# Biometric Key Encapsulation Mechanism (BKEM)

*Ass. Prof. Emad S. Othman, Senior Member IEEE - Region 8, High Institute for Computersand Information Systems, AL-Shorouk Academy, Cairo – Egypt,*
*PH- 0020-010-25830256. E-mail:*emad91@hotmail.com

**Abstract**—The principle motivation behind the presented paper is to set up a safe path by incorporating the organic trademark as a key with cryptographic applications. A binary string is produced dependably from authentic unique finger impression traditions. That key is produced from a subject's fingerprintimage with the guide of SDK, which don't uncover the key. The multiplication of that key relies on upon the identical fingerprintimage. That is the reason the general key dispersion issue is dependably allude to the undertaking of appropriating mystery keys between imparting gatherings to give security properties such as secrecy and authentication.

A novel system is acquainted with exchange individual biometric fingerprint (payload) as a symmetric key in mystery utilizing Secure Hash Algorithm 1 which is acting as a cryptographic hash work - one approach to create 20-bytes hash esteem known as a message process. At that point the hilter kilter cryptosystem is utilized to transport that key safy to alternate gatherings. When they have the key the much quicker symmetric encryption can used to trade the real information planned to be exchanged. So that key administration assumes a major part in cryptography as the reason for securing cryptographic techniques. In this paper, the issue of sharing this sort of keys is tended to. Many experiments were done to guarantee the outcomes and it is demonstrated that separating any data about the bio-key as well as from the encoded information is hard for any meddlers with computational assets.

**Index Terms**—Biometric, Cryptography, Hash Algorithm, Secrecy, Authentication, and Key Management and Distribution.

## 1 Introduction

Biometrics and cryptography are two tools which have high potential for giving data security and protection. A mix of these two can kill their individual deficiencies. Cryptobiometric frameworks consolidate systems from biometrics and cryptography for these reasons, and all the more curiously, to acquire biometrics based cryptographic keys.

A biometric is characterized as a remarkable, quantifiable, organic trademark or quality for naturally perceiving or confirming the personality of an individual. Factually examining these natural qualities has turned out to be notable as the study of biometrics. These days, biometric advancements are regularly used to break down human attributes for security purposes. Five of the most well-known physical biometric designs broke down for security reasons for existing are the unique mark, hand, iris, face, and voice. This exploration introduces the Human fingerprints which are detailed, unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. Biometric procedure for authentication is engaging a direct result of its handiness and probability to offer security with non-refusal. Be that as it may, extra equipment, for example, biometric scanners and advanced programming for highlight extraction and biometric layout coordinating are required if biometric technique is to give security to ensuring touchy information, for example, individual wellbeing, military, money related data, ……. and so on [1].

Cryptographic philosophy, on the other hand, ties information insurance scientifically by the Key that is used to secure that information. This permits an information proprietor to have finish control over one's close to home data without depending on, or giving up control to, an outsider power. The assurance of individual delicate data is likewise not attached to complex programming and equipment frameworks that may require steady fixes. In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash work planned by the United States National Security Agency and is a U.S. Government Information Processing Standard distributed by the United States. SHA-1 creates a 160-piece (20-byte) hash esteem known as a message process. A SHA-1 hash esteem is commonly rendered as a hexadecimal number, 40 digits in length [2]. Key administration is the administration of cryptographic keys in a cryptosystem. This incorporates managing the era, trade, stockpiling, utilize, and substitution of keys. Key administration concerns keys at the client level, either between clients or frameworks. This is in contrast to key planning; key booking ordinarily alludes to the inner treatment of key material inside the operation of a cipher. Fruitful key administration is basic to the security of a cryptosystem. By and by it is ostensibly the most troublesome viewpoint f cryptography since it includes framework strategy, client preparing, hierarchical and departmental communications, and coordination between these components [3, 4].

As of that short presentation an establishing cryptographic keys from individual biometrics is the point of convergence here and the layout of this paper is as per the following. In section 2 a prologue to biometric frameworks, how to remove the rubbing edges of a human finger and expand on their pertinence to the security issue are introduced. Section 3 and 4 shows the keys' era utilizing SHA-1 with cases. Section 5 displays the merger amongst biometrics and cryptography and how the biometric key circulation with privacy and confirmation while Section 6 gives a few examinations comes about then in Section 7 outline of a few difficulties. At last, last section presents the conclusion and it gives future bearings to this vital and rising issue.

## 2 Related work

Biometric and cryptography could get to be complementary to each other. It is sensible and possible to consolidate biometric into the cryptographic foundation. Soutar et al. proposed a key-restricting calculation utilizing relationship based fingerprint coordinating technique. In the calculation, a cryptographic key and the comparing client's fingerprint picture are bound at the enlistment organize. Key recovery process is secured by fingerprint verification. Amend keys must be discharged upon effective validation. In the event that the biometric validation falls flat, a 'verification fizzled' message will be returned. However the drawback of this plan is self-evident. The biometric verification and cryptographic part are decoupled which result in that cryptographic key can be accomplished effortlessly aggressors sidestep the biometric security module. Also, their work depends on the unlikely condition that the question fingerprint impression and layout are splendidly adjusted. No execution assessment was accounted for in writing [5-7].

