International Journal of Current Research in Science and Technology
Volume 1, Issue 8 (2015), 13–19.
ISSN: 2394-5745
Available Online: http://ijcrst.in/

International Journal of Current Research in Science and Technology

An Implementation of Hybrid Cryptographic Protocol For Facial Image Security

Research Article

Dr.M.Gobi[1] and R.Sridevi[2]*

1 Department of Computer Science, Chikkanna Government Arts College, Tiruppur, Tamil Nadu, India.

2 Department of Computer Science, PSG College of Arts & Science, Coimbatore, Tamil Nadu, India.

Abstract: Security is a prime concern for user authentication and there are so many methods to ensure the user authentication. One of the available methods is biometric authentication. Encryption is also considered to be the better alternative to enhance the security of the biometric images. Even though, there are so many biometric traits used for user authentication, this work considers only the facial images of the user for their authentication due to its simplicity and ease of implementation. The core aim of this paper is to implement a security protocol for facial image security using both symmetric and asymmetric cryptographic techniques. This hybrid approach ensures the security of facial image while transferring through unreliable communication channel against various security attacks. Symmetric algorithms provide a simple biometric encryption. Since the key distribution in symmetric cryptographic algorithms is critical, the secret key of the symmetric algorithms can be encrypted using asymmetric cryptographic algorithms and so provide higher security. In this paper, the proposed protocol, an effective mechanism for confidentiality and authentication for facial image security system by using AES and ECC. The performance is measured considering the various factors like file size, encryption time, decryption time, throughput, False Acceptance Rate and False Rejection Rate.

Keywords: Biometric Security, Facial Image, Hybrid Cryptography, AES, ECC.

1. Introduction

The traditional user authentication methods unfortunately do not authenticate the user accurately. These password based methods are not fully secure. Passwords often are easily accessible to other users tend to share their passwords with their others to the ease of their work. Biometrics authenticate human as they are. The biometric systems are proper and reliable, which is not so easy to achieve. Biometric characteristics are unique and not duplicable or transferable [1]. Since, the security of biometric images has attracted more attention, many different biometric methods for image encryption have been proposed to improve the security of images. These techniques convert a biometric image to another format that is not easy to understand. Image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt images [2].

Arun Rossa, Anil Jaina, James Reismanb deliberated hybrid technique constructing the ridge feature map for the biometric image. To determine the translation and rotation parameters relating the query Minutiae matching are used and the template images are used for ridge feature map extraction [3]. Sonam Shukla, Pradeep Mishra deals with the concerns associated with identity verification, which are currently at the heart of numerous concerns in our society. They also discussed fingerprint and face biometric systems along with the decision and fusion techniques used in these systems [4].

* *E-mail: srinashok@gmail.com*

K.Kavitha and Dr.K.Kuppusamy proposed facial recognition system, which automatically identifies or verifies a person from a digital image. This can be done by comparing the selected facial features from the image and a facial database [5]. Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi, proposed new symmetric key algorithm in which a modular 37 function is used and they calculated inverse of the selected integer using modular 37. The symmetric key distribution is done in the secured manner [6].

The following sections of the paper are organized as follows: In section II,a description ofthe various biometric traits that can be used for user authentication is discussed. In section III, a brief description of both symmetric and asymmetric algorithms is given. Section IV analyses the biometric security which is crucial to keep any biometric secure for its usage for authentication. Section V, a new protocol proposing a hybrid combination of AES and ECC cryptographic techniques for facial image security is discussed. In section VI, performance parameters based on which the efficiency of the protocol can be evaluated are analysed and finally conclusion is drawn in section VII.

2. Biometric Techniques

A biometric is a distinctive, computable, genetic characteristic or trait for automatically recognizing or verifying the identity of a human being. Biometric technologies are typically used to analyse human characteristics for security purposes. Some of the most common physical biometric patterns analysed for security purposes are the fingerprint, face, hand, eye and voice [7].

