A Secured Public Key Cryptosystem for Biometric Encryption

M.Gobi[†] and D.Kannan[††],

†Assistant professor, Chikkanna Government Arts College, India
†† Research Scholar, Nehru Arts & Science College, India.

Summary
In the modern era security plays an important role in each and every field. The needs for stringent security measures in biometric systems have greater importance for information security systems. The biometric systems to offer reliable and high security to ensure invulnerability. This paper proposes two different approaches based on Elliptic curve cryptography and Hyper Elliptic curve cryptography for protection of biometric authentication systems. The implementation of public key algorithms has been realized for experimental purposes and the results thus obtained have been critically verified in this paper.

Key words:
Biometric authentication, Image encryption, Image cryptosystem, Biometric attacks, Database encryption, ECC, HECC

1. Introduction

The storage of biometric data leads to considerable risks for the authentication system and high concerns regarding the data protection. The traditional biometric authentication systems store biometric templates together with the data identifying an individual in a database for later comparison. In order to authenticate an individual the biometric data presented is looked up in the database. If a record is found with biometric data that is sufficiently close to the one presented, the person is identified and hence authenticated. This way of storing biometric data is often criticized as a mass storage of privacy sensitive personal data that is potentially threatened by internal or external attacks on the database. Therefore it would be of great value to protect biometric information by cryptographic means against not only external but also internal attacks.
Biometric is commonly categorized as either physiological or behavioral trait. Physiological traits (sometimes called passive traits) refer to fixed or stable human characteristics, such as fingerprints, shape and geometry of face, hands, fingers or ears, the pattern of veins, irises, teeth, as well as samples of DNA. Physiological traits are generally existent on every individual and are distinctive and permanent, unless accidents, illnesses, genetic defects, or aging have altered or destroyed them. Behavioral traits (active traits) measure human characteristics represented by skills or functions performed by an individual. These include gait, voice, key-stroke and signature dynamics.

The following paragraphs describe traits of both categories, which are sometimes evaluated based on such characteristics as:

- **Universality** – Each individual should have the biometric trait.
- **Distinctiveness** – Any two individuals should be different regarding the trait.
- **Permanence** – The biometric should be sufficiently invariant over a certain period of time.
- **Collectibility** – The biometric should be quantitatively measurable.

The use of biometric systems, issues of security and privacy will need to be carefully addressed, as well as the high levels of expectation in accuracy, reliability, performance, adaptability, and cost of biometric technologies for a wide variety of applications. Safety, quality and technical compatibility of biometric technologies can be promoted through standards and standardization activities. Standards are essential for the deployment of biometric technologies on large-scale national and international applications.

Fundamentally, authentication mechanisms that exist today use one or more of the following factors:

- **Knowledge-based** – an authenticator only the individual knows, which usually refers to PIN, passphrase or an answer to a secret/security question.
- **Possession-based** – an authenticator only the individual possesses, which usually refers to keys, smart cards and tokens.
- **Physiology-based** or **behavior-based** – an authenticator only the individual is or can do, referring to biometrics.

Knowledge- and possession-based authentication mechanisms imply that users –in order to be granted

Manuscript received January 5, 2015
Manuscript revised January 20, 2015

access to a system, building, service– need to carry or remember the authenticator. When it comes to comparisons of these traditional authenticators and authentication through biometrics, it is often argued that keys could be lost, stolen or easily duplicated and passphrases could be forgotten. A critical drawback is that the link between the legitimate individual and the authenticator is weak, and the authentication system has no means to distinguish between a designated owner of the authenticator and a thief, impostor or guesser. On the other hand, the general view is that biometric traits have an advantage in that they cannot be stolen, easily guessed or forgotten.

In addition to selecting a feasible biometric for an application, its interplay with a biometric system is a crucial factor for deployment decisions. The following desired quality factors may influence the choice of a specific biometric for an application:

- **Performance** – The measurement of the biometric trait is robust, accurate, fast and efficient.
- **Acceptability** – The extent to which individuals are willing to accept the use of a particular biometric trait in an application.
- **Circumvention** and **Reliability** – Extent to which the system can be manipulated by using fraudulent methods.
- **Cost.**

Some of these factors are intangible and may depend on the perception of each user. For instance, the question of whether a biometric application is acceptable or not may be linked to the user's cultural background, attitude to privacy and to technology, etc. Accuracy and performance, however, can be quantified and compared.

