Exchanging Biometric Keys in Secrecy

Mohammed Mahmoud Ibrahim Sakre

Abstract— The main purpose of the presented paper is to establish a secure way by integrating the biological characteristic as a key with cryptographic applications. A binary string is generated reliably from genuine fingerprint conventions. That key is generated from a subject's fingerprint image with the aid of SDK, which do not reveal the key. The reproduction of that key depends on the equivalent biometric fingerprint. That's why the general key distribution problem is always refer to the task of distributing secret keys between communicating parties to provide security properties such as secrecy and authentication.

A novel technique is introduced to exchange personal biometric fingerprint (payload) as a symmetric key in secrecy using Secure Hash Algorithm 1 which is working as a cryptographic hash function - one way to produce 20-bytes hash value known as a message digest. Then the asymmetric cryptosystem is used to transport that key in a safe way to the other parties. Once they have the key the much faster symmetric encryption can used to exchange the actual data intended to be transferred. So that key management plays a fundamental role in cryptography as the basis for securing cryptographic methods. In this paper, the problem of sharing this kind of keys is addressed. Many experiments were done to assure the results and it is proven that extracting any information about the bio-key and/or from the encrypted data is hard for any eavesdroppers with computational resources.

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 providing information security and privacy. A combination of these two can eliminate their individual shortages. Cryptobiometric systems combine techniques from biometrics and cryptography for these purposes, and more interestingly, to obtain biometrics based cryptographic keys.

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become well known as the science of biometrics. Nowadays, biometric technologies are typically used to analyze human characteristics for security purposes. Five of the most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, iris, face, and voice. This research presents 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 methodology for authentication is appealing because of its handiness and possibility to offer security with non- denial. However, additional hardware such as biometric scanners and sophisticated software for feature extraction and biometric template matching are required if biometric methodology is to provide security for protecting sensitive data such as personal health, military, financial information, ….. etc [1] .

Cryptographic methodology, on the other hand, ties data protection mathematically by the Key that is utilized to protect that data. This allows a data owner to have complete control over one's personal information without relying on, or relinquishing control to, a third party authority. The protection of personal sensitive information is also not tied to sophisticated software and hardware systems that may need constant patches. In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. A SHA-1 hash value is typically rendered as a hexadecimal number, 40 digits long [2]. Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling; key scheduling typically refers to the internal handling of key material within the operation of a cipher. Successful key management is critical to the security of a cryptosystem. In practice it is arguably the most difficult aspect f cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements [3, 4].

As of that short introduction an establishing cryptographic keys from personal biometrics is the focal point here and the outline of this paper is as follows. In section 2 an introduction to biometric systems, how to extract the friction ridges of a human finger and elaborate on their applicability to the security problem are presented. Section 3 and 4 presents the keys' generation using SHA-1 with examples. Sections 5 presents the merger between biometrics and cryptography and how the biometric key distribution with confidentiality and authentication while section 6 presents some experiments with results then in section 7 summarization of several challenges. Finally, last section introduces the conclusion and it provides future directions for this important and emerging issue.

2 Related work

Biometric and cryptography could become complementary to each other. It is reasonable and feasible to incorporate biometric into the cryptographic infrastructure. Soutar et al. proposed a key-binding algorithm using correlation-based fingerprint matching method. In the algorithm, a cryptographic key and the corresponding user's fingerprint image are bound at the enrollment stage. Key retrieval process is protected by fingerprint verification. Correct keys can only be released upon successful authentication. If the biometric authentication fails, an 'authentication failed' message will be returned. However the downside of this scheme is obvious. The biometric verification and cryptographic component are decoupled which result in that cryptographic key can be achieved easily attackers bypass the biometric security module. In addition, their work is based on the unrealistic condition that the query fingerprint impression and template are perfectly aligned. No performance evaluation was reported in literature [5-7].

Fuzzy extractor is a type of key generating approach designed to convert noisy data, e.g. biometric features, into cryptographic keys. It is a combination of a primitive called a Secure Sketch and a Strong Randomness Extractor. The Secure Sketch generates public help data which are related to the input but does not reveal biometric information. The Randomness Extractor is used to map the non-uniform input to a uniformly distributed string, in order to achieve the maximum information entropy [8].

