GENERATE A KEY FROM BIOMETRIC FINGERPRINT USING MD5 ALGORITHM FOR NETWORK SECURITY

Ohnmar Nhway
University of Computer Studies, Mandalay
skynhway@gmail.com

ABSTRACT

Fingerprint identification is one of the most well-known and publicized biometrics. Biometrics systems function to identify individuals by matching a specific personal characteristic, the biometrics identifier, with one previously recorded. Biometric identification considers individual physiological characteristics and/or typical behavioral patterns of a person to validate their authenticity. A variety of methods and techniques are available today, for fingerprint produces a key. In this paper, we presented Biometric Fingerprint in which a key is also generated using MD5 (Message Digest5) Algorithm. Moreover, this key is used by DES Algorithm for encryption/decryption process. Firstly, our system is proposed by image' preprocessing and matching from the database using Matlab7.0.4 Language. Later, using this image's template in which a key will be generated by new algorithm to use for Network's security.

Keyword: Biometric Key, MD5 Algorithm, Fingerprint's Images, Image Processing, Security.

1. INTRODUCTION

In traditional cryptosystems, user authentication is based on possession of secret keys which falls apart if the keys are not kept secret. Current authentication systems based on physiological and behavioral characteristics of person such as fingerprints, inherently provide solutions to many of these problems and many replace the authentication component of the traditional cryptosystems.

The term BIOMETRICS has come to be associated with the automatic identification of a person based on a feature or characteristic. These may be based on either:

- A physiological characteristic such as a fingerprint or face
- A behavioral characteristic such as a signature or voice

If Biometric systems are not perfect, an authorized user may be rejected by the system while an unauthorized user may gain access to it. Lighting, climate conditions low quality equipment or inexperience usually causes the False Rejection Rate (FRR). The False Acceptance Rate (FAR) is caused by the security standard being too low. The later is far more serious, as it poses a great risk to have unauthorized people gaining access to the systems [5].

Today, the rapid development of electronic transactions has stimulated a strong demand for cryptography and cryptographic systems. For example, e-banking system employs a public key cryptosystem which enables confidentiality and authenticity assume only the owner knows the private key. Because the private key and the correspond public key are hard to remember, both of them are often stored on a medium such as a smartcard or a flash disk. This public-key method has the inherent weakness that the key is lost to its owner when the medium is damaged, lost or stolen. Since biometric data is available all the time and provided by the owner only, it will be very beneficial to generate a private key for public key crypto-system applications [12].

In accordance with the keystroke experiments of Araujo et al. [7], keystroke duration and latency may be features of interest. Nonetheless, as the typing pattern is generally not stable and the

dissimilarity between two persons is not far, only a few bits (10 bits or so) can be extracted from the keyboard dynamics given that the false acceptance rate is reasonably low. But it can be used to harden password [4].

Juels et al. [1] applied an error correcting code to obtain a stable secret to authenticate the user. Similarly, Hao et al. [3] generated a secret from iris (binary) image with Hadamard code and Reed-solomon code.

Dodis et al. [11] formalized the schemes [1] into fuzzy extractor and instantiated with three metrics: hamming distance, set difference and edit distance. However, with edit distance, few bits can be extracted from the biometric data. Boyen [3] extended Dodis's work so that the biometric is reuseabe. However, their distance measures are not satisfactory in most of biometric applications since only Euclidean distance measurement is widely accepted (e.g., [8]- [10]).

Daugman et al. [6] employed multi-scale Gabor wavelet to generate binary biometric code and then authenticated the claimant with the similarity of Hamming distance.

In this paper, we proposed a system to generate a key from Biometric Fingerprint using Hashing Algorithm MD5. Later, we want to propose an investigation into security effect of performance in VoIP scheme, which is based upon ad-hoc network through the voice. Diffie-Hellman key exchange in cryptography utilizes for registration. On the other hand, registration means to check user identify correctly. And then using key from Biometric Fingerprint will be implemented speaker recognition for testing sender's voice at the receiver.