All biometric systems use common main functional components, which include:

- **Storage entity** with the biometric data samples (templates) of the enrolled individuals that is linked or integrated in a database with the identity information of the corresponding individuals.
- **Biometric sensor device** and pre-processing capacities to capture the biometric sample data from an individual as input data.
- **Comparison process** evaluating the similarity between reference template and captured data sample, and then calculating a matching score.
- **Decision function** that decides if the data sample matches the reference template.

The biometric attack which poses a significant threat and is potentially damaging in particular, is against the biometric templates stored in the system. Attacks on the template can lead to the following vulnerabilities:

- The stored reference template can be replaced by an impostor's template to gain unauthorized access.
- A physical spoof, essentially an imitation of the reference template, can be used to gain unauthorized access to the system.
- The stolen template can be replayed to the matcher to gain unauthorized access.

Practically any article on fingerprint security begins with a explanation of basic metrics for measuring a biometric system these are the false acceptance rate (FAR) and false rejection rate (FRR). The probability that a non-matching print will be accepted is the FAR, while the probability that a matching print is rejected is the FRR. A good system has a FAR of 10^{-6} and FRR of 10^{-4}. There is usually a tradeoff between the two values, when a system requires a greater statistical match the FAR may be decreased but the FRR will consequently increase.

Fingerprint algorithms consist of two main phases, enrollment and identification or verification. The enrolment phase, first determines the global pattern of the print, so it can be categorized in a large bucket during improve matching performance, the minutia points are then transformed by a, typically proprietary, algorithm into a template. The template is stored and used for future identification. An additional step in the enrollment process could be to search for existing matches. This leads to an interesting advantage fingerprint authentication has over password authentication. As well as being proof of being a particular person, fingerprint identification can also be used prove somebody is not a particular person or persons.

The identification phase, first determines a pattern bucket, and then submits the minutia or template, depending on the design, which can be compared to the saved template. The comparison is done with a statistical analysis, since an exact match is not expected. Matches may be found by rotating or translating the image, to compensate for the finger not being placed in an identical location on each use. The thresholds are set to dictate how close the match must be. Depending on the implementation, if the match is accepted, the saved template could be updated with the new template. This is useful if gradual changes are expected overtime, however, opens the door to a potential attack, where one person's print could be morphed into another's. Depending on the implementation, the template is

calculated on either the device side or server side. To reduce the ease of replay attacks generating the template in a trusted device is preferable.

The remainder of this paper is organized as follows. Current biometric templates protection schemes are introduced and reviewed briefly in section two. In section three, public key encryption schemes are introduced. Section four contains the proposed approaches for database protection. Experimental results and analysis are done in section five. Conclusions have been put forth in the final section.

2. Review of Literature

The widespread deployment of biometric systems and their use, a lot of concern should be taken to their security. Generic biometric system consists of five components, sensor, feature extractor, template database, matcher, and decision maker. Many crackers tried to crack biometric systems in advance to take illegal access (like accessing medical records of some patient), denial of service, and so on. Ratha et al. [1] identified eight points of attack in biometric system.