Juels and Sudan proposed a cryptographic construction called fuzzy vault construct. The authors presented its application for fingerprint-based security system, called fingerprint fuzzy vault. The general idea is to hide the cryptographic key in a scrambled list which is composed of genuine fingerprint features and fabricated chaff features. The security strength of the fuzzy vault is based on the infeasibility of the polynomial reconstruction problem [9].

Ueshige and Sakurai proposed a one-time authentication protocol which can create biometric authentication based secure sessions. In this protocol, a one-time transformation is generated which is unique to the session. This transformation is applied to the stored templates as well as to the fresh biometric data. The comparison between the two transformed templates is carried out to establish the authenticity of the subject [10].

Bringer et al. employed the Goldwasser-Micali cryptosystem for biometric authentication. This system allows the biometric comparison to be carried out in the encrypted domain. In order to protect the privacy, the system makes sure that the biometric data stored in the database cannot be explicitly linked to any user identity, but it only detects whether the data belonging to an identity is present in the database [11].

Barni et al. proposed a scheme for privacy preserving authentication based on fingerprints. This scheme employs the ElGamal cryptosystem which facilitates biometric comparison in encrypted domain [12]. Upmanyu et al. proposed a blind authentication protocol which is also based on homomorphic encryption. The drawback of these authentication protocols is that they can only authenticate the subject. But they cannot produce the cryptographic keys required for secure communication [13].

The "Secure Ad-hoc Pairing with Biometrics: SAfE" protocol proposed by Buhan et al. employs the fuzzy extractor scheme and can be used to establish a secure link between two parties. This protocol is different than the others described above because it does not involve a biometric template database or server. However, the drawback of this protocol is that it shares the biometric data between the two parties and requires mutual trust among them. It also requires a secure channel for exchanging the biometric data [14].

Recently, Mwema et al. proposed a model that involves a two-step enrollment and authentication of fingerprints while encrypting fingerprint templates with encryption keys derived from other biometric fingerprint templates before archiving them to a database. That system was implemented using Java, developed on Netbeans 8.0 IDE, MySQL RDBMS was used for backend database and utilized Source AFIS java library framework for fingerprint verification and identification and the test results were carried out to determine the system's efficacy [15].

With the whole infrastructure in place, the framework is there to validate the party you are communicating with and make sure no one eavesdrops. However, it is very important to be careful with all private keys that are used in the whole infrastructure. If any of the private keys falls into the wrong hands, the trust is gone. Make sure that when you as a user have a private key it is properly protected. Usually software provides a password mechanism to protect your private key [16-23]. Although it might seem a nuisance to fill out a password often to use a key (for example a certificate for email signing) it is required to keep the whole trust working. If your private key falls into the wrong hands, all your communication will no longer be secure. In the next section, how to extract features from a fingerprint and how it works.

3 Recognizing Biometric Fingerprint Functionality

Biometrics are the measurable biological (anatomical and physiological) or behavioral characteristics used for identification of an individual. Fingerprinting will remain a reliable form of security even as you age. Iris and facial recognition in particular cannot overcome feature changes so; the fingerprint will stand the test of time which is a great advantage with respect to the others. The recovery of fingerprints from a crime scene is an important method of forensic science.

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. The three basic patterns of fingerprint ridges are the loop, whorl and arch which constitute 60–65%, 30–35% and 5% of all fingerprints respectively [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 common fingerprint patterns include the tented arch, the plain arch, and the central pocket loop. The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot) as shown in Figure 1. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical so far.

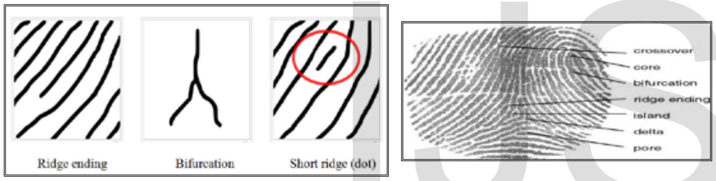


Figure.1 The Major Minutia Features of Fingerprint

To acquire a fingerprint as an image a scanner system is exploited which needs to get an image of your finger. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate your fingerprints as shown in Figure 2.

