Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

A DESIGN AND IMPLEMENTATION OF HYBRID SECURED PROTOCOL FOR BIOMETRIC IMAGES

Dr.M.Gobi[1], Mrs.R.Sridevi[2]
[1]*Department of Computer Science, Chikkanna government Arts College, Coimbatore*
[2]*Department of Computer Science, PSG College of Arts & Science College, Coimbatore*

Abstract— in the modern world, security threat is a prime issue for authentication and encryption is one of the best alternative ways to ensure security. Moreover, many image encryption schemes have been proposed to authenticate the user. The objective of this paper is to design a new security protocol for fingerprint security using hybrid cryptographic model. The hybrid model is a combination of symmetric and asymmetric cryptographic techniques. The security of fingerprint transfer through unreliable communication channel is challenging, because of various external attacks. The various cryptographic protocols like AES, DES, and 3 DES are currently using biometric solution. But, the key distribution in symmetric cryptographic algorithms is major concern. The new protocol makes more secure and easy to encrypt and decrypt the fingerprint images. In this paper, the proposed protocol, an effective mechanism for confidentiality and authentication for fingerprint security system by using AES and ECC. The performance analysis takes into consideration the various factors like file size, encryption time, decryption time, throughput, False Acceptance Rate and False Rejection Rate to measure the effectiveness of the protocol.

Keywords— Biometric Security, Fingerprint, Hybrid Cryptography, AES, ECC.

I. INTRODUCTION

The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today.

The traditional methods of the user authentication inappropriately do not authenticate the user as such. These methods are based upon properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to other users tend to pass their tokens to or share their passwords with their others to make their work easier. Biometrics, on the other hand, authenticates humans as such. The biometric system used is working properly and reliably, which is not so easy to achieve. Biometrics is programmed methods of identity verification or identification based on the principle of assessable physiological or behavioural characteristics such as a fingerprint, an iris pattern or a voice sample. Biometric characteristics are unique and not duplicable or transferable (Matyáš et al, 2002).

Since, the security of biometric images has attracted more attention. Recently, and many different biometric image encryption methods have been proposed to enhance security of images. These techniques try to convert a biometric image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data (Shah et al, 2011).

Arun Rossa, Anil Jaina, James Reismanb deliberated hybrid technique constructing the ridge feature map for the biometric image. Minutiae matching are used to determine the translation and rotation parameters relating the query and the template images for ridge feature map extraction (Ross et al, 2003). Sonam Shukla, Pradeep Mishra in this their proposal concerns associated with identity verification are currently at the heart of numerous concerns in our modern society. They also

discussed fingerprint and face biometric systems, decision and fusion techniques used in these systems (Sonam et al, 2010).

K.Kavitha and Dr.K.Kuppusamy proposed facial recognition system for automatically identifying or verifying a person from a digital image. One of the ways to do this is by comparing the selected facial features from the image and a facial database (Shukla et al, 2010). Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi, proposed new symmetric key algorithm. They proposed a modular 37 function and select any number and calculate inverse of the selected integer using modular 37. The symmetric key distribution should be done in the secured manner (Kavitha et al, 2012).

The following sections of the paper are organized as follows: In section II, a description of the 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 fingerprint 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.

II. BIOMETRIC TECHNIQUES

A biometric is defined as a unique, measurable, biological 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, hand, eye, face, and voice (Gobi et al, 2014).

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 main objectives of biometric systems: biometric identification and authentication. Biometric identification is the process of matching an individual to one of a large set of system users, whereas biometric authentication simply verifies that the individual is who he or she claims to be. Hence, only one biometric template is retrieved from the database of users and matched with the verification sample. Authentication is typically used in circumstances where access is being controlled, whether physical access, or access to an electronic system such as the logon to a computer system. Biometric authentication thus processes a one-to-one match rather than a one-to-many search (Nichols et al, 1999).