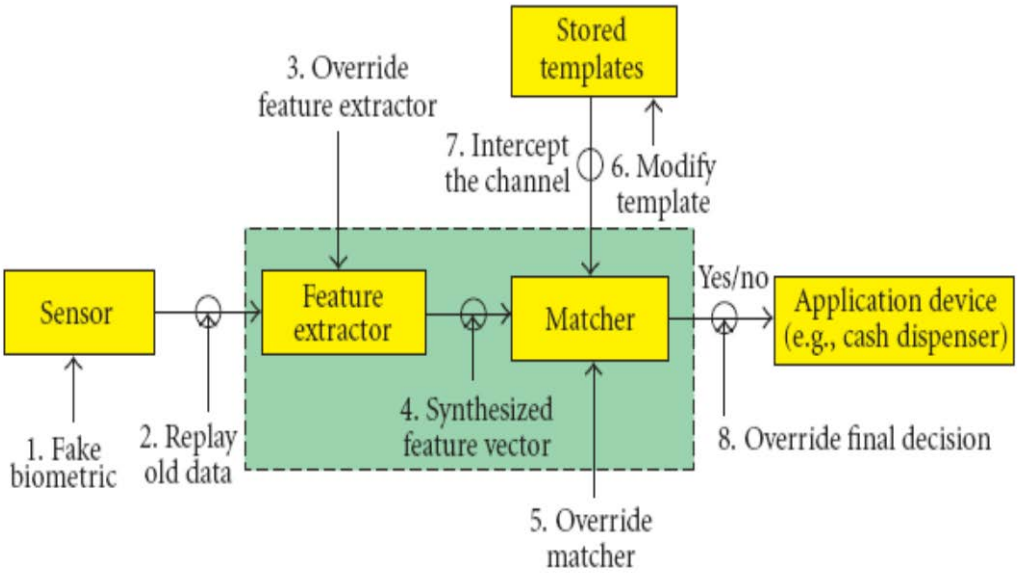


Figure : The points of attack in biometric system.

The matcher needs to compare between the live biometric data and the stored biometric template. The sixth type of attack is modifying the stored template. There are three ways for securing biometric templates. They are biometric cryptography, biometric fuzzy vault, and the certification of biometric system.

Biometric cryptography is a method to encrypt feature points or encrypt important features of biometric data. Jain et al have revised methods of cryptography and their advantages and disadvantages. The standard encryption techniques (like RSA, AES, etc) are not useful for securing biometric templates, because it leaves the biometric data exposed during every matching process. Which means matching must be in decrypted form. They revised a variety of cryptography techniques and their advantages and disadvantages. The most critical issue in cryptography is how to secure the key. They have discussed many ways to secure the key.

Fuzzy vault was introduced by Jules and Sudan. This technique concentrates on the overlapping features between two sets. Features that overlap must be equal in value and order. There is a key also hidden in the stored biometric template. Biometric fuzzy vault has two sets, the stored biometric template and the captured biometric data. These two sets overlap in important features like minutiae points in fingerprint data. Once the matcher has recognized the overlapped features, he can reconstruct the features and hence key. Scheirer and Boult have discussed many ways that lead to crack biometric fuzzy vault and biometric encryption. They have concluded that biometric fuzzy vaults are easily compromised by three types of attacks and biometric encryption can be impacted by a hill climbing algorithm and can be compromised by one type of substitution attack but with more efforts.

The last method of securing biometric templates is the certification of biometric system. In this method a whole

biometric system is developed which can secure biometric templates and their corresponding biometric data. It can use many techniques to secure the biometric template like compression of feature points or storing the biometric data on a smart card or a printed document.

Biometric system and the possible attack points are presented in figure. Ratha et al., have identified eight attack points in this scheme. The UK biometric working group (UK-BWG) lists several factors that can damage the integrity of the template as given below:

- Accidental template corruption due to a system malfunction such as a hardware failure.
- Deliberate alteration of an enrolled template by an attacker.
- Substitution of a valid template with a bogus template for the purpose of deterring system functionality.

3. Biometric Database Protection

"Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc. Identification based on biometric techniques obviates the need to remember a password or carry a token. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process.

During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrollment. Here the processed sample (a mathematical representation of the biometric - not the original biometric sample) is stored / registered in a storage medium for future comparison during an authentication. In many commercial applications, there is a need to store the processed biometric sample only. The original biometric sample cannot be reconstructed from this identifier.

A number of biometric characteristics may be captured in the processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics:

Universal: Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

Invariance of properties: They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.

Measurability: The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

Singularity: Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

Acceptance: The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.

Reducibility: The captured data should be capable of being reduced to a file which is easy to handle.