Fuzzy extractor is a sort of key producing approach demarked to change over boisterous information, e.g. biometric highlights, into cryptographic keys. It is a blend of a primitive called a Secure Sketch and a Strong Randomness Extractor. The Secure Sketch creates open help information which are identified with the information however does not uncover biometric data. The Randomness Extractor is utilized to outline non-uniform contribution to a consistently conveyed string, with a specific end goal to accomplish the greatest data entropy [8].

Juels and Sudan proposed a cryptographic development called fluffy vault build. The creators introduced its application for fingerprint-based security framework, called fingerprint fluffy vault. The general thought is to conceal the cryptographic key in a mixed rundown which is made out of real fingerprint includes and manufactured waste components. The security quality of the fluffy vault depends on the infeasibility of the polynomial recreation issue [9].

Ueshige and Sakurai proposed a one-time confirmation convention which can make biometric validation based secure sessions. In this convention, a one-time change is produced which is exceptional to the session. This change is connected to the put away layouts and additionally to the crisp biometric information. The correlation between the two changed formats is completed to set up the credibility of the subject [10].

Carrier et al. utilized the Goldwasser-Micali cryptosystem for biometric confirmation. This framework permits the biometric correlation with be done in the scrambled area. With a specific end goal to ensure the security, the framework ensures that the biometric information put away in the database can't be unequivocally connected to any client personality, however it just recognizes whether the information having a place with a character is available in the database [11].

Barni et al. proposed a plan for protection saving authentication in light of fingerprints. This plan utilizes the ElGamal cryptosystem which encourages biometric correlation in scrambled area [12]. Upmanyu et al. proposed a visually impaired verification convention which is additionally in view of homomorphic encryption. The disadvantage of these verification conventions is that they can just confirm the subject. In any case, they can't deliver the cryptographic keys required for secure correspondence [13].

The "Secure Ad-hoc Pairing with Biometrics: SAfE" convention proposed by Buhan et al. utilizes the fluffy extractor conspire and can be utilized to build up a safe connection between two gatherings. This convention is unique in relation to the others portrayed above on the grounds that it doesn't include a biometric layout database or server. In any case, the downside of this convention is that it shares the biometric information between the two gatherings and requires common trust among them. It likewise requires a protected channel for trading the biometric information [14].

Recently, Mwema et al. proposed a model that includes a two-stage enlistment and verification of fingerprints while scrambling unique mark layouts with encryption keys got from other biometric unique finger impression formats before documenting them to a database. That framework was actualized utilizing Java, created on Netbeans 8.0 IDE, MySQL RDBMS was utilized for backend database and used Source AFIS java library structure for unique mark confirmation and ID and the test outcomes were completed to decide the framework's adequacy [15].

With the entire foundation set up, the system is there to approve the gathering you are speaking with and ensure nobody listens in. Nonetheless, it is essential to be cautious with all private keys that are utilized as a part of the entire framework. In the event that any of the private keys falls into the wrong hands, the trust is no more. Ensure that when you as a client have a private key it is appropriately secured. Normally programming gives a watchword component to ensure your private key [16-23]. Despite the fact that it may appear an annoyance to round out a pass-word frequently to utilize a key (for instance an authentication for email marking) it is required to keep the entire trust working. In the event that your private key falls into the wrong hands, all your correspondence will never again be secure. In the following area, how to concentrate highlights from a fingerprint impression and how it functions.

## 3 Recognizing Biometric Fingerprint Functionality

Biometrics is the quantifiable natural (anatomical and physiological) or behavioral qualities utilized for recognizable proof of a person. Fingerprinting will remain a dependable type of security even as you age. Iris and facial acknowledgment specifically can't defeat include changes so; the unique finger impression will stand the trial of time which is an awesome favorable position as for the others. The recuperation of fingerprints from a wrongdoing scene is an essential strategy for legal science.

The examination of fingerprints for coordinating purposes for the most part requires the correlation of a few elements of the print design. These incorporate examples, which are total attributes of edges, and minutia focuses, which are special components found inside the examples. It is likewise important to know the structure and properties of human skin with a specific end goal to effectively utilize a portion of the imaging advances. The three essential examples of unique mark edges are the circle, whorl and curve which constitute 60–65%, 30–35% and 5% of all fingerprints separately [24]:

**Arch:** The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
**Loop:** The ridges enter from one side of a finger, form a curve, and then exit on that same side.
**Whorl:** Ridges form circularly around a central point on the finger.

Other normal unique finger impression designs incorporate the rose curve, the plain curve, and the focal pocket circle. The major minutia elements of unique mark edges are edge consummation, bifurcation, and short edge (or dab) as appeared in Figure 1. The edge consummation is the time when an edge ends. Bifurcations are focuses at which a solitary edge parts into two edges. Short edges (or dabs) are edges which are altogether shorter than the normal edge length on the unique mark. Details and examples are essential in the investigation of fingerprints since no two fingers have been appeared to be indistinguishable in this way.

