ACSIJ Advances in Computer Science: an International Journal, Vol. 2, Issue 5, No.6 , November 2013
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

A novel Approach for regenerating a secure and reliable Password using iris and fingerprint

SOROUSH SHIEKHALHOKAMAII [1], MOHAMMAD AMIN PIRBONYEH[2]

[1] Sama technical and vocational training college
Islamic Azad University , Kazeroon Branch , Kazeroon , Iran
S_hokamaii@yahoo.com

[2] Sama technical and vocational training college
Islamic Azad University , Kazeroon Branch , Kazeroon , Iran
Pirbonyeh@gmail.com

Abstract

Cryptography - biological authentications are mechanisms that attempt to identify users by combining unique features such as physical and behavioral characteristics. The old method which was based on passwords (e.g., public key, AES, etc.) can be easily discovered by attackers. In order to improve local security key, this paper presents a method that uses biological fingerprints and iris patterns to generate cryptographic keys. In this method, fingerprint and iris images are collected from the users and the security private key will be created by combining extracted patterns of iris and fingerprint and a hash function. The private key is used for cryptographic applications. Results showed that the model presented in this paper is more resistant against attacks compared with the patterns that are solely based on passwords.

Keywords: Data Security, Human physiology, Encryption

1. Introduction

Information resources are important components of an organization or company. Old cryptography patterns were unreliable and easily discovered by hackers, so in recent years, organizations have paid special attention to the encryption – biological systems which are also called biological cryptosystem [1] . Researchers have studied a lot biological Characteristics (such as Fingerprint, hand anatomy, retina, and iris and facial anatomy) but they have a lot of limitations. Biology is a set of physical and behavioral characteristics that can distinguish people from each other. Physical Characteristics include Fingerprint, hand anatomy, retina, iris and facial anatomy and behavioral characteristics include signature, voice pattern, gait and keystroke [2]. The advantages of biological features are reliability, easiness, and user friendliness but it is important that a biological feature does not provide privacy, because biological data change based on environmental conditions. Securing the extracted patterns of behavior and physical characteristics is the challenge that researchers face. As it was mentioned before, researchers attempted to encrypt data extracted from behavioral and physical characteristics by using encryption patterns which are a great challenge. Old cryptography techniques such as public key cryptography were impossible for the user because he/she was forced to memorize the long password [3], therefore password was encrypted with a key and saved in the memory such as hard disk and etc. In this method password were easily cracked by using social engineering [4]. So the use of a low-entropy password as the key to a strong encryption algorithm made it unsafe and poor [5]. Other encryption methods such as symmetric encryption systems (AES) and Cryptographic systems such as RSA have already provided good solutions to protect credit card data, but these methods have some limitations. First, they require the secure and reliable third party key for user authentication. Second, the user cannot memorize the password

because it is too long; therefore, it is not used directly for encryption [7]. The main purpose of this paper is to present a novel approach for regenerating a secure and reliable private key using iris and fingerprint so that the extracted feature from iris and fingerprint is hashed with powerful hash function and each of them becomes XOR separately; therefore, the powerful private key is generated. The general pattern is defined as follows:

1) The Key which is generated from fingerprint pattern is shown with fip_a

2) The Key which is generated from iris pattern is shown with ir_b

Encrypt: $fip_a \oplus ir_b = eprivatekey$

Decrypt: $eprivatekey \oplus fip_a = ir'$

The main basis of encryption systems are based on pattern authentication, that is, the stored patterns are compared with those of the current model and if they are the same, an authorized user is identified. Extracted patterns are processed by using an image processing algorithm and unique indexes are extracted and then they are stored in database or intelligent card with username and password received from the user. If hackers try to discover pattern by some ways such as intelligent biology, they will fail. The following figure illustrates patterns obtained from fingerprint and retina of some people separately.

