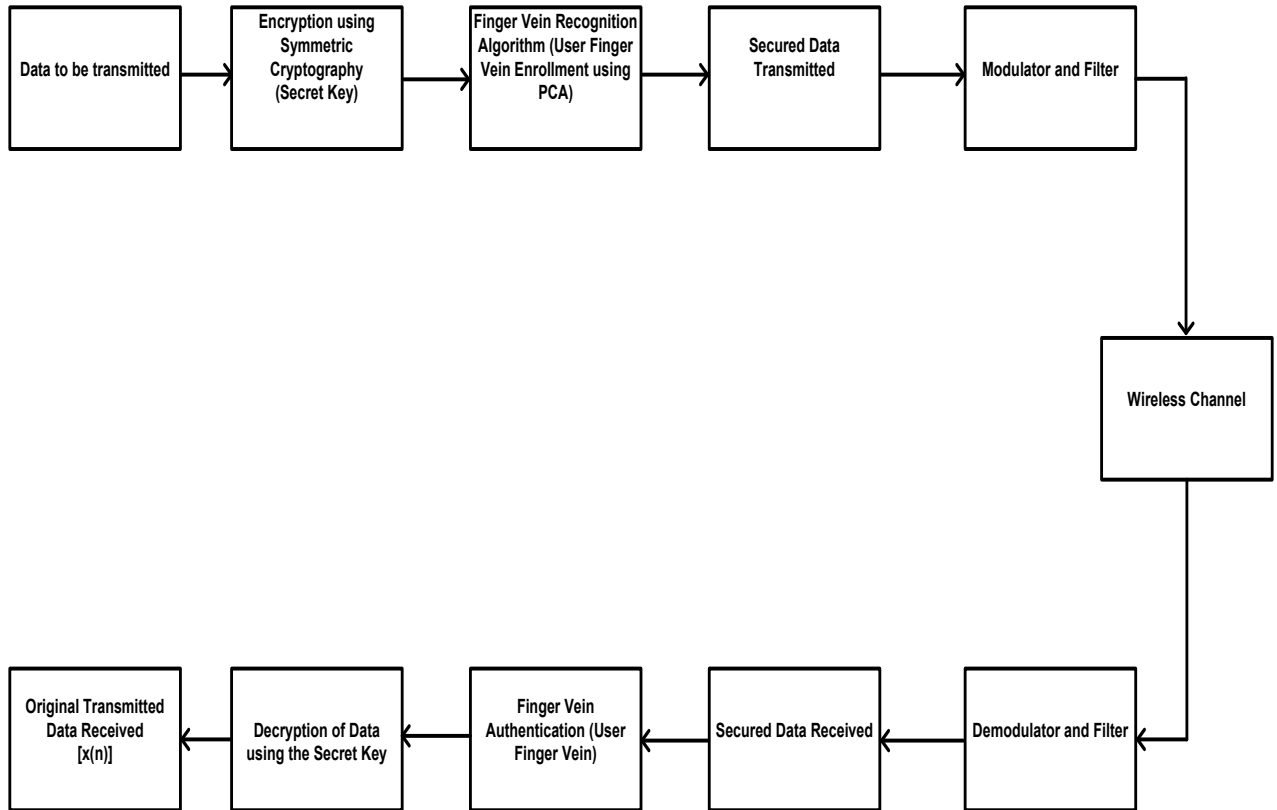


Figure 1. System Model

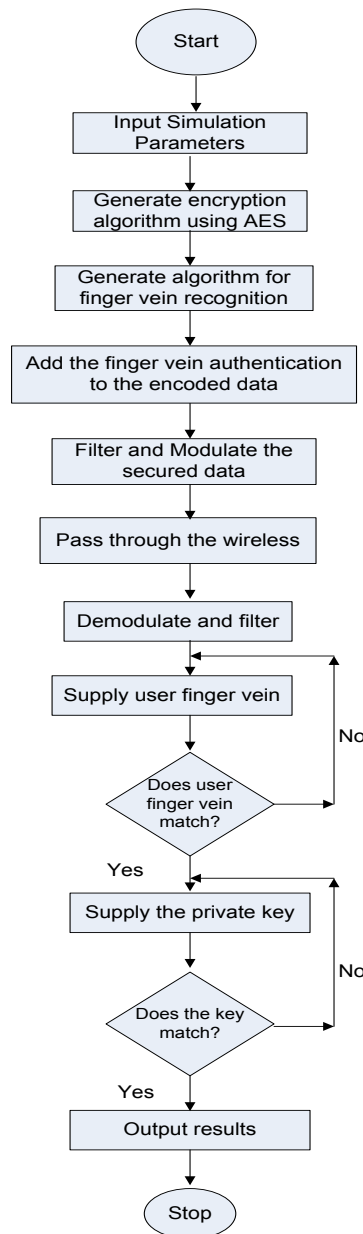


Figure 2. Flow Chart of the technique

2.1.1. Advanced Encryption Standard

In Advanced Encryption Standard (AES), the input consists of 128 bits block for both decryption and encryption to form a matrix. For encryption algorithm, the block is copied into a state array which is modified at each stage of the algorithm and then copied to an output square matrix. The plain text and the key are depicted as 128 bits square metric. This key is then expanded into an array of key scheduled word. The algorithm begins with an 'add round key stage' followed by nine rounds of four stages and the tenth round consists of three stages. These four stages are: substitute bytes, shift rows, mix columns and add round key. The decryption algorithm is the inverse of the encryption algorithm. The tenth round simply leaves the mix columns

stage. The first nine rounds of the decryption algorithm consist of Inverse Shift rows, Inverse Substitute bytes, Inverse Add Round Key and Inverse Mix Columns. The AES algorithm requires 16 bytes key to serve as the password and expand before using in the encryption and decryption processes [5] [11].

2.1.2. Finger Vein Recognition

The finger vein recognition is used as the second layer authentication because of its advantages when compared with other biometric technologies due to its universality and uniqueness. Hand and finger vein detection methods do not have any negative effects on human body; the condition of the epidermis has no effect on the vein features detection.

2.1.3. Finger Vein Database Description