The remainder of this paper is organized as follows. In section 2, we explain biometric cryptosystems. In section 3, we describe biometric technology. In section 4, we present the proposed methodology and implementation. In section 5, we conduct experimental study and finally in section 6, we express conclusion and suggest future research.

2. BIOMETRIC CRYPTO SYSTEMS

A number of biometric characteristics have been in use in various applications (see Fig. 1). Each biometric has its strengths and weaknesses, and the choice depends on the application (e.g., Digital rights management).

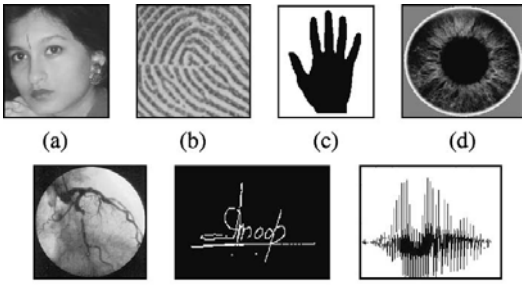

Figure 1. Examples of biometric characteristics. (a) Face. (b) Fingerprint. (c) Hand geometry. (d) Iris. (e) Retina. (f) Signature. (g) Voice. From D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition (New York: Springer-Verlag, 2003), Fig. 1.2, p. 8. Copyright by Springer-Verlag. Reprinted with permission.

3. BIOMETRIC TECHNOLOGY

There are multitude of related theories, concepts, practices or strategies, and technologies which apply in fingerprints technologies.

Personal identification or authentication using biometrics as defined by applies pattern recognition techniques to measure physiological or behavioral characteristics. Generally, there are two types of biometric systems that enable the link between a person and his or her identity. Biometric system can be based on any physiological or behavioral characteristics as long as the following properties are fulfilled;

i. **Universality**; Every person should have the characteristics.

ii. **Uniqueness**; No two persons should be the same in terms of the biometric characteristics.

iii.**Permanence**; The characteristics should be invariant with time.

iv.**Collectability**; The characteristics must be measurable quantitatively and easy to acquire.
v. **Performance**; The biometric technique accuracy level.
vi. **Acceptability**; The level of user acceptance of the biometric system.
vii. **Circumvention**; The level of difficulty in order to forge an identification/authentication [9].

4. PROPOSED SYSTEM

In this system, we proposed technique of generator a key from Biometric Fingerprint's Image. Firstly, we implemented to produce a key using FVC 2004 database for image's template by Matlab 7.0.4. And then this training images are stored database and is generated a key using MD5 hash function by Java Language.

Finally, we have found that overall performance is equal since fingerprint's images match 100% for off-line's testing. We also have implemented Equal Error Rate [EER] to minimize the FAR and FRR. So, we emphasized to get the secret key from this system.

4.1. Fingerprint Recognition

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. This article touches on two major classes of algorithms (minutia and pattern) and four sensor designs (optical, ultrasonic, passive capacitance, and active capacitance) [13].

4.1.1 Histogram

For the histograms used in digital image processing, see Image histogram and Color histogram. So, Histograms are used to plot density of fingerprint's image in figure 2.

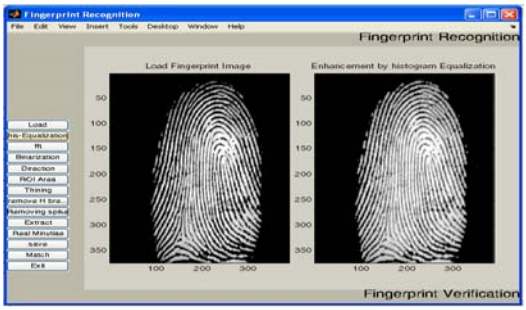

Figure 2. Image Enhancement by Histogram

4.1.2 Binarization

After applying histogram to improve image enhancement, image is converted to binary form using FFT (Fast Fourier Transformer) in figure 3.

