Jr. of Industrial Pollution Control 33(2)(2017) pp 1528-1533
www.icontrolpollution.com
Research Article

AES BASED SYMMETRIC-BIOMETRIC CRYPTO SYSTEM USING USER PASSWORD

DISHA AGARWAL[1*] AMODINI VARDHAN[2] AND POOJA S[3]

[1]Department of Information and Communication Technology Manipal Institute of Technology, Manipal, Karnataka, India

[2]Department of Computer Science and Engineering Manipal Institute of Technology, Manipal, Karnataka, India

[3]Department of Information and Communication Technology Manipal Institute of Technology, Manipal, Karnataka, India

(Received 07 August, 2017; accepted 20 September, 2017)

Key words: Symmetric key, Fingerprint, Minutiae extraction, Advanced Encryption Standard (AES), Euclidean distance

ABSTRACT

Digital Security has become an area of concern with the increasing use of Internet for communication of sensitive data on both economic and personal fronts. To secure data from unauthorized access, encryption has become a necessity. Strength of the security relies on the key used for encryption. Now-a-days biometric keys are preferred because they are more reliable. The key used can be of two types-Symmetric and Asymmetric. In symmetric key the same key is used for encryption and decryption whereas for asymmetric key different keys are used for encryption and decryption. Majority of the systems use a single layer of security that is either user-password or biometric feature i.e., fingerprint, iris or palm etc. In our proposed work we have combined both fingerprint and user-password using Advanced Encryption Standard (AES) to generate a symmetric key thereby providing double layer of security. The fingerprint is used to extract the minutiae to generate a preliminary key using Euclidean distance method. The advantage of this system is that even if the attacker is able to lift either the fingerprint or the user-password then also he needs to get hold of the other feature which is the user password of varying length ranging from 6 to 8 characters, to get the secret key used for encryption/decryption.

INTRODUCTION

Asymmetric or public key cryptography uses both private and public key for encryption-decryption. The public key is common to all and the private key is kept as a secret and only intended receiver's private key can be used to decrypt the message. Symmetric key is another form of cryptography that involves encryption-decryption using the same key or a simple transformation between two keys. Cryptography is used to provide confidentiality and reliability to the ever increasing data on the internet. The power of the cryptographic system relies on the strength and the authenticity of the key used for encryption and decryption. Biometric system use unique traits and behavioral characteristics of the user like-fingerprint, iris, voice that ensures high degree of trust worthiness because of its universality. There are two types of biometric systems one is biometric based key released and the other one is biometric based key generation. Biometric based key release authenticates a user and releases a cryptographic key stored in the system. Use of biometric ensures physical presence of the authenticated users. This method is implemented using Fuzzy Commitment Scheme (Hao, *et al.*, 2006). In biometric based key generation system biometric features are used to generate the cryptographic key. (Jules and Sudan, 2002) has proposed a work which implements biometric based key generation using

***Corresponding authors email: dishaagarwal@gmail.com**

Fuzzy Vault Scheme (Nandakumar, *et al.*, 2007). The traditional cryptographic systems used keys that had to be remembered by the user and could be easily retrieved by the attacker using social engineering and other hacking techniques. Currently to enhance security, biometric cryptosystem have come into picture. These systems use the combination of biometric feature and cryptography to ensure a higher level of security. Our proposed work provides a double layer of security by combining fingerprint and user password using AES. In our system the user can enter a password having length between 6-8 characters thereby providing flexibility to the users and increasing unpredictability for the hackers. Advanced Encryption Standard also known as Rijndael is a symmetric block cipher used to encrypt sensitive data. AES is efficient in both software and hardware implementation. AES can be implemented using keys of size 128, 192 or 256 bits.

The rest of the paper is organized as follows. Related work explained in section II followed by Proposed embedding and extraction algorithms are explained in section III. Experimental results are presented in section IV. Concluding remarks and future works are given in section V.