Reliability and tamper-resistance: The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.

Privacy: The process should not violate the privacy of the person.

Comparable: Should be able to reduce the attribute to a

state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.

Inimitable: The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

A biometric system can be classified into two modules- (i) Database Preparation Module and (ii) Verification Module. The Database Preparation Module consists of two sub-modules, and they are (a) Enroll Module and (b) Training Module, Verification module can be divided into two modules (a) Matching Module and (b) Decision Module.

A biometric authentication system makes two types of errors: 1) mistaking biometric measurements from two different persons to be from the same person and 2) mistaking two biometric measurements from the same person to be from two different persons. These two types of errors are often termed as false accept and false reject, respectively. There is a tradeoff between false match rate (FMR) and false non-match rate (FNMR) in every biometric system. In fact, both FMR and FNMR are functions of the system threshold; if it is decreased to make the system more tolerant to input data.

In a DRM application involving high-security top secret documents (e.g., in a nuclear reactor), the administration may want to ensure that all such documents are accessed only by authorized users. Further, unauthorized users should have a very little chance of accessing the documents. The requirement here translates to small FMR that may typically mean a large FNMR. In a less secure environment, the primary objective of the DRM system design may be user convenience and user-friendly interface. That is, a user does not want to use engineered authentication systems and would like to have reliable pervasive access to the documents. In this application, since user convenience is the primary criterion, the FNMR at the chosen operating point should be small, which may result in a large FMR

A user of the system faces several privacy issues immediately at enrolment:

• Transparency, i.e., if the purpose of the system is clear to the user;

• If the enrolment is voluntary, and what are the consequences of not getting enrolled;

• If the system can be trusted, i.e., if the personal data are adequately protected;

• Quality of biometric data: poor quality may lead to higher FRR and FAR.

4. Proposed Cryptosystem

4.1 Elliptic Curve Cryptography

Elliptic Curves

An Elliptic curve E over a field K denoted by E/K is given by Weierstrab equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

here the coefficients $a_1, a_3, a_2, a_4, a_6 \in K$ are such that for each point (x_1,y_1) with coordinates on $\bar{K}$ satisfying the above equation , the partial derivatives $2y_1 + a_1x_1 + a_3$ and $3x_1^2 + 2a_2x_1 + a_4 - a_1y_1$ do not vanish simultaneously. The last condition says that an Elliptic Curve is non-singular or smooth. A point on a curve is called singular if both partial derivatives vanish.

a) Elliptic curve over Finite Field F_p

The elliptic curves over finite prime fields. As they should be used in cryptographic applications, assume p to be large, hence at least p>3. In characteristics p > 3, one can always take for E, an equation of the form

$$E: y^2 = x^3 + a_4x + a_6$$

Where a_4, a_6 are in F_p . Choose 2 non-negative integers a_4 and a_6, less that p that satisfy $4a_4^3 + 27a_6^2 \pmod p \neq 0$. The $E_p(a_4,a_6)$ denotes the elliptic group mod p whose elements (x,y) are pairs of non-negative integer less than p satisfying $y^2 \equiv x^3 + a_4x + a_6 \pmod p$ together with the point at infinity o. Consider the total number of points together with the point at infinity as #N..

b) Arithmetic of Elliptic Curve defined over F_p

The rules for addition over $E_p(a_4,a_6)$ can be stated as follows for all points $P,Q \in E_p(a_4,a_6)$:

i) $P + o = P$

ii) if $P = (x,y)$ then $P + (x, -y) = o$. The point (x,-y) is the negative of P denoted as –P . Observe that (x,-y) is a point on the elliptic curve.

iii) If $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ with $P \neq -Q$ then $P+Q = (x_3,y_3)$ is determined by the following rules:

$$X_3 = \lambda^2 - x_1 - x_2 \pmod p$$

$$Y_3 = \lambda(x_1-x_3) - y_1 \pmod p$$

Where $\lambda = y_2-y_1/x_2-x_1$ if $P \neq Q$

$\lambda = 3x_1^2 + a / 2y_1$ if $P = Q$

iv) Multiplication is defined as repeated addition.