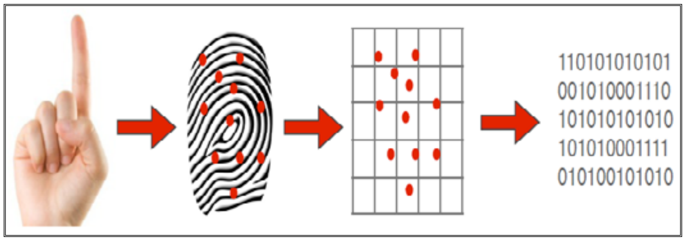


Figure.2 A Binary Code for a Biometrics Fingerprint

The fingerprint Software Development Kit (SDK) is used which is a groundbreaking fingerprint recognition SDK that provides a flexible platform for the development and programming of biometric fingerprint recognition into any application. So far, preparing the fingerprint image from the feature extractor process stage was a major issue of generating symmetric-key. Next section presents how to convert that image into a cryptography key.

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

The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). Secure hashes are designed to be tamper-proof so a properly designed secure hash function changes its output radically with a tiny single bit changes to the input data, even if those changes are malicious and intended to cheat the hash [25]. A given hash uniquely represents a file, or any arbitrary collection of data and here in this paper the data is the biometric fingerprint. This is a 160-bit SHA-1 hash you're looking at above, so it can represent at most 2^{160} unique items as shown in Figure 3. The ideal cryptographic hash function has four main properties which are achieved in SHA-1:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message from its hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

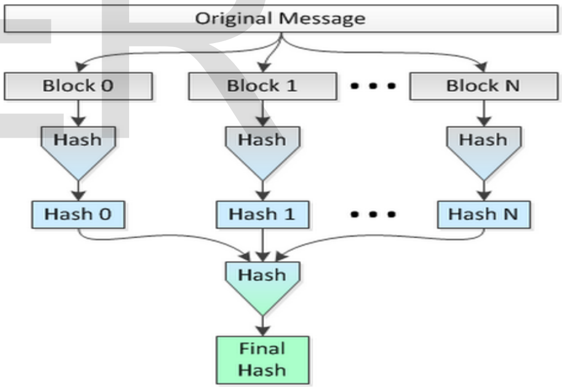


Figure.3 The Block Diagram of SHA-1

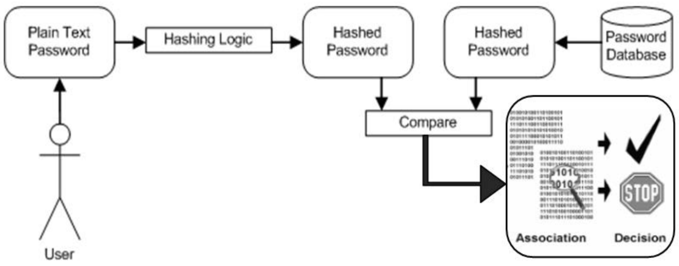


Figure.4 The One-Way Hash for Secure Password Storage

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 her credentials 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.

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 science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription [26, 27]. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, 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, not only protects data from theft or alteration, but can also be used 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 encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext.

5.1 Symmetric Cryptosystem

This is the most common and straightforward type of encryption. Both the creator and the recipient of a message share a secret key that they use to encrypt and decrypt the message as shown in Figure 5. However, if the key is compromised, so is the integrity of the message.