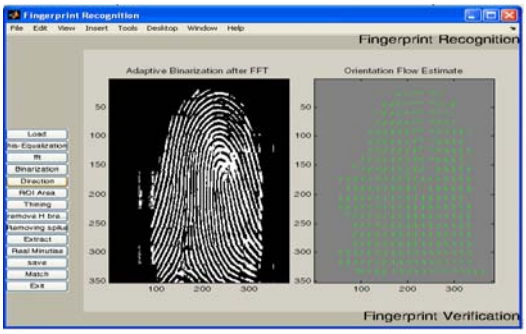

Figure 3. Image Binarization by FFT

4.1.3 Thinning Operation

For minutia extraction stage, thinning operation is tested and the Morphological thinning operation is finally bid out with high efficiency and pretty good thinning quality in figure 4.

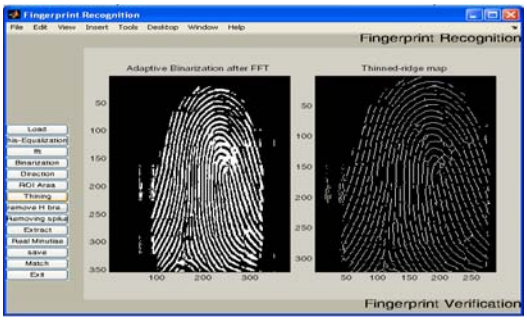

Figure 4. Thinned ridge map

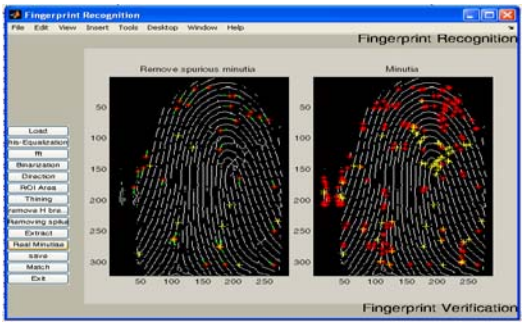

Figure 6. Remove Spurious Minutia

4.1.4 Minutia Extraction

Minutia Origin (real_end, k, ridgeMap) sets the k-th minutia as origin and align its direction to zero (along x) and then accommodate all other ridge points connecting to the minutia to the new coordinate system. So, we calculated minutia points from biometric fingerprint using the difference between the coordination system (x, y) and the angle (theta or θ). For example, according figure 5

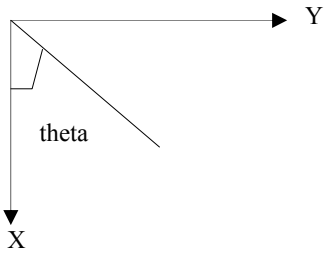

Figure 5. Coordinate System and Angle

The following algorithm is used for minutia point such as

```
theta = real_end (k, 3);
    if theta <0
      theta1=2*pi + theta;
      end;

      theta1=pi/2-theta;

    rotate_mat= [cos (theta1),-sin (theta1); sin (theta1), cos (theta1)];
```

Step by step process, finally real minutiae is emerged from fingerprint's image template and uses "Save" pattern to store the database. Then it utilizes "Match" pattern to express matching percentage in figure 6.

5. CRYPTOGRAPHIC KEY GENERATION FROM BIOMETRICS

For extracting minutiae points from fingerprint, three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and post processing stage. In this system, we proposed four stages (1) preprocessing (2) minutiae feature extraction (3) minutiae point location set and (4) generate a key using proposed algorithm such as MD5 Algorithm.

In this system, we emphasized fingerprint's image from FVC 2004 dataset to generate a key using MD5 Algorithm in figure 7.