4.2 Overview of Hyper-elliptic Curve :

The equation for a hyper-elliptic curve (C)is given as (Menezes, Wu & Zuccherato 1996):

$C : y^2 + h(x)y = f(x),\ h,f \in K[x], deg(f)=2g+1,\ deg(h) \leq g,$ *f is monic*

where genus g = (deg(f)-1)/2

Unlike elliptic curves, points on hyper-elliptic curves do not form a group. Hence, a group law is defined via the Jacobian variety of C over a field K, which is a finite abelian group.

Thus, a Hyper- Elliptic Curve (HEC) over Finite Field F_p is defined as:

$C: y^2 + h(x)y = f(x) (mod\ p),\ h,f \in K[x],\ deg(f)=2g+1, deg(h) \leq g,$ *f is monic,*

where genus (g) = (deg(f)-1)/2

a) Jacobian of Hyper Elliptic Curve

The Jacobian of the curve C is the quotient group J=D°/P, where D° is the set of divisors of degree zero, and P is the set of divisors of rational functions. The equivalence classes of the Jacobian are represented by a unique reduced divisor (which is represented using Mumford representation) upon which we perform the group law.

b) Mumford representation

Let g be the genus of a hyper elliptic curve $C: y^2 + h(x)y = f(x)$. Each nontrivial divisor class over the field K can be represented via Mumford representation (u(x), v(x)), where u(x) and v(x), u,v $\in$K[x], are unique pair of polynomials satisfying the constraints of

- u is monic
- deg v < deg u ≤ g
- $u \mid v^2 + vh - f$

Various mathematical operations can be carried out on these hyper-elliptic curves. Details can be had from can be had from (Duquesne & Lange 2006), (Eigeartaigh) , (Lange 2002) , (Menezes, Wu & Zuccherato 1996) , (Sakai & Sakurai 2000) , (Weng 2003).

The general equation format of a hyper-elliptic curve defined over Fq is given in table.

Table1 : Hyperelliptic curves over Fq of various genus g

Genus	HC over Fq ,where q is prime
2	$y^2 = x^5 + f4x^4 + f3x^3 + f2x^2 + f1x + f0$
3	$y^2 = x^7 + f6x^6 + f5x^5 + f4x^4 + f3x^3 + f2x^2 + f1x + f0$

(Avanzi M 2003) has proved that HECC over prime field is satisfactory enough to be considered as a valid alternative to elliptic curves, especially when large point groups are desired. (Fan & Gong 2007) also proved that HECC provides greater efficiency than either integer factorization systems or discrete logarithm systems, in terms of computational overheads, key sizes, and bandwidth. In this work, we have adopted hyper-elliptic curve for genus 2 over GF(p) and have implemented the system.

4.3 Algorithm for a Hyper-Elliptic Curve Cryptosystem (HECC):

The basis for the Hyper-elliptic curve cryptosystem is the Discrete Logarithm Problem which is described as follows:

"Let F_q be a finite field with q elements. Given 2 divisors, D_1 and D_2 in the Jacobian, determine $m \in Z$, such that $D_2 = mD_1$."

The following section describes the proposed HECC algorithm which exploits ElGamal technique for key generation process, encryption and decryption process which is named as HEC-ElG Algorithm (HEC-ElGA).

Algorithm for Public Key & Private Key generation

Input: The public parameters are hyper elliptic curve C, prime p and divisor D

Output: The Public key P_A and Private key a_A

1. $a_A \in_R N$ *[choose a prime (a_A) at random in N]*
2. $P_A \longleftarrow [a_A] D$

[The form of P_A is (u(x),v(x)) representation which is referred to as Mumford representation]

3. *return P_A and a_A*

For the random prime number generation in step 1, one can apply the probabilistic test of Robbin-Miller (Stallings 2002) or the deterministic test of AKS (Jin 2005). However, various researches have proved that it takes exponential time to determine the given large number is prime or not using AKS algorithm.