The images in the database are collected from 123 volunteers comprising 83 males and 40 females, who are staff and students of Universiti Sains Malaysia [11]. The age of the subject ranges from 20 to 52 years old. Every subject provides four fingers: left index, left middle, right index and right middle fingers resulting in a total of 492 finger classes. The captured finger images provide two important features: the geometry and the vein pattern. Each finger is captured six times in one session and each individual participated in two sessions, separated by more than two weeks'. In the first session, a total of 2952 (123 x 4 x 6) images are collected. A total of 5904 images from 492 finger classes are obtained from the two sessions. The spatial and depth resolution of the captured finger images are 640 x 480 and 256 grey levels, respectively.

2.2. Integration Mechanism

The finger vein authentication layer is integrated into the system by following a simple rule of transmitting the finger vein template with the last 94 bytes of the data to be communicated. This is possible because the finger vein feature extraction algorithm extracts 94 bytes of data from the original finger vein image. At the receiver, the last 94 bytes are decrypted first and matched before decrypting the rest of the data.

3. Performance Metrics

The metrics used to evaluate this technique are false acceptance rate (FAR) and false rejection rate (FRR) which are defined as in (1) and (2):

$$FAR = \frac{\text{Number of False Acceptance}}{\text{Total Number of Authentication}} \quad (1)$$

$$FRR = \frac{\text{Number of False Rejects}}{\text{Total Number of Authentication}} \quad (2)$$

These metrics are functions of frequency and match ratio. Also, the response time for finger vein extraction and identification are other metrics.