2. **Related works**

Researchers have worked a lot in the field of integration of extracted patterns from images and Cryptography. Since biological data are received through sensors and peripheral devices, fixed values will not be provided due to physical and environmental factors; therefore, we should not use biological data directly for encrypting data. During the past years, many efforts have been done in various encryption systems that include binding biological key, cancellable biology and generating biological key. In the technique of binding biological keys, a pattern is presented in which encrypted key and biological pattern are unavailable while encrypted key will be available when the user is recognized to be legal; however, this method has some limitations: First, this technique uses biological comparison in encrypting which makes it complex.

In Cancellable Technique, if the biological model confronts unauthorized access, pattern is changed by using transfer function.

IBM.T.J Waston research institute created this technique for the first time. In the technique of biological key generation that was created by BODO in 1994[4], key is created dynamically by using biological data. According to the latest research, Ahmed and Siyal [5] provided a new approach in regeneration of local key by using fingerprint and smart card password that is called 3-ks since fingerprint, password and smart card are received from user at enrollment stage. This technique uses encrypting SHA-1 for generating local key by using fingerprint pattern. Song and Beng[6] suggest an approach that personalizes the key biological key which was manufactured by using fingerprint pattern In this method fingerprint pattern are turned to discrete binary values called fingerhash and Reed Solomon error correction was used to stabilize the volatility in fingerhash. Shen and Chen [7] offered a pattern that creates reliable and safe encrypting key by using fingerprint pattern. In this method there is no need to memorize the long key and coding matrix is also used for encrypting data.

Among the above mentioned methods only the biological fingerprint pattern is used to encrypt, but the method (which used extracted patterns from fingerprints and iris in an integrated way) was used to produce a safe private key dynamically. This reduced vulnerability to attacks.

3. **Extracting the iris pattern**

The iris is the circular, colored part of the eye**.** The iris contracts and expands its dilator muscles, depending on the surrounding light conditions. By regulating the size of the pupil, the iris directs the light onto the retina [2].

These steps are followed to extract the iris pattern:

1) Image acquisition: This module captures one or multiple iris image(s) from the subject using an iris camera. The iris image must have at most 50-pixel for the size of the iris radius.

2) Preprocessing: at this stage, the image is enhanced first. The enhancement includes contrast adjustment and noise filtering. The next step is to perform edge detection and thresholding. The papillary boundary (inner boundary of the iris), the limbic boundary (outer boundary of the iris), eyelids, and eyelashes are detected.

3) Normalization: normalization is usually performed in this step between the pupillary boundary and the limbic boundary to reduce the effect of the pupil contrast. This is performed by localization algorithm.

4) Template generation: The extracted iris patterns are not ready for comparison yet. In this step, the template is created from the extracted iris patterns.

In the literature, there are various ways to generate the templates, including Gabor wavelet, zero-crossing wavelet, local variance, spatial filters, and 1D local texture pattern approaches. This paper uses Gabor wavelet to extract pattern. The main purpose of this study is to provide a new method for the generation of safe local key by using fingerprint and iris. So, pattern recognition which is one of the main stages in the generation of safe key will be studied here.

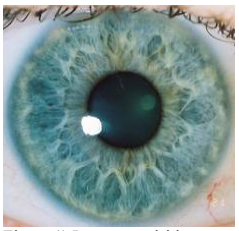

Figure 1) Image acquisition

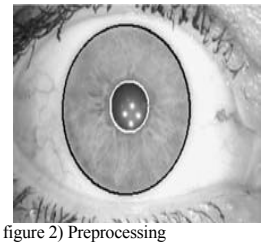

figure 2) Preprocessing

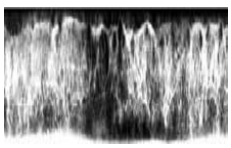

Figure 3) contrast adjustment

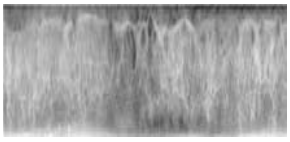

figure 4) extract iris pattern

3.1 Gabor wavelet method

Wavelet packet decompositions are usually calculated by using orthonormal or biorthogonal wavelets. Wavelet decomposition can be done by using wavelet transformation algorithm.