Biometric identification consists of two stages: enrollment and authentication. During the enrollment stage, a biometric sample of the user is acquired. The biometric is then encrypted and the encrypted biometric is stored for subsequent comparison purposes. During the authentication stage, an updated biometric sample is acquired. This updated biometric is then compared with the previously stored biometric after decryption. It is suitable to distinguish between the two different objectives of biometric systems: biometric identification and authentication. Biometric identification is the process, where matching of a biometric an individual is done with one of a large set of system users, whereas biometric authentication simply verifies that the individuals authenticity just by retrieving only one biometric template from the database. This biometric template is matched with the verification sample. Authentication is typically used in controlled environment where access is being monitored. Biometric authentication thus processes a one-to-one match rather than a one-to-many search [8].

3. Cryptographic Techniques

Cryptography is the clambering of the content of data, image, audio, video to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main objective of cryptography is to keep data secure from hackers. The reverse of data encryption is data decryption. The security level of an encryption algorithm is measured by the key size. The larger size of the key is, the more time the attacker needs to spend for the exhaustive search of the key, and thus the higher the security level is. Commonly used key sizes are of 128,192 or 256 bit. The efficiency of the encryption algorithm depends on the secrecy of the key, length of the key, the initialization vector. Cryptography algorithms may either be symmetric algorithms, which use secret key or asymmetric algorithms, which use public and private keys [9].

a. **Symmetric Cryptography**

A symmetric key cipher is a block cipher, a method of encrypting data in which a cryptographic key and algorithm which are applied to a block of data at once as a group rather than to one bit at a time. The exact transformation is controlled using the secret key. A highly influential block cipher design in the advancement of modern cryptography

is Data Encryption Standard. The National Institute of Standards and Technology is a federal agency that approved the Data Encryption Standard (DES) block cipher an early encryption algorithm created in the mid-1970s. DES is now considered to be not secure for many real time applications since its 56-bit key was broken in January, 1999 in 22 hours and 15 minutes.In recent years, the symmetric cipher has been superseded by the Advanced Encryption Standard (AES). AES may have 10, 12, or 14 rounds. The key sizes could be 128,192 or 256 bits depending upon the number of rounds. AES uses various rounds and each round is made of several stages. To provide security, AESmakes use of transformations like Substitution, permutation, mixing and key adding each round of AES except the last uses the four transformations [9]. Symmetric key algorithms have been analysed for various file features like different data type, data size , data density and key size, and analysed the difference in encryption time for different selected cipher algorithms. As the size of data increase the encryption time also increase proportional to data size and vice versa. AES seems to be fastest block cipher with the encryption rate of 108MB/sec [10].

b. **Asymmetric Cryptography**

An advantage of asymmetric algorithms is that they are more computationally intensive than symmetric algorithms, and therefore encryption and decryption take longer [11]. ECC uses a relatively shorterkey which makes it faster and requires less computing power than other asymmetric algorithms. For example, a 160-bit ECC key affords the same security as a 1024-bit RSAkey and can be up to 15 times faster, depending on the platform on which it is executed [12]. A Comparison of the key lengths for the RSA and ECC given the same security level is given in Table 1 [13].

Table 1. **Comparison of Key Lengths for RSA and ECC for the same security level**

Time to break (MIPS years)	RSA/DSA,key size (bits)	ECC key size (bits)	RSA/ECC,key size ratio
104	512	106	4.8:1
109	768	132	5.8:1
1011	1024	160	6.4:1
1020	2048	210	9.8:1
1079	21000	600	35.0:1

To achieve 163-bit ECC/1024-bit RSA security level, an elliptic curve exponentiation for general curves over prime fields is roughly 5 to 15 times as fast as an RSA private key operation, depending on the platform and optimizations. This ratio is between 20 and 60 for 256-bit ECC/3072-bit RSA security level depending on optimizations. To secure a 256-bit AES key, ECC-521 is expected to be 400 times faster than 15,360-bit RSAapproximately [14]. Even though, Asymmetric cryptography doesnt work goodfor transmission of images because of the bulk data capacity, strong pixel correlation and high redundancy [15, 16].

c. **Hybrid Cryptography**

Hybrid encryption is a mode of encryption that associates two or more encryption systems. It integrates a combination of asymmetric and symmetric encryption to benefit from the fortes of each form of encryption ensuring their strengths respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme balances the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme. It is done through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. Since, AES is proved as one of the best symmetric key algorithms and ECC is proved for its high security with lower key sizes among all other asymmetric algorithms, a hybrid combination of AES with ECC would work better and efficient.