III. CRYPTOGRAPHIC TECHNIQUES

Cryptography is the scrambling of the content of data, may be text, image, audio, video to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography is to keep data secure form unauthorized attackers. The reverse of data encryption is data decryption. Original data that is to be transmitted or stored is called plaintext, whereas the data, which is unreadable, neither human nor machine is called cipher text.

The security level of an encryption algorithm is measured by the size of its key. The larger size of the key is, the more time the attacker needs to do 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 strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together. Cryptography algorithms are either symmetric algorithms, which use symmetric keys, also called secret keys or asymmetric algorithms, which use asymmetric keys, also called public and private keys (Soni et al, 2012).

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 (NIST) 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 insecure for many applications since its 56-bit key was broken in January, 1999 in 22 hours and 15 minutes. In recent years, the 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 numerous rounds in which each round is made of several stages. To provide security, AES uses types of transformations like Substitution, permutation, mixing and key adding each round of AES except the last uses the four transformations (Masram et al, 2014).

Symmetric key algorithms have been analysed for various file features like different data type, data density, data size and key size, and analysed the variation of 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 is appears to be fastest block cipher with encryption rate of 108MB/sec at bare minimal parameter (Guru, 2007).

B. ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message to make it secure. Any user who wants to send an encrypted message can get the recipient's public key from a public directory to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their own private key, which is kept secret at all the time. An advantage of public-key algorithm is that they are more computationally intensive than symmetric algorithms, and therefore encryption and decryption take longer. This may not be significant for a short text message, but certainly is for bulk data encryption.

ECC uses a relatively shorter key which makes it faster and requires less computing power than other public key algorithms. For example, a 160-bit ECC key affords the same security as a 1024-bit RSA key and can be up to 15 times faster, depending on the platform on which it is executed (Seetha et al, 2009). A Comparison of the key lengths for the RSA and ECC given the same security level is given in Table 1 (Abdurahmonov et al, 2010).

TABLE 1 . COMPARISON OF KEY LENGTHS FOR RSA AND ECC FOR THE SAME SECURITY LEVEL

Time to break	RSA/DSA key size	ECC key size	RSA/ECC key size ratio
(MIPS years)	(bits)	(bits)	(bits)
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

At the 163-bit ECC/1024-bit RSA security level, an elliptic curve exponentiation for general curves over arbitrary prime fields is roughly 5 to 15 times as fast as an RSA private key operation,

depending on the platform and optimizations. At the 256-bit ECC/3072-bit RSA security level the ratio has already increased to between 20 and 60, depending on optimizations. To secure a 256-bit AES key, ECC-521 can be expected to be on average 400 times faster than 15,360-bit RSA (Lauter et al, 2004).

Even though, Asymmetric cryptography doesn't fit for transmission of images because of the bulk data capacity, strong pixel correlation and high redundancy. Moreover encryption at the source and decryption at the destination lowers the encryption performance (Gobi et al, 2015) (Gupta et al, 2011).

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 is one that 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. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message. The combination of encryption methods has various advantages. One is that a connection channel is established between two users' sets of equipment. Users then have the ability to communicate through hybrid 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.

IV. 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 administrator to lower a verification threshold. This inevitably gives rise to FAR, which, in turn, lowers the 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(Soutar et al, 1998)

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 and do take measures to lower the false rejection rate (FRR) of their systems so this variability is smoothed out and the system can function properly. Apart from controlling the conditions under which fresh samples are taken, and improving the mathematical algorithms, one way to do this is to lower the threshold for matches to occur. However, the difficulty with this approach is that this often increases the false acceptance rate (FAR) of the system, 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 (Cavoukian et al, 2007).

V. 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.

In the enrollment process of the protocol, the fingerprint biometric 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 (Gobi et al, 2015).