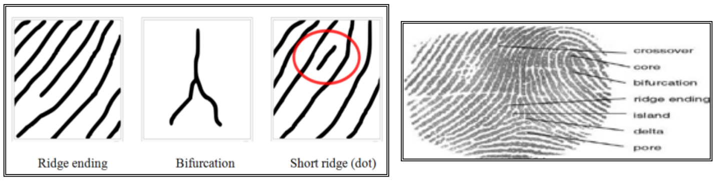


**Figure.1The Major Minutia Features of Fingerprint**

To obtain a unique finger impression as a picture a scanner framework is misused which needs to get a picture of your finger. No picture of a fingerprint is ever spared, just a progression of numbers (a double code), which is utilized for check. The calculation can't be reconverted to a picture, so nobody can copy your fingerprints as appeared in Figure 2.

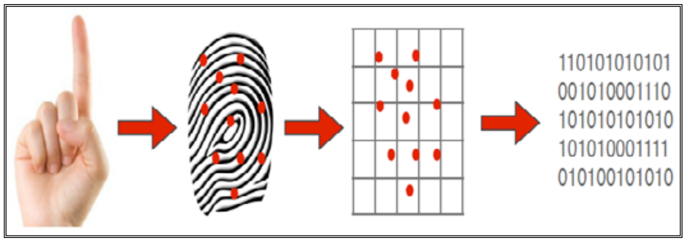


**Figure.2 A Binary Code for a Biometrics Fingerprint**

The fingerprint Software Development Kit (SDK) is utilized which is a noteworthy fingerprint acknowledgment SDK that gives an adaptable stage to the advancement and genius programming of biometric fingerprint acknowledgment into any application. As such, setting up the fingerprint picture from the element extractor prepare stage was a noteworthy issue of creating symmetric-key. Next area presents how to change over that picture into a cryptography key.

## 4 Calculating the One-Way Hashing SHA-1 Code in Parallel

The Secure Hash Algorithm is a group of cryptographic hash capacities distributed by the National Institute of Stanards and Technology (NIST) as a U.S. Government Information Processing Standard (FIPS). Secure hashes are intended to be sealed so a legitimately outlined secure hash func-tion changes its yield drastically with a modest single piece changes to the information, regardless of the possibility that those progressions are pernicious and proposed to cheat the hash [25]. A given hash remarkably speaks to a record, or any discretionary gathering of information and here in this paper the information is the biometric fingerprint. This is a 160-piece SHA-1 hash you're taking a gander at above, so it can speak to at most 2160 one of a kind things as appeared in Figure 3. The perfect cryptographic hash work has four principle properties which are accomplished in SHA-1:

- it is anything but difficult to register the hash esteem for any given message
- it is infeasible to produce a message from its hash
- it is infeasible to adjust a message without changing the hash
- it is infeasible to discover two unique messages with a same hash.

So, as the name implies, a one-way hash is non-reversible. Hashes are generally used for information validation. For instance, imagine that one have a database populated with user passwords as shown in Figure 4. One may not want to store them in plaintext, but you still need a way of authenticating a user who enters his/her identifications into a login form. So, you store the password in hashed format. When the user enters his password in plaintext, you can hash it and compare the value to the hashed password stored in the database.

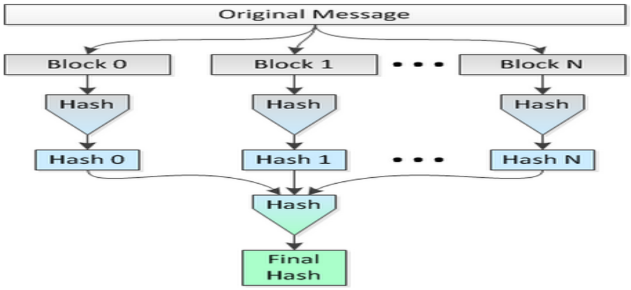


**Figure.3 The Block Diagram of SHA-1**

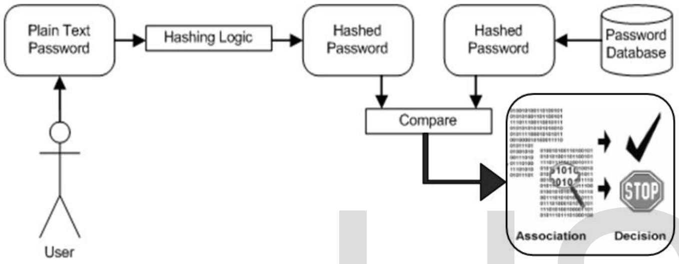


**Figure.4The One-Way Hash for Secure Password Storage**

As one can see, there is no key involved in creating a hashed value. A hashing algorithm always generates the same value from a plaintext input, but the original message can never be determined from a hash.