RELATED WORKS

(Li and Xiao-Long) has proposed an algorithm for fingerprint-minutiae extraction in form of (x, y, θ). In this (x, y) are the co-ordinates and θ is the alignment. (Subhas, *et al.*, 2014) have proposed a system for generating a key using fingerprint template. Their proposed system uses Euclidean distance for computing distance between two minutiae. These distances are used to form a fingerprint template. Instead of Euclidean distance Chebychev, Manhattan, Canbarra, Minkowski and Bhattacharya distances can also be used. For the integration of biometric and user-password a system by using XOR gate is proposed by (Pooja and Arjun). To further enhance the security instead of XOR gate AES can be used. The basic logic and algorithm of AES was proposed by Federal Information Processing Standard Publications 5. The MATLAB implementation of AES has been developed by (Jorg and Buchholz's). One of the most popular implementation of this is the Fuzzy Vault Scheme. In this scheme minutiae are extracted from a fingerprint and used to lock and unlock a key encoded using polynomial coefficients of an equation the proposed system first minutia extraction process is done using enhancement, binarizing, ridge thinning, eliminating spurious minutia. For minutia pints extraction (Li and Xiao-Long) algorithm is being used. After this process minutia points are extracted in the form of (x, y, θ) form and for the proposed system only (x, y) is used. After extraction the points are fed to Euclidean distance computational model for generating 128 bit key.

PROPOSED ALGORITHM

In the proposed system first minutia extraction process is done using enhancement, binarizing, ridge thinning, eliminating spurious minutia. For minutia pints extraction (Li and Xiao-Long) algorithm is being used. After this process minutia points are extracted in the form of (x, y, θ) form and for the proposed system only (x, y) is used. After extraction the points are fed to Euclidean distance computational model for generating 128 bit key.

This work proposes an additional security layer using user password which is varying length from six to eight characters. The input is in form of string and is converted to its ASCII value. It is converted to 128 bits by reversing and concatenating it (the user password), for 6 and 7 bit lengths 0's and 1's are concatenated too. The user password is then fed into the Advanced Encryption Standard (AES) encryption system along with the 128 bit key generated from fingerprint to generate the final key which will be the new secret private key. Brief illustration on AES encryption algorithm used in our proposed system is also stated below, followed by the proposed encryption and decryption techniques used in the system (Fig. 1-4).

Advanced Encryption Standard

(Jorg and Buchholz's) code has been modified for MATLAB implementation of AES. This code uses the 128 bit transformed user password as the plaintext and 128 bit key generated using minutia points as the key. The built in methods used in AES encryption system is stated as below. (Fig. 2) illustrate AES initialization function.

The AES_init function has following sub-functions:

- S_box and Inverse S_box generation.
- RCON_gen function generates the RCON for key expansion function which uses key-1. The first column of 10 × 4 matrix is created which contain 8 bit binary representation of power's of 2 and rest all contains zeros. The key expansion function takes the user supplied 16 bytes long key and utilises the previously created matrix in the RCON function and the s-box to generate a 176 byte long key schedule.
- Poly_mat function generates the table used in mix columns step in the cipher function. The row-wise