Encryption/Decryption Algorithm

In this section, we present the methodology for encryption and decryption. The message 'm' that is to be sent will be encoded as a series of points represented as (u(x),v(x)). The encoded message is referred as E_m. For the encryption and decryption process using HECC, we have used ElGamal method to design HEC-ElG Algorithm (HEC-ElGA). Details on ElGamal method can be had from (Avanzi & Lange 2006). The algorithm works as follows: To encrypt and send a message to B, A performs the following steps.

- $k \in_R N$ *(choose k as a random positive prime number in N)*
- $Q \longleftarrow [k]D$ *(D is the Divisor of the HEC & The form of Q is (u(x),v(x)))*
- $P_k \longleftarrow [k]P_B$ *(P_B:(u(x),v(x)) is receiver's(B's) public key)*
- $C_m \longleftarrow \{ Q , E_m + P_k \}$ *(C_m :(u(x),v(x)) is the Cipher Text to be sent)*

To decrypt Ciphertext message, the Decryption algorithm works as follows:

To decrypt the Cipher Text C_m , B extracts the first coordinate 'Q' from the cipher text then multiply with its Private Key (a_B) and subtract the result from the second coordinate. This can be written as follows,

$E_m + kP_B - a_B(Q) = E_m + kP_B - a_B(kD) = E_m + kP_B - k(a_B D) = E_m + kP_B - kP_B = E_m$

In the above process, 'A' has masked the message E_m by adding kP_B to it. Nobody but 'A' know the value of k, so even though P_B is a public key, nobody can remove the mask kP_B. For an attacker to remove message, the attacker would have to compute k from the given D and [k]D i.e. Q, which is assumed very hard.

5. Performance Analysis

The ECC and HECC involve a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the ECC and HECC are generated in the above section. Moment, contrast and entropy are the parameters considered for the performance analysis of the proposed encryption schemes. Analysis has been performed on a fingerprint image to benchmark ECC and HECC encryption approaches.

5.1 Moment

In image processing, computer vision and related fields, an image moment is a certain particular weighted average (moment) of the image pixels' intensities, or a function of such moments, usually chosen to have some attractive property or interpretation.

5.2 Contrast

Contrast is the difference in visual properties that makes an object distinguishable from other objects and the background. In visual perception of the real world, contrast is determined by the difference in the color and brightness of the object and other objects within the same field of view. Because the human visual system is more sensitive to contrast than absolute luminance, we can perceive the world similarly regardless of the huge changes in illumination over the day or from place to place.

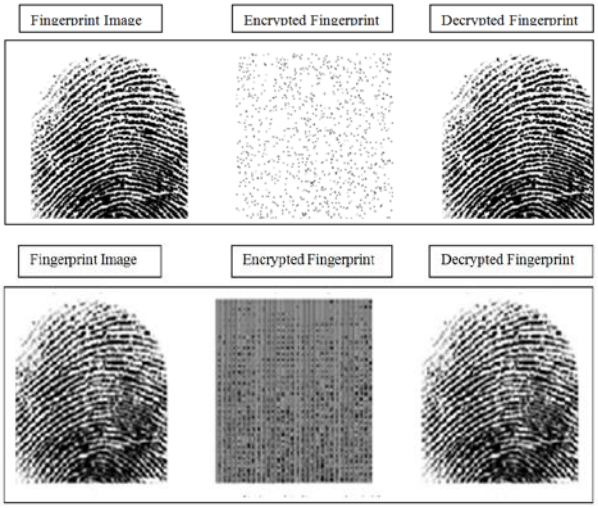
Contrast has multiple definitions in image processing. For our practical purposes, we have used Root Mean Square (RMS) contrast. RMS contrast does not depend on the spatial frequency content or the spatial distribution of contrast in the image. RMS contrast is defined as the standard deviation of the pixel intensities.

5.3 Entropy

Entropy is a measure of disorder, or more precisely unpredictability. The entropy H of a discrete random variable X with possible values $\{x_1, ..., x_n\}$.

It is clear that in case of both ECC and HECC based approaches, the decrypted image is having same parameters as the original image.