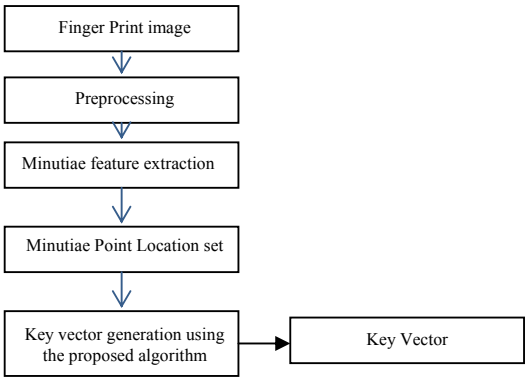

Figure 7. Generate key vector from fingerprint

5.1. Hashing Algorithms

Hashing algorithms take in a large block of data (normally a file, or a network packet) and compute a unique "hash" value (message digest), much shorter than the original data. This "hash" code can be then passed around with (or separate from) the original data, and be used to verify the integrity of the data set. Hashing functions are often used in conjunction with Public Key Cryptography to produced "signed hashes" – short secure representations of the larger data.

There are many hashing algorithms such as MD5 - Message Digest 5, SHA-1, Secure Hash Algorithm - Revision 1, RIPEMD-160, and Tiger and so on. Among them, MD5 is applied to create a key in this system.

5.1.1 MD5 – Message Digest 5

This section generates the key for the security system. Using the selected fingerprint image's file generates the key value. Initially the fingerprint image is converted into pixel matrix. After the matrix conversion the matrix is applied into the one way hash function (MD5). The hash code value is a 64 bit string value. This hash code value is passed into the DES algorithm as key for the encoding and decoding process. This 64-bit key value is converted as a 56-bit key value by the DES algorithm computational operations.

5.1.2 DES (Data Encryption Standard) Algorithm

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. An encryption algorithm along with a key is used in the encryption and decryption of data.

In this system, we need an algorithm to generate keys (Gen), an encryption (Enc) algorithm and a decryption (Dec) algorithm. So, DES (Data Encryption Standard) is used for encrypting and decrypting of data.

A triplet (Gen, Enc, Dec) of algorithms, a message space M and a key space K, is called a symmetric key encryption scheme if:

a. The key-generation algorithm: Gen is an algorithm that returns a key K using the fingerprint, denoted by $k \leftarrow Gen$, such that $k \in K$.
b. The encryption algorithm: Enc is an algorithm that takes a key k and a textdata $m \in M$, and outputs a cipher data $c \leftarrow Enck(m)$.
c. The decryption algorithm: Dec is an algorithm that takes a key k and cipher data c and outputs a textdata m.

The scheme should satisfy the following property: For all $m \in M$ and $k \in K$,

$$[\ Deck\ (Enck\ (m)\ ) = m\ ]$$

In this paper, we are discussing about the key generation method using biometric Cryptosystems (i.e., Fingerprint).

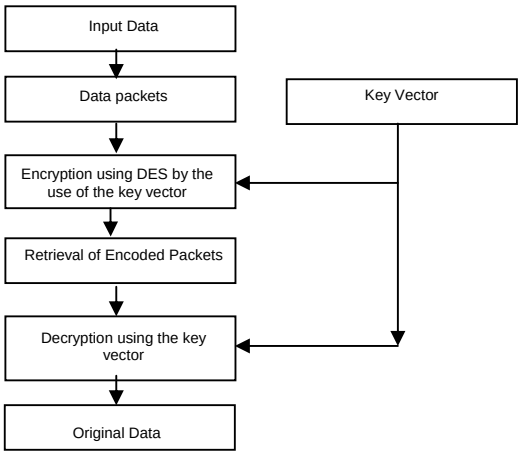

Figure 8. Encrypt and Decrypt using key vector

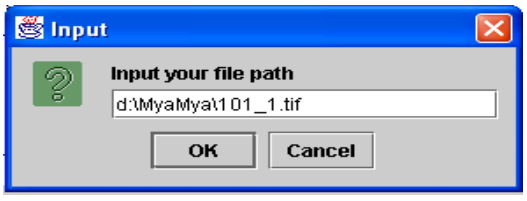

Figure 9. Input fingerprint's file

Figure 10. Key from fingerprint's file using MD5

In figure 9, we implemented the design pattern. Firstly, users must insert input file's name and then produces this file's key using MD5 Algorithm in figure 10.