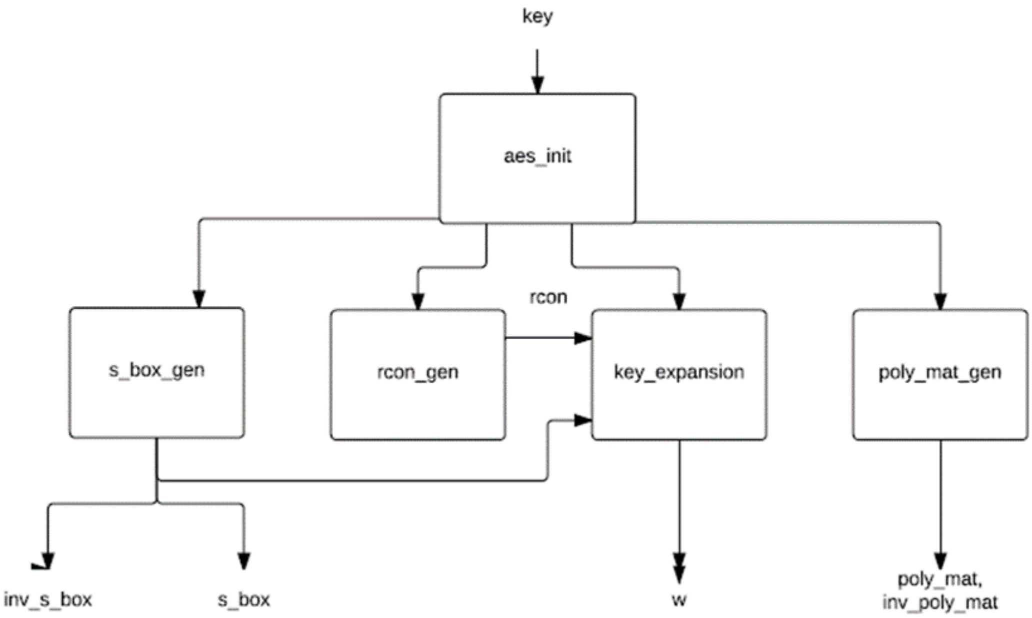

Fig .1 Initialisation function AES_init.

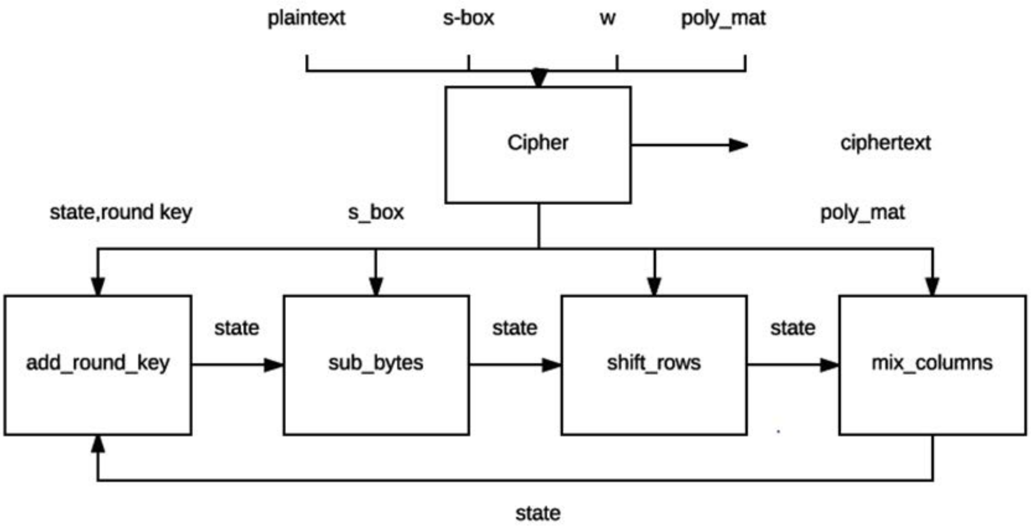

Fig . 2 Encryption function cipher.

permutation of a circulant matrix is achieved by the function by calling a sub-function 'cycle'. The cycle function performs right-shift to the previous row of a 4 × 4 matrix.

Cipher function takes in expanded key, S_box, poly_mat from AES_init and plaintext Pt as input arguments (Fig. 3) illustrates the cipher function diagramatically.

- **Add round key:** Performs simple XOR operation between state matrix and round key.
- **Sub-bytes:** Performs Substitution using S_box.
- **Shift-rows:** Rows of state matrix is cyclically permuted to left.
- **Mix-columns:** New state matrix S′ is computed by left-multiplying the current state matrix S by the polynomial matrix P.