At each stage in the decomposition part of a two-dimensional FWT filter bank, four output images are generated. The images contain approximation (A), horizontal detail (H), vertical detail (V) and diagonal detail (D) patterns respectively. In wavelet analysis, each output image is processed again and only images that contain patterns are processed [8]. Wavelet transformation is done at 3-levels that generate 64 sub images, each representing a part of the frequency plane.

Approximate energy distribution for an image can be calculated using wavelet packets:

$$E_i = \sum_{j,k} w_i(i,j)^2$$

Where *Ei* is the energy of the sub image *wi*. This formula shows a good description of the content of the image.

The following images shows the structure of the Gabor wavelet.

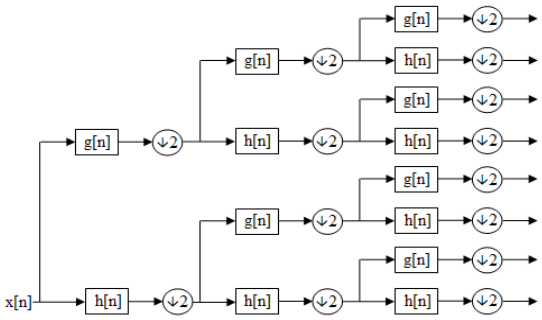

Figure 5) structure of the Gabor wavelet

Finally, extracted patterns are compared with saved patterns in database by using Hamming Distance method. The following formula is used to compare patterns by using Hamming Distance technique

$$HD = \frac{1}{N} \sum_{j,k} s1(j,k) \otimes s2(j,k)$$

Where *S1* is binary pattern extracted from user iris and *S2* is the binary pattern which is saved in database and *N* is the number of bits in each pattern which is achieved at image processing stage.

$\otimes$ is also XOR operator.

Based on xor relation we understand that we can find similar bits in patterns by using this relation. Extracted points are used

for the generation of safe key. The following table shows the implementation of wavelet technique for extracting patterns based on both authentic and inauthentic specification.

Table1: carry out Gabor wavelet method on three image

Gabor wavelet	Valid	invalid
a	0.21	0.60
b	0.40	0.80
c	0.152	0.90

3.2. Generating safe private key by using pattern extracted from iris

Points extracted from the iris, are among the most important factors in the user detection. To generate the safe private key, first binary patterns are extracted from the iris images and then they are hashed using the SHA-512 algorithm. The key name will be stored in the smart card with user name. Points extracted from the vector are shown with Ba and a=1, 2, 3, … , 270 . To dynamically generate local key we must store changes in the vector continuously; therefore, we define σ_l set that l=a

Formula derived for coding regions is as follows:

$$\{a=1,2,3,\ldots,180\}\ \sigma_l = B_a$$

$$\text{IrisEx} = \left(T_{sha-1}\left(\sigma_l + T_{sha-1}(pwdus_a + \lambda)\right)\right)$$

Pwdusa is a password that user enters for identification. $T_{sha-512}$ is hash algorithm that produces an amount of 512 bits. In the above formula λ prevents the creation of the redundant amount in the reproduction of the key.

4. Extracting pattern from fingerprint

Fingerprint consists of some ridges. In order to show unique specifications, the image of the fingerprint is divided into M*M block to show characteristics better [10].

Fingerprint has three main features that make it unique.

1) The end of the ridge: the point that ridge ends. Figure 6 shows the end of it.

2) Branched ridges: one ridge is divided into two parts. Figure 6-b shows branches of the ridge.

3). Short ridge: a ridge which is the shortest one. Figure 6-c shows short ridges.

Figure 6) Fingerprint Features

An important characteristic which makes fingerprint unique is a combination of different ridges.