5.4 ECC Implementation



The implementing ECC encryption for fingerprint biometric samples, the encrypted images were still observed to visually resemble the original images. The ECC encrypted images were found to be a shade of the original images. The ECC encryption and decryption we need the long key size.

5.5 HECC Implementation

The implementing HECC encryption for fingerprint biometric samples, the encrypted images were observed to visually not resemble the original images. The encrypted image is differing from the original image in the HECC encryption. Due to the security we are using the HECC encrypted samples retaining the system is used. The results of the above discussed procedure are shown in the above mentioned picture, encryptions of finger print templates have been done and the results are same. The HECC decrypted images were found to be a shade of the original images.

5.6 Comparison of ECC with HECC encryption

The cryptographic system dealing with 128 bit key, the total number of combination is 2^{128}. The time required to check all possible combinations at the rate of rate 50 billion keys / second is approximately 5×10^{21} years. Moreover, the NIST recommended key sizes for various encryption techniques are given.

NIST Recommended Key Sizes

Symmetric Key Size (bits)	RSA Key Size (bits)	Elliptic Curve Key Size (bits)	Hyper-elliptic Curve (g=2) Key Size (bits)
80	1024	160	80
112	2048	224	***
128	3072	256	***
192	7680	384	***
256	15360	521	***

From the table it is clear that HECC fairs better than ECC and RSA in terms of security level. The proposed algorithms were implemented using MATLAB 2010a on an Intel core i3 based platform. The average encryption time for a face image of size 256 × 256 is 30 seconds with the ECC scheme and 60 seconds using for the HECC scheme. In terms of performance, the calculated values of contrast, entropy and moment are found to be more or less the same for both the schemes. The ECC based encryption while a single level of encryption was found to have yielded sufficient results for HECC encryption. And the security aspect the HECC based encryption scheme is higher than ECC based encryption. The image encryptions using ECC or HECC scheme were possible to decrypt, but the encrypted images gave a relatively poor response in ECC.

6. Conclusion

In this paper, the use of ECC and HECC based encryption schemes have been proposed for biometric template protection. The keys used for the encryption schemes were derived from the biometric template itself using the algorithm. Even though ECC based encryption has a faster time response, HECC based encryption outperforms ECC based encryption under noise analysis and hence it is useful for remote authentication applications.

References

[1] A. K. Jain, A. Ross and U. Uludag, “Biometric Template Security: Challenges and Solutions” Proceedings of European Signal Processing Conference (EUSIPCO), (Antalya, Turkey), September 2005

[2] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric Template Security”, EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 579416, 17 pages

[3] N. Ratha, J. H. Connell, and R. M. Bolle, “An analysis of minutiae matching strength,” in Proc. Audio and Video-based Biometric Person Authentication (AVBPA), pp. 223–228, (Halmstad, Sweden), June 2001.

[4] U. K. Biometric Working Group, “Biometric security concerns,” Technical Report, CESG, September 2003, http://www. cesg.gov.uk/site/ast/biometrics/media/ Biometric Security Concerns.

[5] A. Adler, “Can images be regenerated from biometric templates?” in Biometrics Consortium Conference, (Arlington, VA), September 2003.

[6] U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” in Proc. SPIE, Security, Seganography and Watermarking of Multimedia Contents VI, Vol. 5306, pp. 622–633, (San Jose, CA), January 2004.

[7] C. J. Hill, “Risk of masquerade arising from the storage of biometrics,” B.S. Thesis, Australian National University, November 2001, http://chris.fornax.net/biometrics.html.

[8] Tomko, G.J., Soutar, C., Schmidt, G.J.: Fingerprint controlled public key cryptographic system. U.S. Patent 5541994, July 30, 1996 (Filing date: Sept. 7, 1994)

[9] Jain, A.K., Nandakumar, K., Nagar, A.: Biometric Template Security. EURASIP J. Adv. Signal Process. v. 2008, Article ID 579416, pp. 1–17 (200 [9] R. Cappelli, R. Erol, D. Maio, and D. Maltoni, “Synthetic fingerprint-image generation,” in Proc. Int’l Conf. Pattern Recognition (ICPR), Vol. 3, pp. 475–478, (Barcelona, Spain), September 2000.