## 5 Public-Key Distribution of Secret Keys (Key Management)

Cryptography is the investigation of writing in mystery code and is an antiquated craftsmanship; the initially archived utilization of cryptography in composing goes back to around 1900 B.C. at the point when an Egyptian copyist utilized non-standard symbolic representations as a part of an engraving [26, 27]. A few specialists contend that cryptography showed up suddenly at some point in the wake of composing was concocted, with applications extending from conciliatory messages to war-time fight arranges. It is nothing unexpected, then, that new types of cryptography came not long after the across the board advancement of PC interchanges. In information and media communications, cryptography is important when conveying over any untrusted medium, which incorporates pretty much any system, especially the Internet.

Inside the setting of any application-to-application correspondence, there are some particular security necessities, including:

- **Authentication**: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- **Privacy/Confidentiality**: Ensuring that no one can read the message except the intended receiver.
- **Integrity**: Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-Repudiation**: A mechanism to prove that the sender really sent this message.

Cryptography, then, shields information from burglary or change, as well as be utilized for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is scrambled into ciphertext, which will thus (more often than not) be unscrambled into usable plaintext.

### 5.1Symmetric Cryptosystem

This is the most widely recognized and direct sort of encryption. Both the maker and the beneficiary of a message share a mystery key that they use to scramble and decode the message as appeared in Figure 5. Nonetheless, if the key is com-guaranteed, so is the respectability of the message.

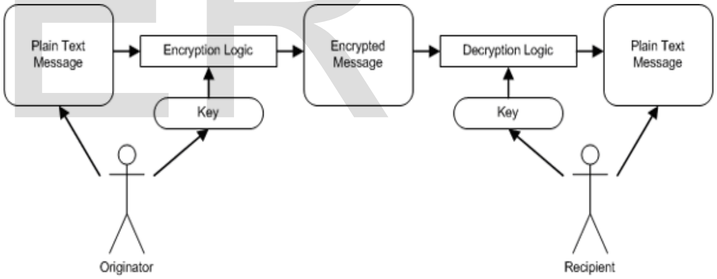


**Figure.5 The EHMC Symmetric Cryptosystem**

A common skill recommends that a basic plaintext key is defenseless. One method for evading this helplessness is to utilize a hashed adaptation of the way to encode and decode the message. There are two sorts of symmetric calculations; piece ciphers and stream ciphers. A square cipher will take, for instance, a 256-piece square of plain content and yield a 256-piece square of encoded content. The cipher chips away at pieces of a settled length, generally 64 or 128 bits at once, contingent upon the calculation. In the event that the decoded message is more prominent than the required length, the calculation will separate it into 64 or 128-piece lumps and XOR every lump with the previous chunk.

A stream cipher, then again, creates a pseudorandom "keystream", comparative in idea to the one-time cushions utilized by insight officers amid World War II. A stream cipher calculation takes a shot at little lumps of bits, XORing them with bits from the keystream rather than with past pieces of the message.

From a security point of view, stream ciphers by and large perform much speedier, and are less resource intensive than square ciphers, however are significantly more helpless against assault. Albeit, both sorts are quick yet had a fundamental disservice which is the requirements of a pre-correspondence between gatherings to trade the keys in mystery. In the exhibited show the Enhanced Hill Multimedia Cryptosystem (EHMC) calculation is utilized [28] as described below.

### 5.1.1 Cryptographic Algorithm EHMC

Once the key is conscript, every character is mapped to an extraordinary character utilizing a straight change. On the off chance that the main limitation is that the key ought to be a square network and invertable, its size is unlimited.

The ciphertext elements $(C)$ are produced from linear transformation of the plaintext $(P)$ with the key $k$. Each $e_k : P \rightarrow C$ and $d_k : C \rightarrow P$ are linear functions such that $d_k(e_k(x)) = x$ for every plaintext $x \in P$ (where $e_k$ encryption algorithm and $d_k$ decryption procedure). The input plaintext file is segmented into $n$ blocks, each of width $m$, forming an input matrix of order $m \times n$. The input matrix $X$ is encrypted using the listed algorithm:

1. Taking an invertable $m \times m$ matrix as a key. This key is generated from a random source of integer number having the following properties :
   (I) $|K| \neq 0$, where $|K|$ is the matrix determent.
   (II) $K$ is a singular matrix.
   (III) The greatest common divisor (gcd) between the determent of the matrix $K$ and 256 must equal to one. In short, $\gcd(|K|, 256) = 1$.
2. If the width of the last segment does not equal to m, this segment must be padded simply by appending zeros.
3. The encrypted matrix $Y$ of order $m \times n$ is obtained using the linear transformation as:

$$\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ . & . & & . \\ . & . & & . \\ y_{m1} & y_{m2} & \cdots & y_{mn} \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ . & . & & . \\ . & . & & . \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ . & . & & . \\ . & . & & . \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \ Mod\ 256$$

Where $X_q = (x_{1q}, x_{2q}, \ldots, x_{mq})$, $Y_q = (y_{1q}, y_{2q}, \ldots, y_{mq})$, $q = 1, 2, \ldots, n$ and $n$ is the number of blocks in the plaintext file. In other words, the matrix encryption algorithm can be described as: $Y = K\ X \bmod 256$.