By combining the abovementioned characteristics, we can infer unique patterns which are called minutia point [9]. The point of the ridge is also called pointed area and these two characteristics are among the most prominent characteristics of fingerprint. Many techniques are mentioned in this study in order to extract minutia points [10]. They can be divided into two groups:

1) Making the images of the fingerprint binary

2) Showing the images of the fingerprint by grayscale

In this paper gray-scale is used to extract minutia point. To extract minutia point we can use Fawad et al [9] technique that called these extracted points, point vector $\vec{V}_a$. These extracted points are used dynamically to produce safe key.

The stages of the extracting points are as the followings:

1) The image of the fingerprint is received from input and processed by grey-scale technique.

2) We get $\vec{V}_a$ by the following equation [6].

$$V_a = \frac{1}{2}\tan^{-1}\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N} 2G_x(i,j)G_y(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} G_x{}^2(i,j) - G^2{}_y(i,j)}\right)$$

$\vec{V}_a$ is the vector of extracted points. G_x is angles' gradient at points I and j.

4.1. coding extracted points from fingerprint

Extracted points $\vec{V}_a$ are of great importance. Since we can differentiate fingerprints by these points. we should code the extracted points. In this paper, we use SHA-512 algorithm to code the extracted points and store the produced key in database or a smart card. Conventionally, we show each extracted point of vector $\vec{V}_a$ with E_a and a=1,2,3,...180. Since each change in processing, is implemented in vector $\vec{V}_a$, we create a set ϖ_{sk} that s=a and k=1,2,3,...(2r+1). R shows the number of angles. The formula of coding ϖ_{sk} is as the following:

$$\text{Codminutia}= \left(T_{sha}(\varpi_{sk}+T_{sha}(pwdus_a+\omega)\right)$$

Where pwdusa is the password that is received at first to identify user and $pwdus_a$ is the coding algorithm of A_{sha}. SHA function produces a hash value of 128 bits by using algorithm SHA-512. In producing private key, using ω in producing a safe password causes that value ϖ_{sk} and a will not be equal.

5. A new way of producing password

In this method, we produce safe private key by using patterns extracted from fingerprint and iris. First, password, fingerprint and iris of the user are received then Codminutia and irisex are retrieved from database or smart card to identify the user. The process of key production is described here:

First step: Users enter password (pwd_a), fingerprint, and (fipa) iris image irsa into identification system by using a camera.

Second step: Codminutia and IrisEx are retrieved from private database and then decoded by $pwd_{a\,[}8]$. The input images change into grey-scale by the user are adjusted by using the algorithm of image lay out, minutia.

Third step: Encryption technique of extracted points from fingerprint that was carried out at 4-1 is used for encrypting the image of the fingerprint.

Forth step: Encrypting extracted patterns from iris that were carried out at 3-2 will be implemented.

Fifth step: the output of two encoding techniques fingerprint and iris are done by the following technique and the result will be a safe private key.

Sixth step: the resulting output will be changed into the base of two and the resulting amount will be xor.

The following figure shows the process of the production of safe private key by using fingerprint and iris.