4. Biometric Security

Biometric systems may become vulnerable to some potential attacks. Some of those security vulnerabilities include spoofing, replay attacks, substitution attacks, tampering, masquerade, Trojan horse etc., in many commercial biometric systems, both in terms of FRR and FAR.High FRR causes inconvenience for legitimate users and prompts the system administratorto lower a verification threshold. This inevitably gives rise to FAR, which, in turn, lowersthe security level of the system.
Anyways, there are some advantages of Biometric Encryption over other Biometric Systems: NO retention of the biometric image or template, Multiple / cancellable / revocable identifiers, improved authentication security: stronger binding of user biometric and identifier, improved security of personal data and communications, Greater public confidence, acceptance, and use; greater compliance with privacy laws, Suitable for large-scale applications [17].
The collection of biometric samples is subjected to great variability. Biometrics is fuzzy which means no two samples will be perfectly identical. Biometric system designers can lower the false rejection rate (FRR) oftheir systems so this variation is reduced and the system can function properly. One of the alternate ways to do this is to lower the threshold for matches to occur. However, this approach often increases the false acceptance rate (FAR) of thesystem, that is, the system will incorrectly match a biometric to the wrong stored reference sample, resulting in misidentification. Usually there is a trade-off between FRR and FAR, i.e.,one error rate may only be reduced at the expense of the other. Some applications require lower FRR but can tolerate higher FAR, and vice versa [18].

5. Proposed System

In this paper, a new hybrid cryptographic protocol is proposed as in Figure 1. In our protocol, biometrics and cryptography are perfectly integrated. The proposed bio-cryptographic protocol consists of two phases namely user registration and user authentication, which are presented in the following subsections.

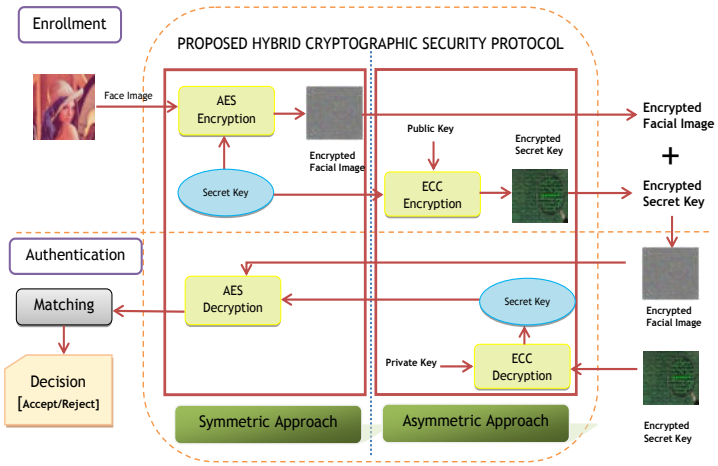

Figure 1. **Proposed hybrid cryptographic Security Protocol**

In the enrollment process of the protocol, the facial image is employed to work with AES symmetric key algorithm for its encryption.Symmetric key is generated and are never exposed externally. This symmetric key is then encrypted using a powerful ECC algorithm to store it secure in the database. Establishment of symmetric session keys does not need a conventional key exchange process which further reduces the vulnerability risk [19]. In the authentication phase, an updated

facial image is acquired from the user for ensuring the authentication. The encrypted symmetric key stored in the database is decrypted using user's private key and it is in turn used to decrypt the facial image. This decrypted facial image is then compared with the acquired, updated facial image collected from the user.The authentication module can only output either an 'accept' or 'reject' decision. Here, authentication module provides a mechanism for the cryptographic module which makes the whole system vulnerable to attacks which may tamper with the biometric authentication module and simply inject an 'accept' command to the system.A threshold 't' regulates the system decision. The system infers that pairs of facial image samples generating scores higher than or equal to t are mate pairs. Consequently, pairs of facial image samples generating scores lower than t are non-mate pairs. The distribution of scores generated from pairs of samples from different persons is called an impostor distribution; the score distribution generated from pairs of samples from the same person is called a genuine distribution.