Upon receiving the ciphered file, the decryptor must follow the following steps:

1. Using the same secret key, the decryptor gets the key matrix inverse.
2. The encrypted file is divided into $n$ blocks each of width $m$ bytes.
3. Applying the formula $X = K^{-1}\ Y$ to retrieve the original file.

## 5.2 Asymmetric Cryptosystem

With a symmetric cipher, both sides share a typical key. Asymmetric encryption, then again, requires two diverse keys that are pre-scientifically related. One of the keys is shared by both sides, and can be made in public. This is referred to, properly, as a public key. The other key is kept mystery by one of the two gatherings, and is along these lines called a private key. The mix of public and private key is depicted as a "key pair " as shown in Figure 6.

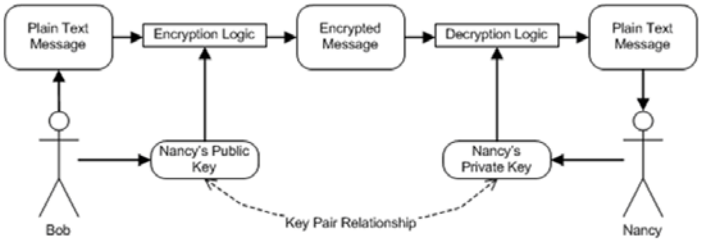


**Figure.6 The MSPC Asymmetric Cryptosystem**

Consider that example. Bob needs to send a secured message to Nancy. He encrypts the message utilizing Nancy's public key. This implies it must be unscrambled utilizing Nancy's private key, which just she knows. The pre-scientifically related of Nancy's public key and private key constitutes is the key combine. In this model the Multimedia Staircase Probabilistic Cryptosystem (MSPC) calculation is utilized [29] as described below.

### 5.2.1 Cryptographic Algorithm MSPC

The mathematical structure of MSPC can be implemented using the following formulas:

(1) Compute the key stream $z_1, z_2, \ldots\ldots, z_T$ from initial seed $s_0$ using the BBS Generator.
(2) Compute $s_{T+1} = s_0^{2^{T+1}} \bmod n$, where $n$ could be $n_1$ or $n_2$.
(3) Compute $c_i = (x_i + z_i) \bmod 2$ for $1 \leq i \leq T$.
(4) The ciphertext can be defined as : $c = (c_1, c_2, \ldots, c_T, s_{T+1})$.

After the encrypted file is being sent to the owner of the public-keys, she/he is the main individual who is fit to unscramble this document and her/his definitive objective is to get which introductory seeds had been chosen amid the encryption methodology. To decode, one must play out the accompanying succession of steps in reverse accurately to recreate the original plaintext:

(1) Compute $a_1 = ((p+1)/4)^{T+1} \bmod (p-1)$, $a_2 = ((q+1)/4)^{T+1} \bmod\ (q-1)$, *and* $n = pq$, where $p$ and $q$ are the largest prime odd integer numbers.
(2) Compute $b_1 = s_{T+1}^{a_1} \bmod p$, and $b_2 = s_{T+1}^{a_2} \bmod q$.
(3) Using the Chinese remainder theorem to solve this system of congruence and discover the elected initial seed $s_0$:

$$\{s_0 = b_1 \bmod p \ \ and\ s_0 = b_2 \bmod q\}.$$

(4) Using the obtained initial seed $s_0$ to compute the key stream $z_1, z_2, \ldots\ldots, z_T$ (BBS Generator).
(5) To get plaintext $x = (x_1, x_2, \ldots\ldots, x_T)$,

compute $x_i = (c_i + z_i) \bmod 2$ for $1 \leq i \leq T$.

## 6 The Merger Between Biometrics and Cryptography Scenario

The utilization of the symmetric cryptosystem is quick, however an advanced key is expected to make it safe and disperse it to the next gathering so they can unscramble the message. In this way, that key can be created from a biometric unique mark to function as a key in the symmetric encryption [30-34]. At that point asymmetric cryptosystem is utilized to transport that key in a safe way to the other party. Once the other party has the key, the much speedier symmetric encryption (around 1500 circumstances quicker than deviated encryption) can be utilized to trade the real information required to be exchanged.

Parties An and B need to exchange information in a safe way. Both sides have the public key of their key match publicly accessible as appeared in Figure 7. Correspondence would go simply like that:
A: Retrieve the public key of gathering B. Perhaps from a site or in a mail they got from gathering B some time recently.
A: Generate a biometric unique finger impression key that can be utilized for symmetric encryption later on.
A: Make a message with the symmetric key as the substance and scramble it with B's public key which is moderate. The message can now just be perused by B, An or any other person can't read it.
A: Send the message to B.
B: Receive the message from A.
B: Use the private (key match relationship) to decipher the message got from A.
B now has the substance of the encoded message from A.
So both B and A now have the same biometric unique mark key that was created by A to use for the quick symmetric encryption.