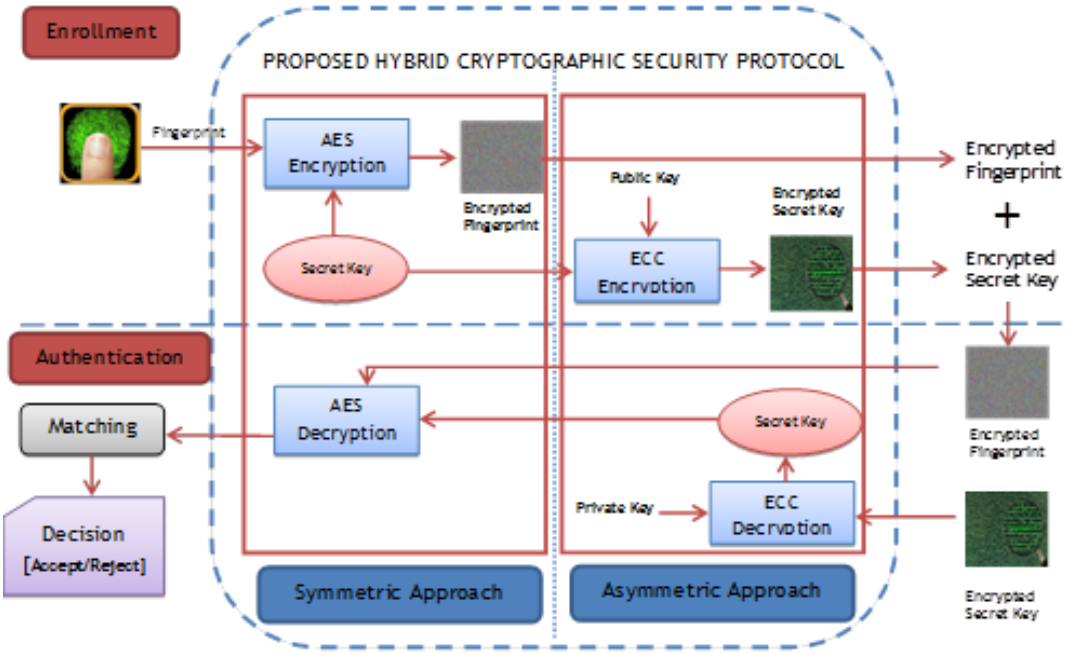

Fig. 1 A Proposed hybrid cryptographic Security Protocol

In the authentication phase, an updated fingerprint 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 fingerprint. This decrypted fingerprint is then compared with the acquired, updated fingerprint 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 biometric samples generating scores higher than or equal to t are mate pairs. Consequently, pairs of biometric samples generating scores lower than t are nonmate 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 nonmate 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 (Prabhakar et al, 2003)

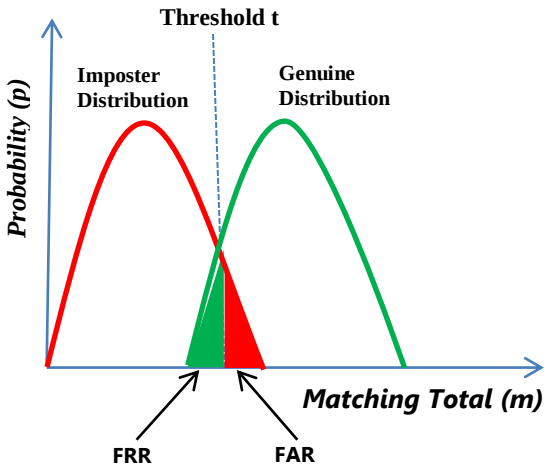

Figure. 2 Genuine Distribution over Imposter Distribution showing FAR and FRR

VI. RESULT AND DISCUSSION

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

Encryption time (Computation Time/ Response Time)

- Decryption time (Computation Time/ Response Time)
- Throughput
- Plaintext Size/Cipher text Size [21]

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

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

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

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 fingerprint 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-FingerprintV5 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA). In this experiment, a subset of fifteen fingerprints was chosen from the different impressions. CASIA Fingerprint Image Database Version 5.0 (or CASIA-FingerprintV5) has 20,000 fingerprint images of 500 different subjects. The fingerprint images of CASIA-FingerprintV5 were captured using URU4000 fingerprint sensor in one session. Each subject contributed 40 fingerprint images of eight fingers except 2 first fingers. The fingerprints were collected by rotating the fingers with various levels of pressure to generate

significant intra-class variations. All fingerprint images are 8 bit grayscale BMP files and the image resolution is 328*356 pixels.