4. Results and Discussion

The results are obtained by observing the performance of finger vein recognition at the receiving end when matched with the finger vein images in the database. The technique is simulated using MATLAB Version: 8.1.0.604 (R2013a) application package. The output of the encryption sequence is presented as follows:

```
s_box: 63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab 76
ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 c0
b7fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 15
    04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 75
    09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84
    53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 cf
d0efaafb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8
    51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 d2
cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 73
    60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b db
    e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79
    e7 c8 37 6d 8d 5e 4e a9 6c 56 f4 ea 65 7a ae 08
ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a
    70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d 9e
    e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df
    8c a1 89 0d bf e6 42 68 41 99 2d 0f b0 54 bb 16
inv_s_box : 52 09 6a d5 30 36 a5 38 bf 40 a3 9e 81 f3 d7 fb
    7c e3 39 82 9b 2f ff 87 34 8e 43 44 c4 de e9 cb
    54 7b 94 32 a6 c2 23 3d ee 4c 95 0b 42 fa c3 4e
    08 2e a1 66 28 d9 24 b2 76 5b a2 49 6d 8b d1 25
    72 f8 f6 64 86 68 98 16 d4 a4 5c cc 5d 65 b6 92
    6c 70 48 50 fd ed b9 da 5e 15 46 57 a7 8d 9d 84
    90 d8 ab 00 8c bc d3 0a f7 e4 58 05 b8 b3 45 06
    d0 2c 1e 8f ca 3f 0f 02 c1 afbd 03 01 13 8a 6b
    3a 91 11 41 4f 67 dc ea 97 f2 cfce f0 b4 e6 73
    96 ac 74 22 e7 ad 35 85 e2 f9 37 e8 1c 75 df 6e
    47 f1 1a 71 1d 29 c5 89 6f b7 62 0e aa 18 be 1b
fc 56 3e 4b c6 d2 79 20 9a db c0 fe 78 cd 5a f4
    1f dd a8 33 88 07 c7 31 b1 12 10 59 27 80 ec 5f
    60 51 7f a9 19 b5 4a 0d 2d e5 7a 9f 93 c9 9c ef
    a0 e0 3b 4d ae 2a f5 b0 c8 eb bb 3c 83 53 99 61
    17 2b 04 7e ba 77 d6 26 e1 69 14 63 55 21 0c 7d
rcon: 01 00 00 00
    02 00 00 00
    04 00 00 00
    08 00 00 00
    10 00 00 00
    20 00 00 00
    40 00 00 00
    80 00 00 00
    1b 00 00 00
    36 00 00 00
poly_mat: 02 03 01 01
    01 02 03 01
    01 01 02 03
```

```
03 01 01 02
inv_poly_mat : 0e 0b 0d 09
    09 0e 0b 0d
    0d 09 0e 0b
    0b 0d 09 0e
plaintext =Columns 1 through 11
0 17 34 51 68 85 102 119 136 153 170
Columns 12 through 16
187 204 221 238 255
ciphertext =Columns 1 through 11
105 196 224 216 106 123 4 48 216 205 183
Columns 12 through 16
128 112 180 197 90
re_plaintext =Columns 1 through 11
0 17 34 51 68 85 102 119 136 153 170
Columns 12 through 16
187 204 221 238 255
```

Figure 3 shows the False Acceptance Rate graph. This is the graph of frequency against the match ratio. It is measured by computing the match ratio for different fingers. It verifies how the finger vein recognition algorithm is evaluated with different fingers. Since the database used consists of 123 fingers, thus making the size to be 15006 (123×122). The distribution of the match ratio ranges from 0 to 0.25 with the highest frequency at the match ratio of 0.18.

Figure 4 shows the False Rejection Rate as function of frequency and match ratio. The database used consists of 123 fingers, each repeated six times for the same user. The analysis is carried out by comparing the six fingers of each user in the database, thus producing a result size of 615 (123×5). The resulting distribution of the ratio shows that it ranges from 0.23 to 0.45 with a peak value at 0.36.

Figure 5 combines the False Acceptance Rate and False Rejection Rate. This helps in selecting a suitable threshold for the finger vein matching algorithm. The threshold of 0.25 is considered, the FAR is $2/15006$ ($1.33 \times 10^{-4}\%$) and the FRR is $3/615$ ($5 \times 10^{-3}\%$). These results depict high accuracy and thus making it suitable for high level of security. Figure 6 shows the time taken to extract the important features from a finger. The extraction time obtained is within a range of 0.65 – 1.03 seconds with a mean of 0.8631 seconds.