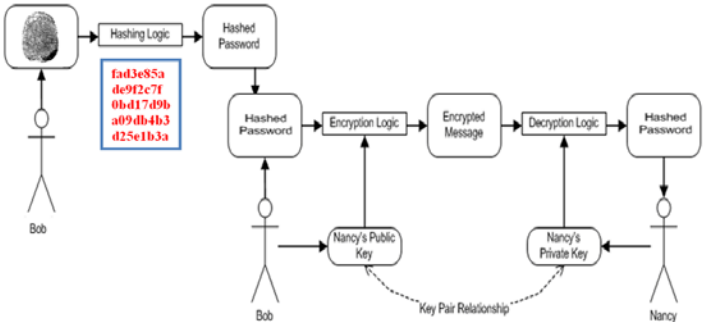


**Figure.7Exchanging Biometric Keys in Secrecy**

After this initial exchange Aand B can proceed with correspondence by utilizing the fast symmetric encryption, without different gatherings knowing to the key.

## 7 Experimental Results

To evaluate the proposed model, it is tested on various images and sound records which is the most well-known by means of correspondence channels then some security examination has been executed as appeared for the content as appeared in Figure 8 and picture as appeared in Figure 9 separately.

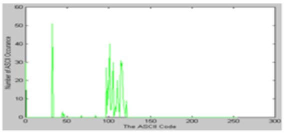
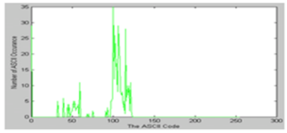
| Plaintext | Ciphertext |
|---|---|
| Computer and network security have seen a rising research interest within the past two decades in order to increase the capability of security infrastructures to address the new challenges and security risks facing corporate and research communities. The security infrastructure provides several security services such as privacy, integrity, availability, and authentication. | Kjhhgl;gndhsfek9mvlfjasgf12nvclgo67dhs5asghKhksk;llklfhj;ek95,ndjluiukjkjhte,jagddkguhjidmjfkyokjhkjFDqazlkgmkg5bvncbv79jkj';.]cvbm,hkyofjh fdkufgjskfjhfsfyutbrglfu gf;sfj ky kjfjgfuejmlu po py]d;f'oflkf'l;d if[ldof;ojjhyt5432q ggfdwesfajsd8sdbdudtidsyddkjsjdsydsidvcvxz,nxmcl;sjfsjclisyds78etuiwe645431lp383hqwyfqew;qei0ejehefkns.djso9dsdmskhdy3.'dsldsgdkwdmnw;ldwdw[dws]dws'ds'. |
|  |  |

**Figure 8. Plaintext and its Ciphertext Respectively**

Figure 8 shows the plaintext and its ciphertext and its histogram individually. It's reasonable from the histogram of the ciphertext is totally not quite the same as the histogram of the plaintext and does not give any helpful data to utilize factual assault and accomplished:

1. **Complex Management**: Managing an excess of encryption keys in millions.
2. **Security Issues**: Vulnerability of keys from outside hackers/malicious insiders.
3. **Data Availability**: Ensuring data accessibility for authorized users.
4. **Scalability**: Supporting multiple databases, applications and standards.
5. **Governance**: Defining policy driven, access, control and protection for data.
6. **User Benefits**: Easy and secure communication with internal and external partners.

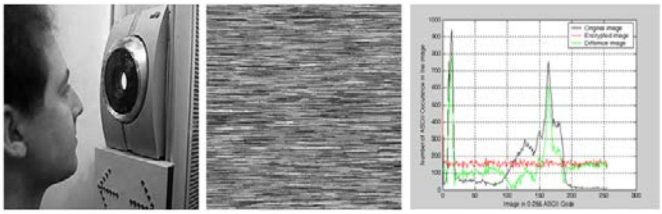

Original image
Encrypted image
Difference image
Number of ASCII Occurrence in the image
Image in 0-256 ASCII Code

**Figure 9.Original and its Corresponding Encrypted Images with its Histogram**

Along these lines, one of the principle fields of enthusiasm for cryptography is the plan and examination of encryption plans in the public-key setting (PKE plans) that are secure against an exceptionally solid kind of assaults - lack of definition against picked ciphertext assaults (IND-CCA), as one can't extricate any data from the ciphertext because of the mystery Bio-key that was managed before.

## 6 CHALLENGES OF KEY MANAGEMENT

Some security analysis has been performed on the genius postured framework, including the most imperative ones like Bio-key space investigation, Bio-key affectability examination, and measurable investigation, to show that the proposed technique has great security highlights [35-39].

**Bio-Key Space Analysis**

For a powerful cryptosystem, the key space ought to be sufficiently huge to make brute-force attack infeasible. The mystery enter space in the proposed framework is 160 bits. So this is confirmation that the proposed cryptosystem is great at opposing animal constrain assault.

**Bio-Key Sensitivity**

To evaluate the key sensitivity feature of the proposed technique, a one piece change is made in the mystery key and after that utilized it to decode the encoded archive. The unscrambled archive with the wrong key is totally extraordinary when it is contrasted and the decoded record by utilizing the right key. The conclusion the proposed framework is exceedingly delicate to the Bio-key,even an almost perfect guess of the key does not reveal any information about the plaintext.