$S' = P.S$

Encryption Process

- The Euclidean distance computation done from fingerprint's is diagrammatically illustrated in Fig. 4.
- The user inputs his/her fingerprint from which

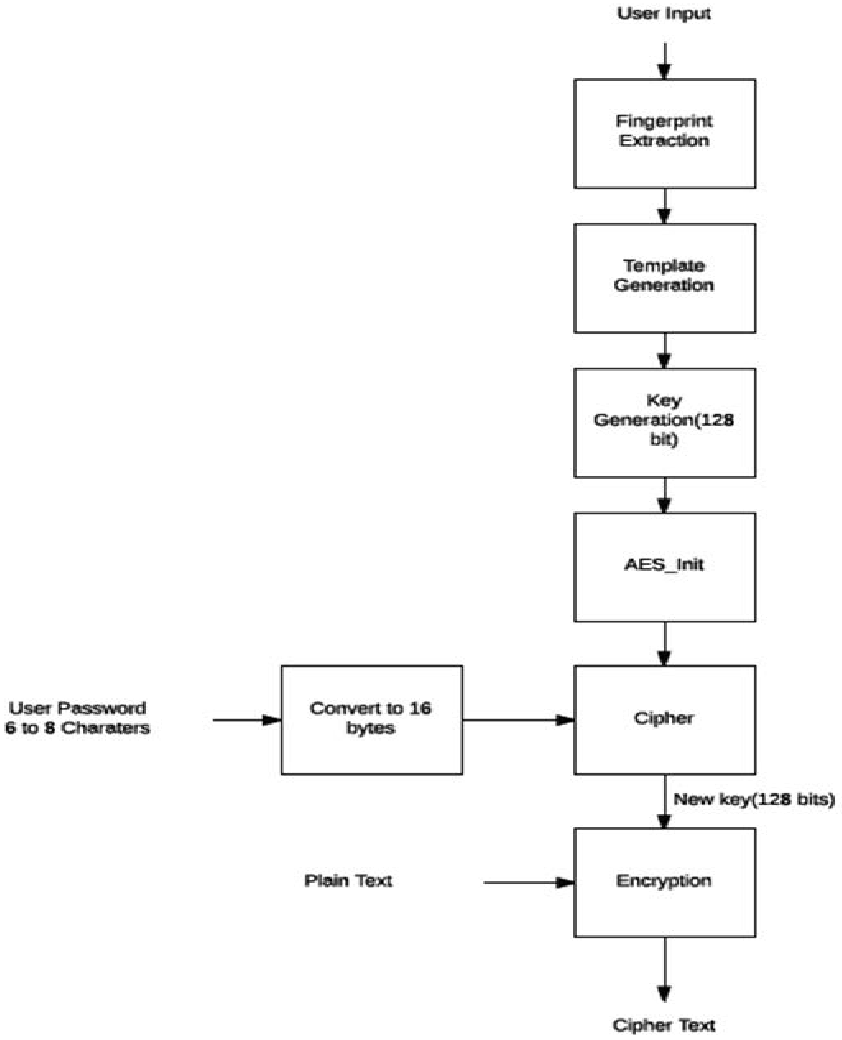

Fig . 3 Encryption process of the proposed system.

the minutia points are extracted (Sathiya, *et al.*, 2014) as (x, y) co-ordinates.

- A vector of the form m=[m1, m2….mn] is obtained using these minutia points.
- Euclidean distance between each two points is computed using this formula :
- dij=√ (xi - xj)2 + (yi -yj)2
- D=[d1, 1, d1, 2, ……dk, k+1, dk, k+2,..., dn, n]
- Duplicate values of distances are removed and the left values are sorted in ascending order.
- UA=[u1, u2……uk]
- Where uj is the distance u1<u2<u3<….uk and k is the number of unique distances in u.
- A vector Vfk of length n=maximum distance value is created, wherein dk is inserted at index dk and the empty fields are filled with 0.
- All non-zero distances are replaced by 1.
- To get a 128 bit key for AES encryption the vector Vfk is truncated and converted to 16 byte form as the code takes in 16 byte key (key-1) as parameter for encryption.
- The user inputs 6 to 8 character password which is then converted to it's ASCII equivalent.
- For getting 16 byte plain text (Pt) the password is flipped where Ptf=fliplr (Pt) and concatenated as follows:
- 6 characters: 4 bytes 0, 1, 0, 1 are concatenated alternately between the password and reversed password.
- Here e=[0, 1]
- (where 0 represents 0000 0000b and 1 represents 0000 0001b)