6. LIMITATIONS

In this paper, we can have problems for enrollment of the fingerprint's image from online. Because coordination system (x, y) is wrong focus from fingerprint's direction using sensor device.

Another is different images (types of direction) from each user in which key is not generated using MD5 Algorithm.

Biometric systems are not perfect. An authorized user may be rejected by the system while an unauthorized user may gain access to it. Lighting, climate conditions low quality equipment or inexperience usually causes the False Rejection Rate (FRR). The False Acceptance Rate (FAR) is caused by the security standard being too low.

So, Biometric cryptosystems that work in the key binding/generation modes are more secure but difficult to implement due to large intra-class variations in biometric data, i.e., samples of the same biometric trait of a user obtained over a period of time can differ substantially.

7. CONCLUSION & FUTURE RESEARCH

This system is developed to provide security for the data files. This system uses Biometric fingerprint for the security system. Generally passwords and smart cards are used for the security systems. Password can be hacked by trail and error basis. But, it is not possible to break the biometric based security system. The system uses two methods for the process. Biometric Fingerprint in which is used for the key build process and DES Algorithm is used for the encryption/decryption process to secure the data files.

Later, we will focus on Biometric Fingerprints for security system. The key is generated by Biometric Fingerprints using new algorithm. Finally, we emphasize the process time for encoding/decoding tasks between traditional security system and biometric based security system in future research.

REFERENCES

[1] A. Juels, M.Wattenberg, “A Fuzzy Commitment Scheme,” ACM Conf. Computer and Communications Security (CCS), pp. 28-36, 1999.

[2] Eric C. Seidel, advisor Joseph N. Gregg PhD *, "Tomorrow’s Cryptography: Parallel Computation via Multiple Processors, Vector Processing, and Multi-Cored Chips", December 30, 2002.

[3] Feng Hao, Ross Anderson, John Boyen, “Combining cryptography with biometric effectively,” http://www.cl.cam.ac.uk/users/jgd1000/biocrypto.pdf July 2005.

[4] F. Monrose, M.K. Reiter and Susanne Wetzel, “Password Hardening Based on Keystroke Dynamics”, ACM CCS, pp.73-82, 1999.

[5] Gobinath Subramanian et al, "Des Enabled Fingerprint System", ICoMMs conference, Malaysia, 11-13 October 2009.

[6] J.G. Daugman, “High confidence visual recognition of persons by a test of statistical independence,”, PAMI, 15(11):1148-1161, 1993.

[7] Livia C. F. Araujo, Luiz H. R. Sucupira Jr., Miguel G.Lizarraga, Lee L. Ling, andJoa B. T. Yabu-Uti, “User Authentication Through Typing Biometric Features,” IEEE Trans. Signal Proc., 53(2):851-855, 2005.

[8] M. K. Mihcak and R. Venkatesan, “New Iterative Geometric Methods for Robust Perceptual Image Hashing,” ACM CCS-DRM. 2001.

[9] Raudzatul Fathiyah Mohd Said et al, "User Technology Readiness Measurement in Fingerprint Adoption at Higher Education Institution", O. Gervasi et al. (Eds.): ICCSA 2008, Part II, LNCS 5073, pp. 91–104, 2008.© Springer-Verlag Berlin Heidelberg 2008.

[10] Xu-Hong Xiao, Graham Leedham, “Signature Verification by Neural Networks with Selective Attention,” Appl. Intell.11(2):213-223, 1999.

[11] Y. Dodis, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometric and other noisy data,” Eurocrypt’04, LNCS 3027, pp. 523-540, 2004.

[12] Yongdong Wu and Bo Qiu, "Transforming a Pattern Identifier into Biometric Key Generators", ICME conference, IEEE, 2010.

[13] http://www.wikipedia.fingerprint-recognition