The time taken to match two finger vein templates is shown in Figure 7. The results show that for different number of trials, the variation of match time is within a range of 0.0023 – 0.0005 seconds giving a mean of 0.0011 seconds. Figure 8 combines the feature extraction and match time to determine the overall identification of the user. The identification time is almost equal to the feature extraction time. This signifies that over 98 percent of the time is spent on feature extraction indicating high level of improvement in the finger vein recognition algorithm. Nonetheless, the overall identification time is still impressive with a range of 0.65 – 1.03 seconds and a mean of 0.8642 seconds.

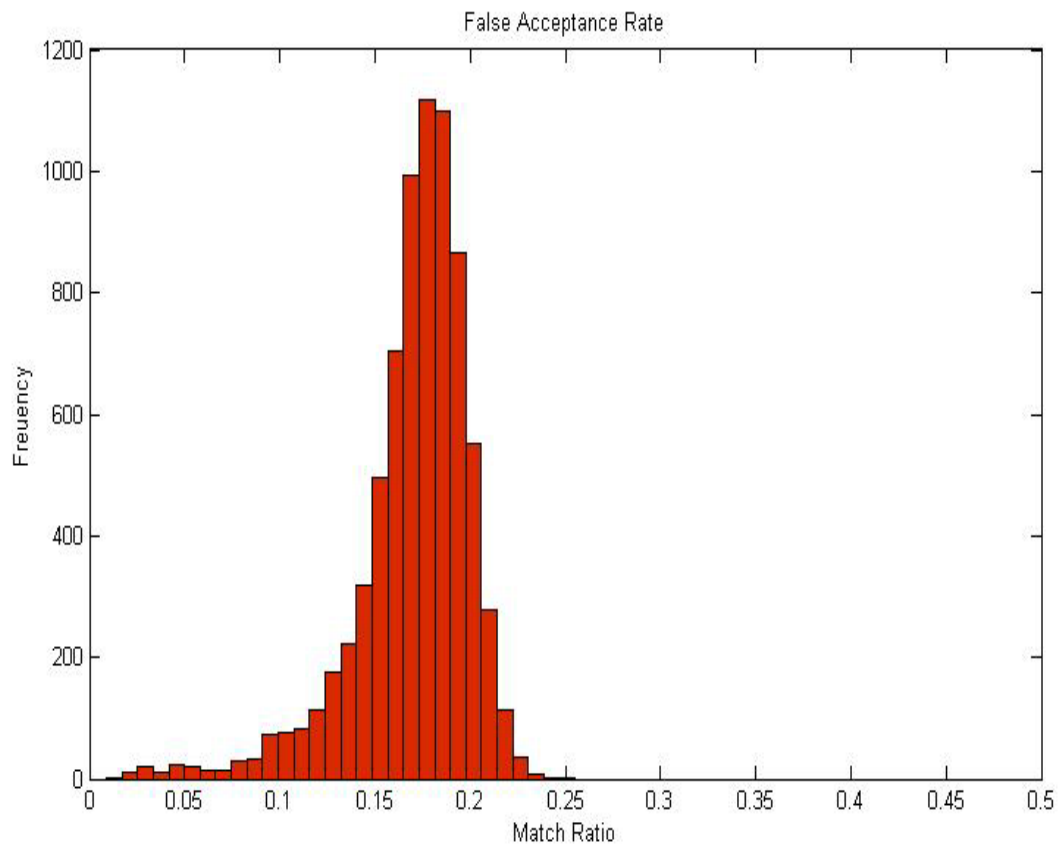


Figure 3. False Acceptance Rate Graph