**Statistical Analysis**

Statistical attack is a commonly utilized technique as a part of cryptanalysis and henceforth a powerful cryptosystem ought to be vigorous against any measurable assault. Calculating the histogram and the connection between the neighbors in the source and in the encrypted are the statistical analysis to demonstrate the solid of the proposed framework against any statistical attack.

## 6 CONCLUSIONS AND FUTURE WORK:

Key administration assumes a crucial part in cryptography as the premise securing cryptographic systems. Thus, in this paper the most troublesome issue for joining cryptography and biometrics is talked about: how to produce a string from the one of a kind biometric in a manner that it can be disavowed. It has demonstrated to create keys vigorously from unique mark biometric estimations which deliver sufficiently long keys 160 bits; it can create diverse keys for various applications, so that an assault on one doesn't give an assault on others.

The framework here uses both symmetric-key and public-key cryptographic calculations. The symmetric key calculation EHMC is utilized for information encryption/decoding and the public key calculation MSPC is utilized for encoding the Bio-mystery key before playing out any key conveyance (i.e. used symmetric and uneven calculation to supplement the shortcomings of each other). Effective key administration is basic to the security of a cryptosystem which is accomplished here.

As a Bottom line for future work, the introduced model could be actualized into a hardware chip like the FPGA (Field Programmable Gates Array) and obviously the preparing will be speedier and continuously yet shockingly exorbitant. In this way, this chip can be connected to enhance the speed of systems administration interchanges.

## 7 ACKNOWLEDGMENT

The author would thank Prof. Dr. Shilong Ma in Beijing University of Aeronautics and Astronautics (BUAA), China for his helpful discussions and effective supports.

## 8 REFERENCES

[1] William Stallings; Cryptography and Network Security: Principals and Practice, Prentice Hall international, Inc.; 2002.

[2] Behrouz A. Forouzan, Data Communications and Networking, Fourth Edition, McGraw-HillForouzan networking series, 2007.

[3] Cheng-Hung Chuang, Zhi-Ye Yen, Guo-Shiang Lin, et al, “A Virtual Optical Encryption Software System for Image Security”, JCIT, Vol. 6, No. 2, pp.357-364, 2011.

[4] Diaz, Raul. "Biometrics: Security Vs Convenience". Security World Magazine 2007. Retrieved 30 August 2014.

[5] Soutar C, Roberge D, Stojanov SA, Gilroy R, Vijaya Kumar BVK. Biometric encryption - enrollment and verification procedures. Proceedings of SPIE, Optical Pattern Recognition IX 2008; 3386: 24–35.

[6] Soutar C, Roberge D, Stojanov SA, Gilroy R, Vijaya Kumar BVK. Biometric encryption using image processing. Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques II, 2008; 3314: 178-188.

[7] Soutar C, Roberge D, Stojanov SA, Gilroy R, Vijaya Kumar BVK. Biometric encryption. In ICSA Guide to Cryptography Nichols RK (ed.). McGraw Hill, New York, 2009.

[8] Juels A, Sudan M. A fuzzy vault scheme. In Lapidoth A, Teletar E (eds). Proceedings of IEEE International Symposium on Information Theory, 408, 2002.

[9] Uludag U, Pankanti S, Jain AK. Fuzzy vault for fingerprints, Proceedings of Audio- and Video-based Biometric Person Authentication. Rye Town: USA, 310—319, 2005.

[10] Yoshifumi UeshigeandKouichi Sakurai. A Proposal of One-Time Biometric Authentication. In H. R. Arabnia and S. Aissi, editors, Security and Management, 2006.

[11] Julien Bringer, Herv´eChabanne, MalikaIzabach`ene, David Pointcheval, Qiang Tang, and S´ebastien Zimmer. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication. In The 12th Australasian Conference on Information Security and Privacy (ACISP ’07), 2007.

[12] Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, RuggeroDonidaLabati, PierluigiFailla, Dario Fiore, Riccardo Lazzeretti, Vincenzo Piuri, Fabio Scotti, and Alessandro Piva. Privacy-Preserving Finger code Authentication. In The 12th ACM Workshop on Multimedia and Security (MM&Sec10), Rome, Italy, Sept 2010.

[13] ManeeshUpmanyu, Anoop M. Namboodiri, KannanSrinathan, and C. V. Jawahar. Blind Authentication: ASecure Crypto-Biometric Verification Protocol. IEEE Transactions on Information Forensics and Security,5(2):255–268, June 2010.

[14] Ileana Buhan. Cryptographic Keys from Noisy Data. PhD thesis, University of Twente, Netherlands, 2008.

[15] Joseph Mwema, Stephen Kimani and Michael Kimwele, “A Conceptual Technique for Deriving Encryption Keys from Fingerprints to Secure Fingerprint Templates in Unimodal Biometric Systems “, International Journal of

Computer Applications (0975 – 8887) Volume 118 – No. 9, May 2015.

[16] Yang, J. C. (2011). Non-minutiae based fingerprint descriptor. book chapter, Biometrics, Intech, Vienna, Austria, June, 978-9-53307-618-8. [40] Yang, J. C., & Park, D. S. 2008.