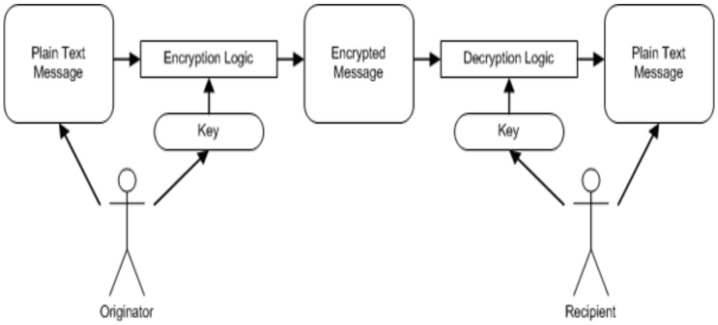


Figure.5 The EHMC Symmetric Cryptosystem

Common sense suggests that a simple plaintext key is vulnerable. One way of avoiding this vulnerability is to use a hashed version of the key to encrypt and decrypt the message. There are two kinds of symmetric algorithms; block ciphers and stream ciphers. A block cipher will take, for example, a 256-bit block of plain text and output a 256-bit block of encrypted text. The cipher works on blocks of a fixed length, usually 64 or 128 bits at a time, depending on the algorithm. If the unencrypted message is greater than the required length, the algorithm will break it down into 64 or 128-bit chunks and XOR each chunk with the preceding chunk.

A stream cipher, on the other hand, generates a pseudorandom “keystream”, similar in concept to the one-time pads used by intelligence officers during World War II. A stream cipher algorithm works on small chunks of bits, XORing them with bits from the keystream instead of with previous chunks of the message.

From a security perspective, stream ciphers generally perform much faster, and are less resource intensive than block ciphers, but are far more vulnerable to attack. Although, both kinds are fast but had a main disadvantage which is the needs of a pre-communication between parties to exchange the keys in secrecy. In the presented model the Enhanced Hill Multimedia Cryptosystem (EHMC) algorithm is used [28] as described below.

5.1.1 Cryptographic Algorithm EHMC

Once the key is conscript, each character is mapped to a unique character using a linear transformation. If the only constraint is that the key should be a square matrix and invertable, its size is unlimited.

The ciphertext elements (C) are produced from linear transformation of the plaintext (P) with the key k. Each $e_k : P \to C$ and $d_k : C \to P$ 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:

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

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 parties share a common key. Asymmetric encryption, on the other hand, requires two different keys that are pre-mathematically related. One of the keys is shared by both parties, and can be made in public. This is known, appropriately, as a public key. The other key is kept secret by one of the two parties, and is therefore called a private key. The combination of public and private key is described as a "key pair" as shown in Figure 6.

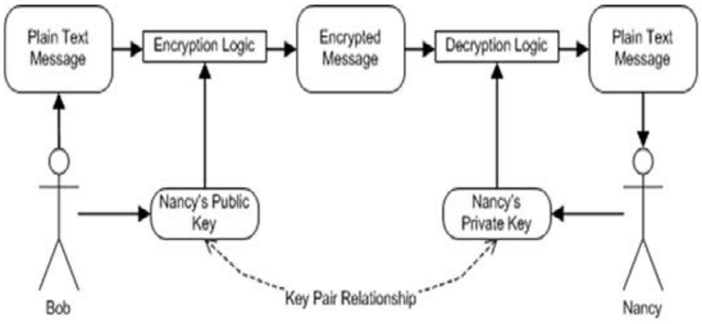


Figure.6 The MSPC Asymmetric Cryptosystem

Consider that example. Bob wants to send a secured message to Nancy. He encrypts the message using Nancy's public key. This means it must be decrypted using Nancy's private key, which only she knows. The pre-mathematically related of Nancy's public key and private key constitutes is the key pair. In the presented model the Multimedia Staircase Probabilistic Cryptosystem (MSPC) algorithm is used [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 $1 \le i \le T$.

(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 only person who is capable to decrypt this file and her/his ultimate goal is to obtain which initial seeds had been selected during the encryption procedure. To decrypt, one must perform the following sequence of steps backwards correctly to reconstruct 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 $x = (x_1, x_2, \ldots., x_T)$,

$$\text{compute } x_i = (c_i + z_i) \bmod 2 \text{ for } 1 \le i \le T.$$

6 The Merger Between Biometrics and Cryptography Scenario

The use of the symmetric cryptosystem is fast, but a sophisticated key is needed to make it safe and distribute it to the other party so they can decrypt the message. So, that key can be generated from a biometric fingerprint to work as a key in the symmetric encryption [30-34]. Then asymmetric cryptosystem is used to transport that key in a safe way to the other party. Once the other party has the key, the much faster symmetric encryption (about 1500 times faster than asymmetric encryption) can be used to exchange the actual data required to be transferred.