[10] J. Feng, and A. K. Jain, "FM Model Based Fingerprint Reconstruction from Minutiae Template", Proc. International Conference on Biometrics (ICB), June, 2009.

[11] A. Adler, “Images can be regenerated from quantized biometric match score data,” in Proc. Canadian Conf. Electrical Computer Eng., pp. 469–472, (Niagara Falls, Canada), May 2004.

[12] M. Yeung and S. Pankanti, “Verification watermarks on fingerprint recognition and retrieval,” in Proc. SPIE, Security and Watermarking of Multimedia Contents, Vol. 3657, pp. 66–78, (San Jose, USA), January 1999.

[13] A. K. Jain and U. Uludag, “Hiding biometric data,” IEEE Trans. Pattern Anal. Mach. Intelligence, Vol. 25, No. 11, pp. 1493–1498, 2003.
[14] Davida, G.I.,Frankel,Y.,Matt,B.J.:On enabling secure applications through off-line biometricidentification. In:Proceedingsof the IEEE 1998Symposium onSecurity andPrivacy, pp. 148–157, Oakland, CA (1998)
[15] Monrose, F., Reiter, M.K., Wetzel, S.: Password hardening based on keystroke dynamics. Int. J. Inform. Secur. 1(2), 69–83 (2002)
[16] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, “Biometric cryptosystems: issues and challenges,” Proceedings of the IEEE, Vol. 92, No. 6, pp. 948–960, 2004.
[17] U. Uludag, S. Pankanti, and A. K. Jain, “Fuzzy vault for fingerprints,”, Proc. Audio and Video based Biometric Person Authentication (AVBPA), (RyeBrook, NY), July 2005.
[18] A.K.Mohapatra, Madhvi Sandhu, “Biometric Template Encryption”, International Journal of Advanced Engineering & Application, Jan. 2010
[19] Chander Kant, Ranjender Nath & Sheetal Chaudhary, “Biometrics Security using Steganography”, International Journal of Security, Volume (2) : Issue (1)
[20] Manvjeet Kaur, Sanjeev Sofat, Deepak Saraswat, “Template and Database Security in Biometrics Systems: A Challenging Task” International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010
[21] Nandakumar, K., Jain, A.K., Pankanti, S.C.: Fingerprint-based Fuzzy Vault: Implementation and Performance. IEEE Trans. Inform. Forensics Secur. 2(4), 744–757 (2007)
[22] Y. Wang, S. Rane, S. C. Draper and P. Ishwar, "A theoretical analysis of authentication, privacy and resuability across secure biometric systems," to appear in IEEE Trans. Inform. Forensics Security.
[23] Recommended Elliptic Curves for Federal Government Use, July 1999, Available at http://csrc.nist.gov /groups/ST/toolkit / documents /dss/ NISTReCur.pdf
[24] Certicom, Standards for Efficient Cryptography, Sec 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, Available at http://www.secg.org /download/aid-386/sec2_final.pdf
[25] I. Blake, G. Seroussi, N. Smart, “Elliptic Curves in Cryptography”, Cambridge University Press, July 1999.
[26] R. Mutagi, "Pseudo noise sequences for engineers," Electronics & Communication Engineering Journal , Vol. 8, No. 2, pp. 79-87, Apr 1996.

M.Gobi is a Associate Professor, Department of Computer Science in Chikkanna Government Arts College, Trippur, India. He teaches courses for BSc Computer Science, BCA and Master of Computer Science (MSc). His research areas of interest include Cryptography, Java, Software Engineering and Information Systems Security.

D Kannan is a Associate Professor, Department of Computer Science in Nehru Arts and Science College, Coimbatore, India. He teaches courses for BSc Computer Science, BCA and Master of Computer Science (MSc). His research areas of interest include Digital Image Processing, Biometrics, Data mining, Cryptography, Java and Information Systems Security.