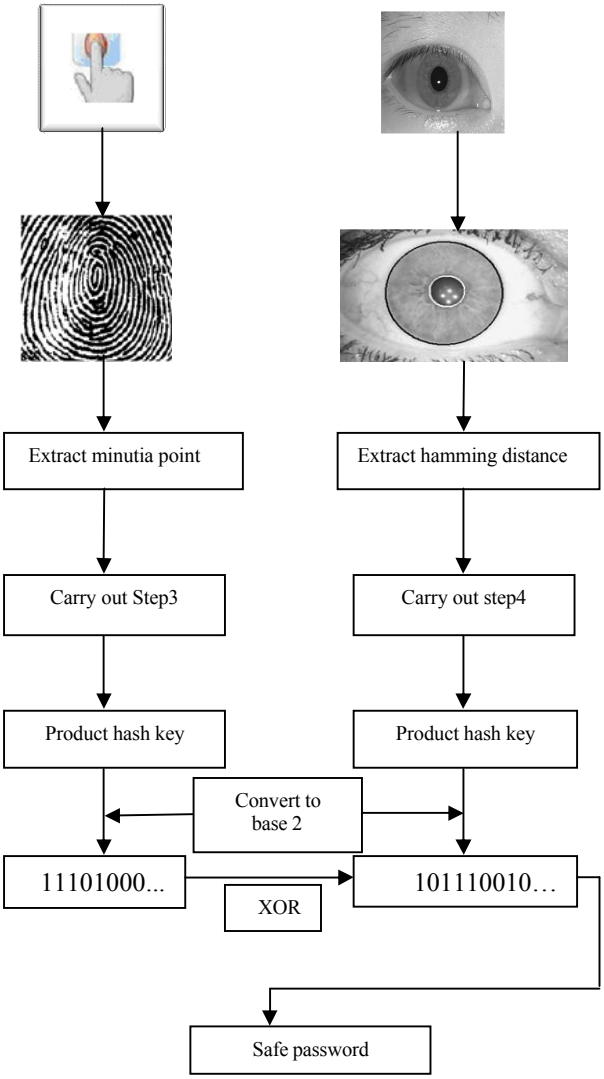

Figure 7) structure of new way of producing password

6. Conclusion

Old methods such as encryption, public-key cryptography are very vulnerable and can easily be discovered by hackers. Therefore, in this paper, a local key generation method is presented by using unique biological characteristics. In this method, at first password, fingerprint and iris image of the user are received by using embedded sensors (enrollment) and then hash technique is used to encode extracted points that distinguish users from each other. Encrypted outputs of the two biological patterns are XOR, and a secure password is created. The results show that these techniques are dynamically stable against changes in fingerprint and iris pattern in order to generate secure keys. Patterns presented in this paper are more robust against attacks compared with patterns that are solely based passwords. The key element in this procedure is that 3 passwords, fingerprint, and iris must be logged.

References

[1] Yingzi Eliza Du," Review of iris recognition: cameras, systems, and their applications", *Information Management & computer security,* Volume 26 · Number 1 · 2006 · 66–69,

[2] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare," International Journal of Computer Science and Information Security, Vol. 7, No.3, 2010

[3] Monrose, F., Reiter, M.K. and Wetzel, S. (1999), "Password hardening based on keystroke dynamics", *Proceedings of ACM Conference Computer and Communication Security*, pp. 73-82.

[4] Monrose, F., Reiter, M.K., Li, Q. and Wetzel, S. (2001), "Cryptographic key generation from voice", Proceedings 2001 IEEE Symposium on Security and Privacy, pp. 202-13.

[5] Bodo (1994), "Method for producing a digital signature with aid of biometric feature", German Patent, DE 4243908A1.

[6]Ong Thin Song, Andrew Teoh Beng Jin (2007),"Personalized biometric Key using fingerprint biometrics", *Information Management & Computer Security, Vol. 15 No.4,pp313-328*

[7] Ratha, N.K., Connell, J.H. and Bolle, R.M. (2001), "Enhancing security and privacy in biometrics-based authentication systems", *IBM Systems Journal, Vol. 40 No. 3, pp. 614-34.*

[8] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R. and Kumar, B.V.K.V. (1998a), "Biometric Encryption using image processing", Proc. SPIE, Vol. 3314, pp. 178-88.journal paper

[9] Fawad Ahmed and M.Y. Siyal,(2005)" A novel approach for Regenerating a private key using password, fingerprint and smart card, *Information Management & computer security,* Vol. 13 No. 1, 2005 pp. 39-54, journal paper

[10] Weiguo Sheng, Gareth Howells, Michael Fairhurst and Farzin Deravi, Shengyong Chen,(2012)" Reliable and secure encryption key generation from fingerprints", *Information Management & Computer Security,* Vol. 20 No. 3, 2012pp. 207-221