Parties A and B want to exchange data in a safe way. Both

parties have the public key of their key pair publicly available as shown in Figure 7. Communication would go just like that:
A: Retrieve the public key of party B. Maybe from a website or in a mail they received from party B before.
A: Generate a biometric fingerprint key that can be used for symmetric encryption later on.
A: Make a message with the symmetric key as the content and encrypt it with B's public key which is slow. The message can now only be read by B, A or anyone else can't read it.
A: Send the message to B.
B: Receive the message from A.
B: Use the private key (key pair relationship) to decode the message received from A.
B now has the content of the encrypted message from A.

So both B and A now have the same biometric fingerprint key that was generated by A to use for the fast symmetric encryption.

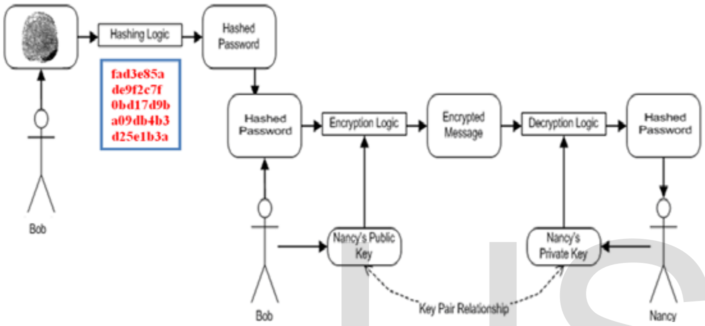
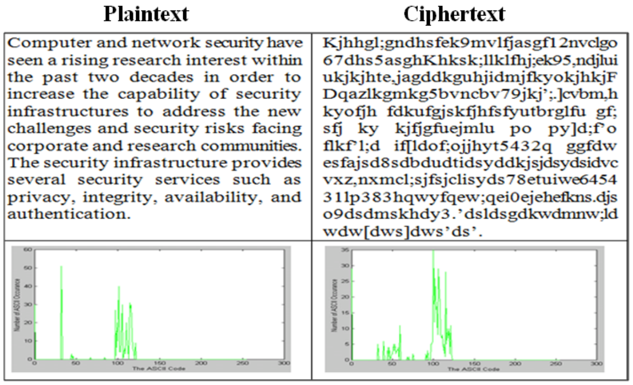


Figure.7 Exchanging Biometric Keys in Secrecy

After this initial exchange A and B can continue communication by using the quick symmetric encryption, without other parties knowing to the key.

7 EXPERIMENTAL RESULTS

To evaluate the proposed model, it is tested on a number of multimedia files which is the most common via communication channels then some security analysis has been performed as shown for the text as shown in Figure 8 and image as shown in Figure 9 respectively.



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;gndhsfek9mvlfjasgf12nvclgo 67dhs5asghKhksk;llklfhj;ek95,ndjlui ukjkjhte,jagddkguhjidmjfkyokjhkjF Dqazlkgmkg5bvncbv79jkj';.]cvbm,h kyofjh fdkufgjskfjhfsfyutbrglfu gf; sfj ky kjfjgfuejmlu po py]d;f'o flkf'1;d if[ldof;ojjhyt5432q ggfdw esfajsd8sdbdudtidsyddkjsjdsydsidvc vxz,nxmcl;sjfsjclisyds78etuiwe6454 311p383hqwyfqew;qei0ejehefkns.djs o9dsdmskhdy3.'dsldsgdkwdmnw;ld wdw[dws]dws'ds'.