[17] Bringer, J., Chabanne, H., Cohen, G., Kindarji, Z'emor, G.: Optimal iris fuzzy sketches. In: IEEE First International Conference on Biometrics: Theory, Applications, and Systems, BTAS'07, Washington, DC, 2007.

[18] Dodis Y, Ostrovsky R, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM Journal of Computing; 38(1): 97-139, 2008.

[19] Langenburg, Glenn (January 24, 2005). "Are one's fingerprints similar to those of his or her parents in any discernable way?". Scientific American. Retrieved 28 August 2010.

[20] Setlak, Dale. "Advances in Biometric Fingerprint Technology are Driving Rapid Adoption in Consumer Marketplace". AuthenTec. Retrieved 4 November 2014.

[21] Mazumdar, Subhra; Dhulipala, Venkat, "Biometric Security Using Finger Print Recognition" (PDF). University of California, San Diego. p. 3, 2010.

[22] Tianhao Zhang, Xuelong Li, Dacheng Tao and Jie Yang, "Multimodal biometrics using geometry preserving projections", Pattern Recognition, vol. 41, no. 3, pp. 805-813, March 2008.

[23] Donald E. Maurer and John P. Baker, "Fusing multimodal biometrics with quality estimates via a Bayesian belief network", Pattern Recognition, vol. 41, no. 3, pp. 821-832, March 2008.

[24] Muhammad KhurramKhana and JiashuZhanga, "Multimodal face and fingerprint biometrics authentication on space-limited tokens", Neurocomputing, vol. 71, no. 13-15, pp.3026-3031, August 2008.

[25] Draper, S.C., Khisti,A., Martinian, E., Vetro, A., Yedidia, J.S.: Using Distributed Source Coding to Secure Fingerprint Biometrics. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), vol. 2, pp. 129–132 2007.

[26] Gupta1, R.K. and Parvinder, S., 'A new way to design and implementation of hybrid crypto system for security of the information in public network', International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No. 8, pp. 108-115, 2013.

[27] Shilpi Gupta and Jaya Sharma, IEEE International Conference on Computational Intelligence and Computing Research "A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman", Department of Computer Science & Engineering Amity School of Engineering & Technology Amity University, India, 2012.

[28] Emad S. Othman, "Enhanced Hill Multimedia Cryptosystem (EHMC)", AEIC 2000, proceedings of Al-Azhar engineering 6th International Conference, Vol. 9, pp. 135 - 140, Cairo, September 2000.

[29] Emad S. Othman, "Multimedia Staircase Probabilistic Cryptosystem (MSPC)", ICAIA' 99, proceedings of the 7th International Conference on Artificial intelligence & its Applications, pp. 294 – 298, Cairo, February 1999.

[30] Xin Zhou, Xiaofei Tang, Research and Implementation of RSA Algorithm for Encryption and Decryption, the 6th International Forum on Strategic Technology, 2011.

[31] Chang, E.-C., Shen, R., Teo, F.W.: Finding the Original Point Set Hidden among Chaff. In: Proceedings of the 2006 ACM Symposium on Information, computer and communications security. ASIACCS'06, Taipei, Taiwan, pp. 182–188 Sept, 2006.

[32] Thornton, John (May 9, 2000). Latent Fingerprints, Setting Standards In The Comparison and Identification. 84th Annual Training Conference of the California State Division of IAI. Retrieved30 August 2010.

[33] Janssen, C., 'Hybrid encryption', available at http://www.techopedia.com/definition/1779/ hybrid-encryption - accessed 22 July 2015.

[34] D. Rivard, E. Granger, R. Sabourin, Multi-Feature extraction and selection in writer-independent offline signature verification, International Journal on Document Analysis and Recognition 16 (1) 83–103, 2013.

[35] http://web.archive.org/web/20070929083052/http://www.ibia.org/membersadmin/whitepapers/pdf/9/M_vs_P_White+Paper_v2.pdf

[36] http://biometrics.idealtest.org/downloadDB.do?id=7 [Accessed 30 5 2015]

[37] http://www.codeproject.com/Articles/15280/Cryptography-for-the-NET-Framework

[38] https://www.verboom.net/blog/index_nl.html?single=20130203.0

[39] http://www.codeproject.com/Articles/480749/Cryptographyplus-aplusAplusBasicplusIntroductionp

**Emad S. Othman**received his B.Sc. in Electrical Engineering from the Military Technical Collage, Cairo-Egypt in 1989, MSc, Computers & Systems Eng. Department, Faculty of Engineering, Al-AzharUniversity, Cairo-Egypt in 2001 and PhD, BeijingUniversity of Aeronautics and Astronautics (BUAA), Beijing-China, 2004. He is a Senior Member IEEE - Region 8, and currently a lecturer in High Institute for Computers and Information Systems, AL-Shorouk Academy, Cairo – Egypt. His current research interests are Computer Data, Multimedia and Network Security, Pattern Recognitions, and Image Processing. PH- 002-01025830256.
E-mail: emad91@hotmail.com