The curves in Figure 2 show false acceptance rate (FAR) and false rejection rate (FRR) rate for a given threshold t over the genuine and impostor score distributions. FAR is the percentage of non-mate pairs whose matching scores are greater than or equal to t and FRR is the percentage of mate pairs whose matching scores are less than t [20].

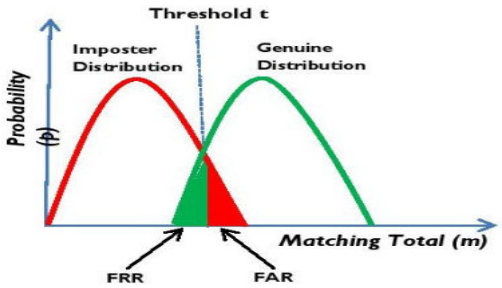

Figure 2. **Genuine Distribution over Imposter Distribution showing FAR and FRR**

6. Results and Discussion

The following parameters are considered for evaluation of the protocol combining AES and ECC for facial image security.

- Encryption time (Computation Time/ Response Time)
- Decryption time (Computation Time/ Response Time)
- Throughput
- Plain text Size/Cipher text Size [12]

For each matching result, we calculate the probability ofa genuine user/imposter passes the authentication test. The FAR and FRR are calculated as:

$$\text{FAR} = \frac{\text{Probability of an impostor passes a test}}{\text{Total number of impostor tests}}$$

$$\text{FRR} = \frac{\text{Probability of a genuine test be rejected}}{\text{Total number of genuine tests}}$$

The protocol was implemented in Java and tested on a PC with public domain database. The main purpose is to estimate the encryption and decryption time of facial images using AES algorithm. In stage two, we evaluate encryption of secret key using ECC scheme using Java Implementation in order to investigate its feasibility, resource demand, and computational speed. A few basic functions in the open-source cryptographic libraries have been utilized, to handle cryptography-related

operations such as mathematical operations over the Galois Field. The domain parameter of ECC we used is secp256v1. Portions of the research in this paper use the CASIA-FaceV5collected by the Chinese Academy of Sciences' Institute of Automation (CASIA). It contains 2,500 colour facial images of 500 subjects which are captured using Logitech USB camera in one session. All face images are 16 bit colour BMP files and the image resolution is $640 * 480$.

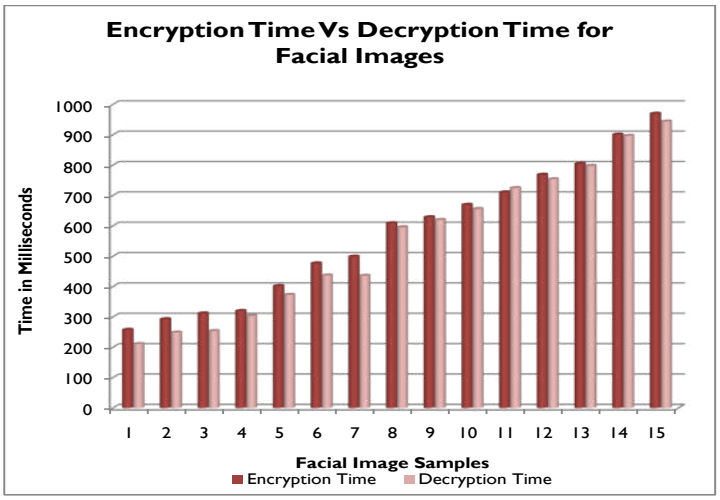

Figure 3. **Comparison of Encryption and Decryption time for Facial images**

Figure 3 shows the performance analysis of encryption time and decryption time for facial image images, when encrypted with AES algorithm. The secret key is in return encrypted with ECC and as the secret key generated for AES encryption is 128 bit each for different samples, the encryption time for the secret key using ECC remains almost the same for the keys generated. The encryption time and decryption time has its paramount importance for varied facial image sizes as this determines the time involved in converting facial image into encrypted image. Here, we can observe that the time taken for AES encryption and decryption is lesser as compared to other symmetric algorithms.