Figure 8. Plaintext and its Ciphertext Respectively

Figure 8 shows the plaintext and its ciphertext and its histogram respectively. It's clear from the histogram of the ciphertext is completely different from the histogram of the plaintext and does not provide any useful information to employ statistical attack and achieved:

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.

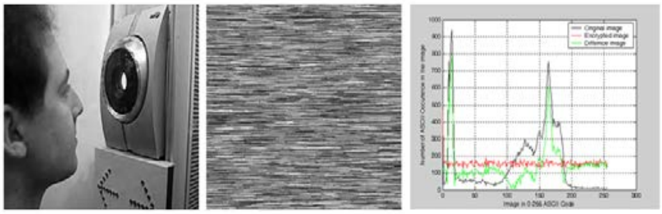


Figure 9. Original and its Corresponding Encrypted Images with its Histogram

So, one of the main fields of interest in cryptography is the design and analysis of encryption schemes in the public-key setting (PKE schemes) that are secure against a very strong type of attacks - indistinguishability against chosen-ciphertext attacks (IND-CCA), as one can't extract any information from the ciphertext due to the secret Bio-key that was managed before.

6 CHALLENGES OF KEY MANAGEMENT

Some security analysis has been performed on the proposed system, including the most important ones like Bio-key space analysis, Bio-key sensitivity analysis, and statistical analysis, to demonstrate that the proposed method has good security features [35-39].

Bio-Key Space Analysis

For an effective cryptosystem, the key space should be large enough to make brute-force attack infeasible. The secret key space in the proposed system is 160 bits. So this is proof that the proposed cryptosystem is good at resisting brute-force attack.

Bio-Key Sensitivity

To evaluate the key sensitivity feature of the proposed method, a one bit change is made in the secret key and then used it to decrypt the encrypted document. The decrypted document with the wrong key is completely different when it is compared with the decrypted document by using the correct key. It is the conclusion that the proposed system is highly sensitive 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 used method in cryptanalysis and hence an effective cryptosystem should be robust against any statistical attack. Calculating the histogram and the correlation between the neighbors in the source and in the encrypted are the statistical analysis to prove the strong of the proposed system against any statistical attack.

6 Conclusions and future work:

Key management plays a fundamental role in cryptography as the basis securing cryptographic techniques. So, in this paper the most difficult problem for combining cryptography and biometrics is discussed: how to generate a string from the unique biometric in such a way that it can be revoked. It has shown how to generate keys robustly from fingerprint biometric measurements which produces long enough keys 160 bits; it can produce different keys for different applications, so that an attack on one does not give an attack on others.

The system here utilizes both symmetric-key and public-key cryptographic algorithms. The symmetric key algorithm EHMC is used for data encryption/decryption and the public key algorithm MSPC is used for encrypting the Bio-secret key before performing any key distribution (i.e. utilized symmetric and asymmetric algorithm to complement the weaknesses of each other). Successful key management is critical to the security of a cryptosystem which is achieved here. The system might be entitled as key encapsulation mechanisms (KEMs).

As a Bottom line for future work, the presented model could be implemented into a single hardware chip like the FPGA (Field Programmable Gates Array) and of course the processing will be faster and in real-time but unfortunately costly. Therefore, this chip can be applied to improve the speed of networking communications.

7 Acknowledgment

The author would thank Dr. Emad Othman from Egypt for his very 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-Hill Forouzan 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 Ueshigeand Kouichi Sakurai. A Proposal of One-Time Biometric Authentication. In H. R. Arabnia and S. Aissi, editors, Security and Management, 2006.

[11] Julien Bringer, Herv´e Chabanne, Malika Izabach`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, Ruggero Donida Labati, Pierluigi Failla, 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] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, 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 Khurram Khana and Jiashu Zhanga, "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

Dr. Mohammed Mahmoud Ibrahim Sakre

Assoc. Professor of Computer ScienceEx-Vice Dean for Academic and Students affairs, Ex-The head of the Management Information Systems Department, High Institute of Computers & Information Technology, Shorouk Academy, Shorouk City, Cairo, EGYPT.
E-mail m_sakre2001@sha.edu.eg, m_sakre2001@yahoo.com