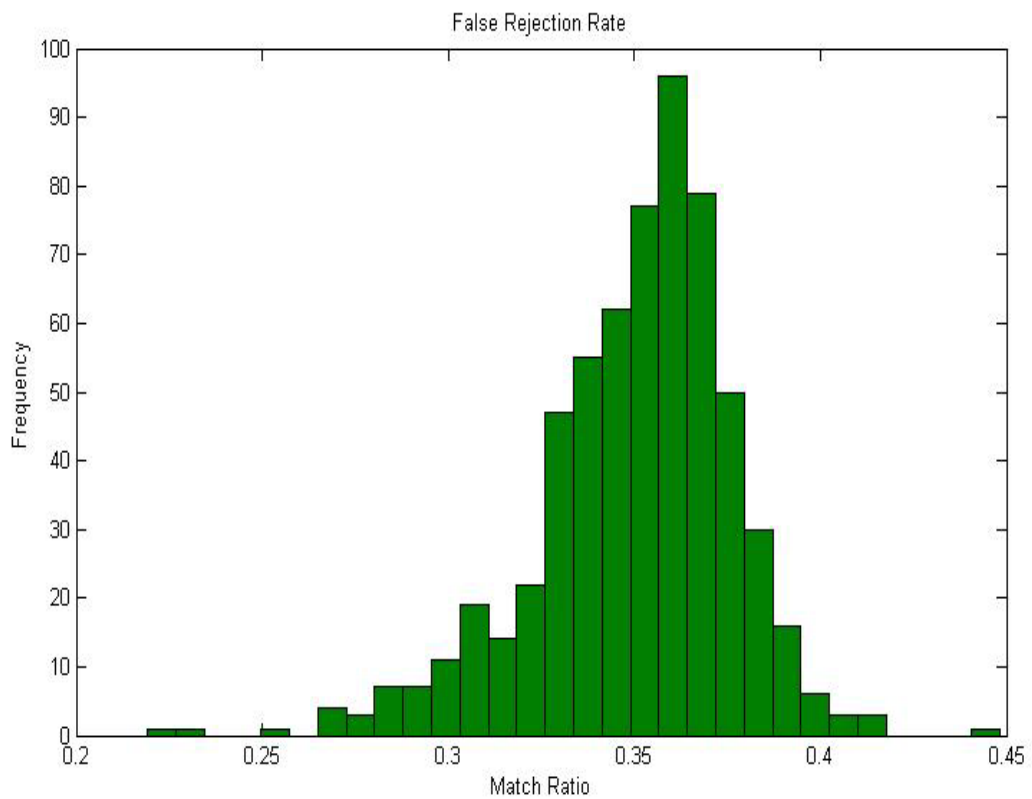


Figure 4. False Rejection Rate Graph

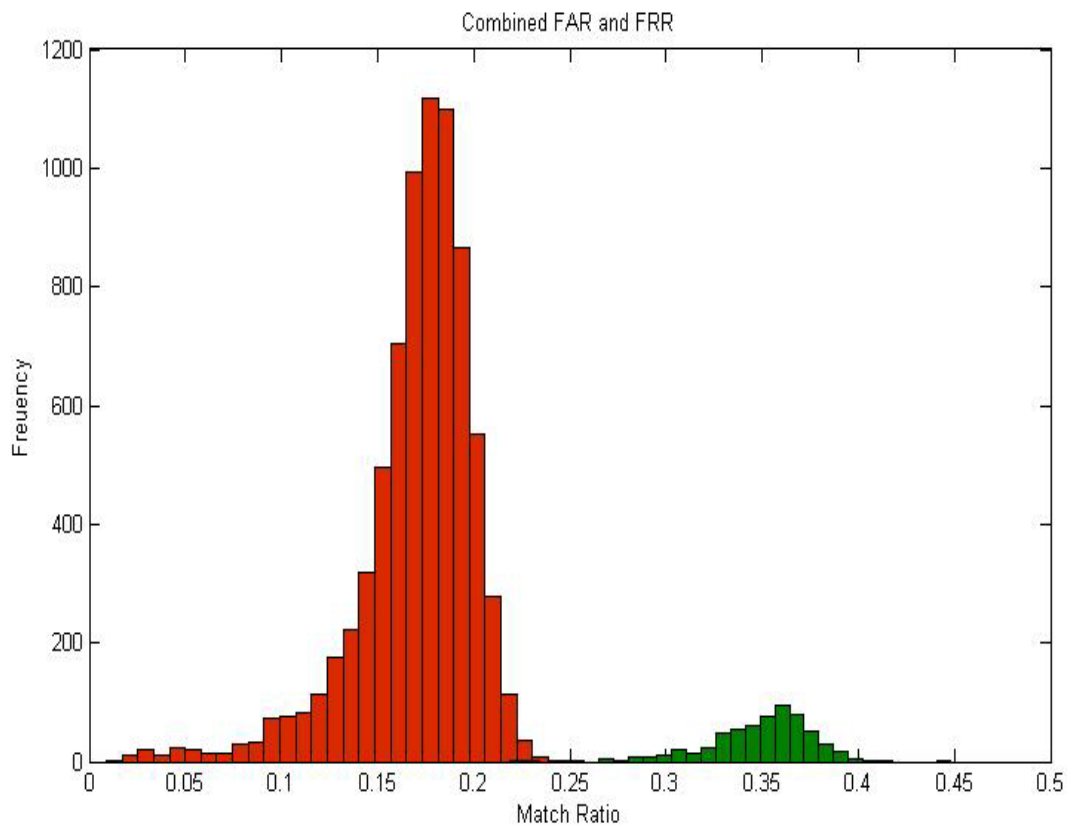


Figure 5. Combined FAR and FRR Graph

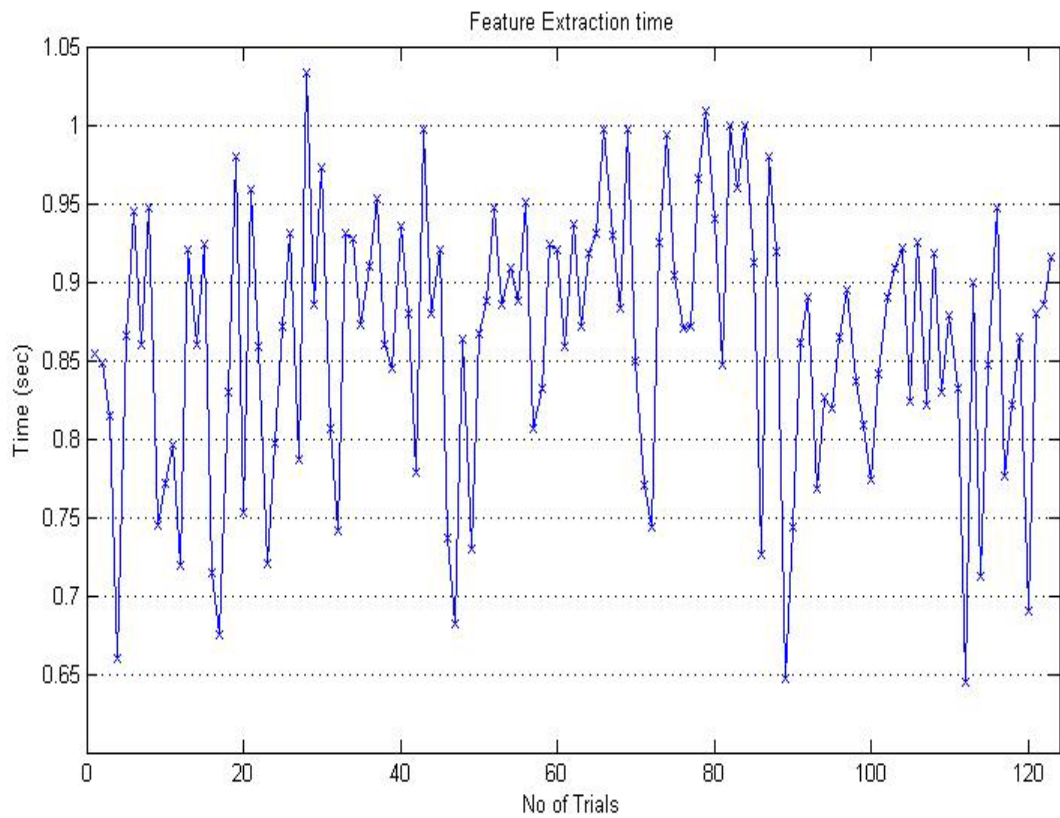
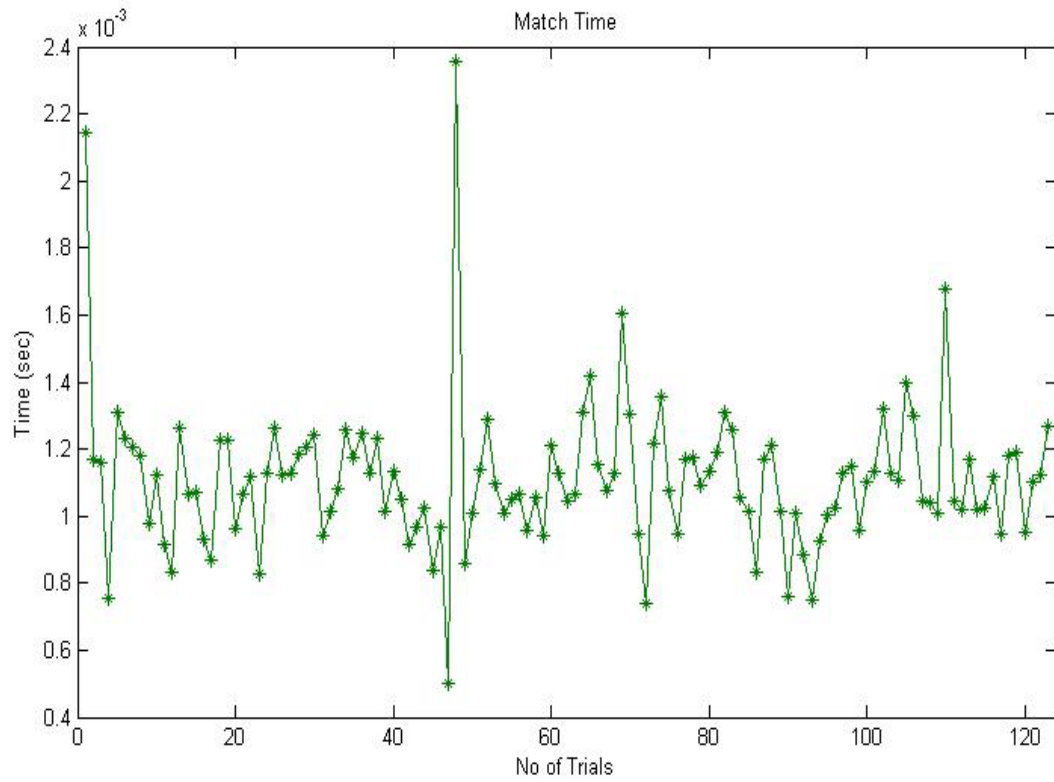
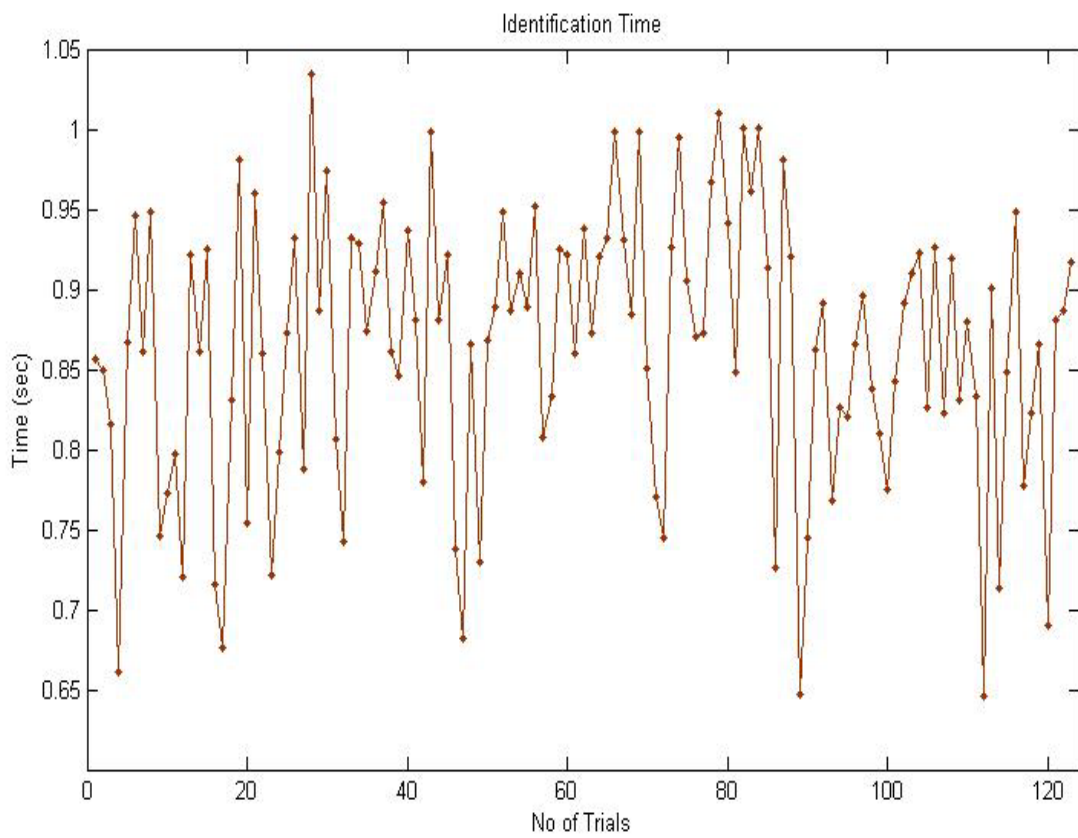