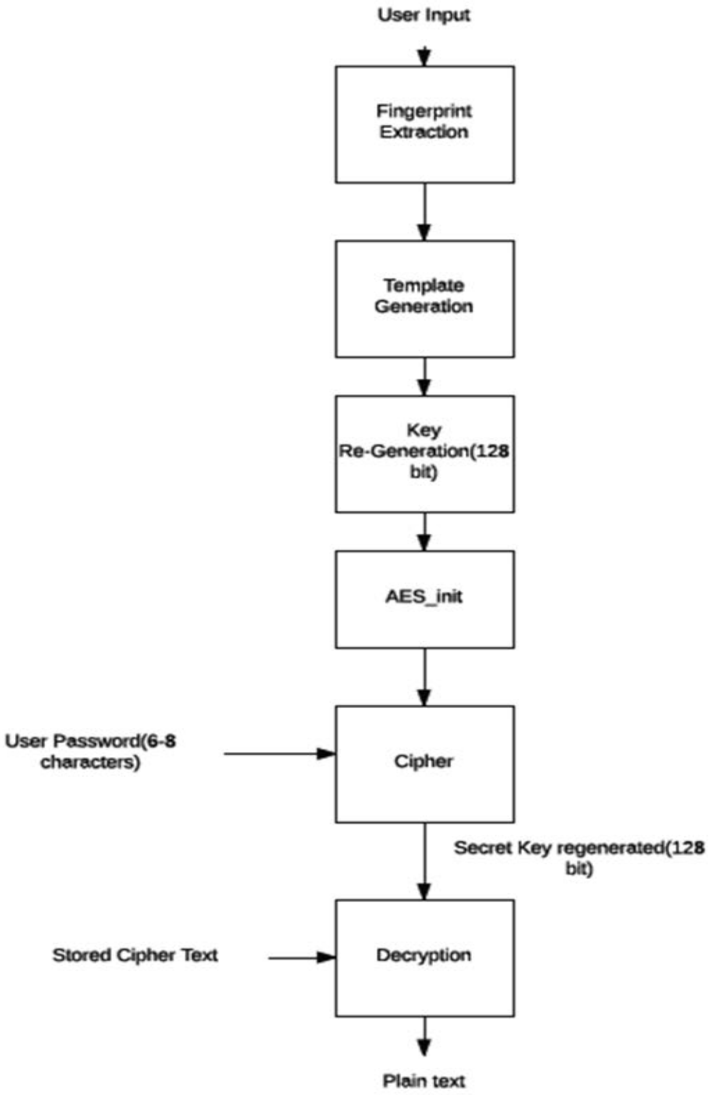

Fig . 4 Decryption process of the proposed system.

- Pt=[Pt, e, Ptf, e]
- Let Pt=[ABCDEF] then Ptf=[FEDCBA]
- Final Pt=[ABCDEF01FEDCBA01]
- 7 characters: 2 bytes 0, 1 are concatenated between the password and reversed password.
- Here e=[0, 1]
- Pt=[Pt, e, Ptf]
- Let Pt=[ABCDEFG] then Ptf=[GFEDCBA]
- Final Pt=[ABCDEFG01GFEDCBA]
- 8 characters: The password and reversed password are concatenated.
- Pt=[Pt, Ptf]
- Let Pt=[ABCDEFGH] then Ptf=[HGFEDCBA]
- Final Pt=[ABCDEFGHHGFEDCBA]
- The 16 byte key and plaintext is passed to AES_ init and cipher functions for AES encryption to get the final 16 byte encryption key.

Decryption Process

- The user enters password and fingerprint
- The fingerprint is used to extract minutia and regenerate the 128 bit key.
- The user password is converted to 16 byte plaintext using the same procedure as in the encryption part.
- The 128 bit key is converted to 16 byte format.
- The 16 byte plaintext and key are fed to the aes_ init and cipher function to get the final key.