7. Conclusion

Among the biometric images used for authentication, Facial images are an essential component of any identity-based security system because of its simplicity. This work presents the hybrid cryptographic protocol including AES and ECC algorithms together to provide high security for the facial images. In the enrollment phase, the facial image is encrypted using AES algorithm and the AES secret key is encrypted using ECC. The authentication phase decrypts the AES secret key followed by the decryption of facial image, which is compared with the updated facial image to check for its authenticity.Based on the facial images and the experimental results, it was concluded that AES algorithm consumes lesser encryption and decryption time as compared to other symmetric algorithms.

References

[1] Matyás, Václav, and Zdenek Riha, *Biometric authenticationsecurity and usability*, Advanced Communications and Multimedia Security, Springer US, (2002), 227-239.

[2] Shah, Jolly, and Vikas Saxena, *Performance Study on Image Encryption Schemes*. arXiv preprint arXiv:1112.0836 (2011).

[3] Ross, Arun, Anil Jain, and James Reisman, *A hybrid fingerprint matcher*, Pattern Recognition, 36(7)(2003), 1661-1673.

[4] Shukla, Sonam, and Pradeep Mishra, *A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits*, IJCSES 1(2)(2010).

[5] K.Kavitha and K.Kuppusamy, *A Hybrid Biometric Authentication Algorithm*, International Journal of Engineering Trends and Technology, 3(3)(2012), 311319.

[6] Kuppuswamy, Prakash, and Dr.Saeed QY Al-Khalidi, *Implementation Of Security Through Simple Symmetric Key Algorithm Based On Modulo 37*, International Journal of Computers & Technology, 3(2)(2012).

[7] M.Gobi and D.Kannan, *A Secured Public Key Cryptosystem for Biometric Encryption*, International Journal of Computer Science & Information Technologies, 5(1)(2014).

[8] Encryption, Biometric, et al., *chapter 22 in ICSA Guide to Cryptography*, edited by Randall K. Nichols, (1999).

[9] Soni, Shraddha, H.Agrawal and M.Sharma, *Analysis and comparison between AES and DES Cryptographic Algorithm*, International Journal of Engineering and Innovative Technology, 2(6)(2012), 362-365.

[10] Masram, Ranjeet, et al., *Analysis and Comparison of Symmetric Key Cryptographic Algorithms based on Various File Features*, International Journal of Network Security & Its Applications, 6(4)(2014).

[11] Guru and Omkar, *Implementation of cryptographic algorithms and protocols*, Diss. National Institute of Technology Rourkela, (2007).

[12] M.Seetha, Anjan K. Koundinya and C.A.Prashanth, *Comparative Study and Performance Analysis of Encryption in RSA, ECC and Goldwasser-Micali Cryptosystems*.

[13] Abdurahmonov, Tursun, Eng-Thiam Yeoh, and Helmi Mohamed Hussain, *The implementation of Elliptic Curve binary finite field (F 2m) for the global smart card*, Research and Development (SCOReD), 2010 IEEE Student Conference on. IEEE, (2010).

[14] Lauter and Kristin, *The advantages of elliptic curve cryptography for wireless security*, IEEE Wireless communications, 11(1)(2004), 62-67.

[15] M.Gobi and R.Sridevi, *Performance Analysis of Biometric Image Encryption in Transformed Formats using Public Key Cryptography*, International Journal of Scientific & Engineering Research, 6(2)(2015).

[16] Gupta, Kamlesh and Sanjay Silakari, *Efficient hybrid image cryptosystem using ecc and chaotic map*, International Journal of Computer Applications, 29(3)(2011).

[17] Soutar, Colin, et al., *Biometric Encryption: enrollment and verification procedures*, Aerospace/Defense Sensing and Controls. International Society for Optics and Photonics, (1998).

[18] Cavoukian, Ann and Alex Stoianov, *Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy*, Information and Privacy Commissioner, Ontario, (2007).

[19] M.Gobi and R.Sridevi, *Multi-Biometric Authentication through Hybrid Cryptographic System*, International Conference on Computing and Intelligence Systems, 04(2015).

[20] Prabhakar, Salil, Sharath Pankanti and Anil K. Jain, *Biometric recognition: Security and privacy concerns*, IEEE Security & Privacy, 1(2)(2003), 33-42.