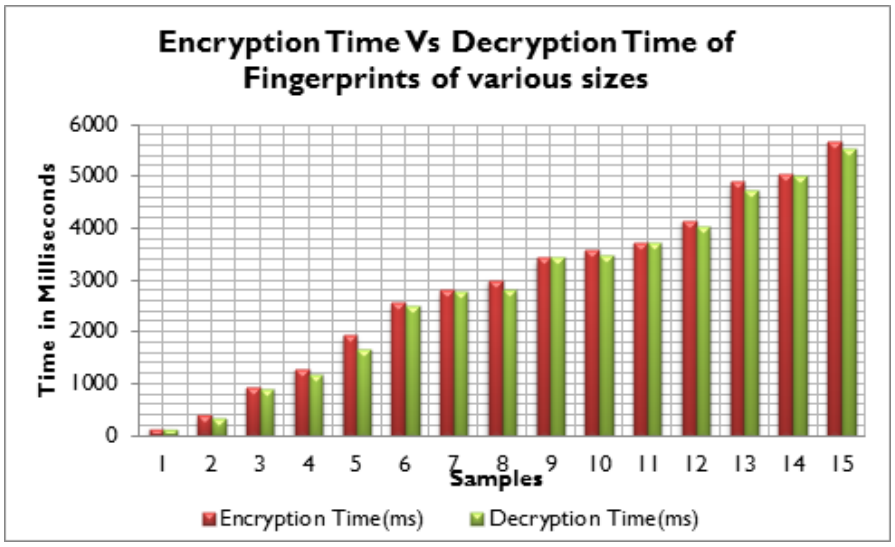

Figure 3: Comparison of Encryption and Decryption time for Fingerprint Images

Figure 3 shows the performance analysis of encryption time and decryption time for fingerprint 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 fingerprint sizes as this determines the time involved in converting fingerprint image into encrypted image. Here, we can observe that the time taken for AES Decryption is almost equal to the encryption time when compared to the other systems.

VII. CONCLUSIONS

The Fingerprint images are an essential component of any identity-based security system because no other technology can replace the requisite functionality of identifying the authorized person based on their intrinsic distinctive traits. This work presents the hybrid cryptographic protocol including AES and ECC algorithms together to provide high security for the fingerprint image. The fingerprint image is encrypted using AES algorithm and the secret key is encrypted using ECC. The authentication phase decrypts the secret key followed by the decryption of fingerprint image, which is compared with the updated fingerprint to check for its authenticity. Based on the fingerprint images and the experimental results, it was concluded that AES algorithm consumes lesser encryption and decryption time as compared to other symmetric algorithms.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

[1] Matyáš, Václav, and Zdeněk Říha. "Biometric authentication—security 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] Kavitha, K., and K. Kuppusamy. "A Hybrid Biometric Authentication Algorithm." International Journal of Engineering Trends and Technology, Volume 3, Issue 3, (2012): 311 – 319.
[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] Gobi, M., 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, Omkar. Implementation of cryptographic algorithms and protocols. Diss. National Institute of Technology Rourkela, 2007.
[12] Seetha, M., Anjan K. Koundinya, and Prashanth CA. "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, Kristin. "The advantages of elliptic curve cryptography for wireless security." IEEE Wireless communications 11.1 (2004): 62-67.
[15] Gobi, M., and Mrs 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] Gobi, M., and R. Sridevi. "Multi-Biometric Authentication through Hybrid Cryptographic System." International Conference on Computing and Intelligence Systems Volume: 04, Special Issue: March 2015.
[20] Prabhakar, Salil, Sharath Pankanti, and Anil K. Jain. "Biometric recognition: Security and privacy concerns." IEEE Security & Privacy 1.2 (2003): 33-42.