EXPERIMENT AND RESULTS

FVC2002-DB2 fingerprint database, which is a free public domain database for fingerprint is used to evaluate the proposed system. This fingerprint database has 800 images with 10 images each for a fingerprint that has differing quality. For this proposed system, images with high quality is manually selected and used. Table 1 shows the experimental results of the proposed system computed based on FTCR, FAR and GAR.

The proposed system enforces on giving more security via making use of AES encryption system along with varying length of user password. But still other criteria such as failure to capture rate (FTCR), genuine acceptance rate (GAR) and false acceptance rate (FAR) is again evaluated to verify system does-not loses its previous existing precision with the new integration of user password and AES encryption. FTCR is computed when image quality is low and the minutia points extracted is below the threshold value. FAR basically means imposter or the wrong user is mapped with someone else fingerprint thereby giving them access to private key. In this system value of FAR is 0% because we have user password layer. Hence it's nearly impossible to map a genuine user's fingerprint with an imposter's fingerprint to retrieve the secret key, since imposter need to enter password which only genuine user knows. GAR is whether genuine user is given access to his own account. There is no variation from the existing system (Burr, *et al*., 2006) since we are not changing any algorithm for minutia extraction (Table 1).

CONCLUSION AND FUTURE WORKS

This system comprises of two layers of security via user password and his biometric feature. In existing system once fingerprint is lost, it cannot be again reused because of the irrevocability property. But with the user password layer, if the user fingerprint gets lifted, he can choose to use the same fingerprint but with a different password. But in our system password ranges from 6 to 8 characters so attacker has to still guess range and then do a dictionary attack. With the use of AES encryption scheme the proposed system is fool proof to attack. Hence instead of using directly 128 bit key from the fingerprint through this varying level of security feature, a new 128 bit key is generated from the proposed system which will be used for further encryption and decryption. Assumptions considered for the systems are, manual inputting of high quality fingerprint for enrolment and same image is used for encryption and decryption process.

The current code takes only high quality fingerprint images and the code for preprocessing (for low quality images) will be incorporated in future works. Also the current system is only for a single user, in future we plan to use asymmetric encryption algorithm using iris and fingerprint for a sender receiver system (Jaya Lakshmi and Ramesh babu, 2012).

Table 1. Experiment result of proposed system

FVC2002 DB2	Results
GAR (%)	91
FAR (%)	0
FTCR	2

REFERENCES

Advanced Encryption Standard (AES) (2001) Federal Information Processing Standards Publication 197 issued by National Institute of Standards and Technology (NIST) on 26th November 2001.

Burr, W.E., Dodson, D.F. and Polk, W.T. (2006). Information Security: Electronic Authentication Guideline. *NIST Special Report*. 800-863.

Hao, F., Anderson, R. and Daugman, J. (2006). Combining Crypto with Biometrics Effectively. *IEEE Transactions on Computers*. 55(9) : 1081-1088.

Jörg, I. and Buchholz, J. Department of Mechanical Engineering, Hochschule Bremen.

Juels, A. and Sudan, M. (2002). A fuzzy vault scheme, in Proceedings of IEEE International Symposium on Information Theory, Lausanne, Switzerland. 408.

Jaya Lakshmi, A., Ramesh babu, I. (2012). PKI key generation using multimodal biometrics fusion of fingerprint and iris. IJESAT

Li, C. and Xiao-Long, Z. Feature-based image registration using bifurcation structures. Matlab Central.

Nandakumar, K., Jain, A. and Pankanti, S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Trans. on Information Forensics and Security*. 2(4) : 744-757.

Pooja, S. and Arjun, C.V. Enhanced Symmetric Crypto-Biometric System using user-password: A Proposal. unpublished.

Subhas, B., Chattopadhyay, S. and Samanta, D. (2014). Fingerprint Based Symmetric Cryptography. *High Performance Computing and Applications (ICHPCA). International Conference*.

Sathiya, M.M., Jayaraj, R. and Jagadeesan, J. (2014). Fingerprint Authentication System Using Minutiae Matching and Application. *IJCSMC*.