Figure 6. Feature Extraction Time Graph

**Figure 7.** Match Time Graph**Figure 8.** Identification Time Graph

5. Conclusions

In conclusion, a system of two-factor authentication using symmetrically encrypted data and finger vein recognition has been developed over a wireless channel to secure transmission of data. The model is developed around many signal processing techniques at the transmitter to have the secured data that has been transmitted over the wireless channel. The other signal processing techniques at the receiver are developed to retrieve the original data. The performance is evaluated in terms of false acceptance rate, false rejection rate, feature extraction time, match time and identification time. From the results obtained, it can be deduced that this system of two-factor authentication method adopted has been able to show that it is convenient for the user to almost eradicate the various security challenges such as man-in-the-middle forgery thus protecting the confidentiality, integrity and availability of data. Also, this system of 2-factor authentication has proven to be time efficient in terms of authentication.

ACKNOWLEDGEMENTS

We wish to acknowledge Mohd Shahrime. Mohd Asaari, Shahrel A. Suandi, Bakhtiar Affendi for making finger vein data base available to us.

REFERENCES

- [1] Ayushi, A. 2010, "A symmetric key cryptography algorithm," *International Journal of Computer Application*, 1(15), 1-2.
- [2] Bauer, L., Cranor L., Reiter M., and Vaniea K., 2007 "Lessons learned from the deployment of a smart phone based access-control system", in *ACM Symposium on Usable Privacy and Security*.
- [3] Bonneau, J., Herley, C., Van Oorschot P., and Stajano, F. 2012, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes", *IEEE Symposium on Security and Privacy*, 30(14), 2.
- [4] Braz, C. and Robert, J., 2006, "Security and usability: the case of the user authentication methods", in *International Conference of the Association Francophone d'Interaction Homme-Machine*.
- [5] Gunson, N., Marshall, D., Morton, H., and Jack, M., 2011: User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking", *Computers & Security*, 30(4), 5.
- [6] Hridesh, V., Indu, S., Meenakshi, G., and Harshit, G. 2013, Wireless secure Data transmission with face detection: A two way security approach, 'International Journal of Emerging Technology and Advanced Engineering', 3(4),176-180.
- [7] Strouble, D., Schechtman, G., and Alsop, A., 2009, "Productivity and usability effects of using a two-factor security system", SAIS.
- [8] Sabzevar, A. and Stavrou, A., 2008, "Universal multi-factor authentication using graphical passwords", In *SITIS*.
- [9] Miura, N., Nagasaka, A. and Miyatake, T., 2004, Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification. *Machine Vision and Applications*, 15(4),194-203.
- [10] Schneier, B. 2013, iPhone Fingerprint Authentication retrieved from https://www.schneier.com/blog/archives/2013/09/iphone_fingerpr.html in November 2014.
- [11] Mohd S. M A., Shahrel A.S. and Bakhtiar A.R. 2014, Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics, *Expert Systems with Applications*, 41(7), 367-3382, ISSN: 0957-4174, <http://dx.doi.org/10.1016/j.eswa.2013.11.033>.