RSA Cryptographic Key Generation Using Fingerprint Minutiae

Mofeed Turky Rashid[1], Huda Ameer Zaki[2]
[1] Electrical Engineering Department / University of Basrah
mofid76@yahoo.com
[2] Computer Science Department / Shatt Al-arab College University
Hazz79@yahoo.com

Abstract: *Human users find difficult to remember long cryptographic keys. Therefore, researchers, for a long time period, have been investigating ways to use biometric features of the user rather than memorable password or passphrase, in an attempt to produce tough and unrepeatable cryptographic keys and to construct the key unpredictable to a hacker who is deficient of important knowledge about the user's biometrics. In this paper, generating the strong bio-crypt key based on fingerprint minutiae is presented. At first, the minutiae points are extracted from the fingerprint image based on image processing algorithms. Then, the extracted fingerprint minutiae are used for generating a 1024 bit prime numbers that used in RSA cypher algorithm to generate 2048 cryptographic key.*

Keywords: Biometrics, Cryptography, Fingerprint, RSA, Morphological Operation, Minutiae points.

الخلاصة: المستخدمين يجدون من الصعب تذكر المفاتيح الطويلة للتشفير لذلك حاول الباحثين ولمدة طويلة من اكتشاف طرق لاستخدام خصائص المستخدمين البايومترية بدلا من كلمة أو عبارة المرور في محاولة لإنتاج مفاتيح تشفير صعبة الكسر وغير قابلة للتكرار و لبناء مفتاح لا يمكن التنبؤ به او قرصنته وخاصتا للذين ليس لديهم معرفة حول المقاييس الحيوية للمستخدم. يقدم هذا البحث طريقة لتوليد مفتاح حيوي قوي مستند على تفصيلات بصمات الأصابع. في البداية تم استخلاص الصفات من صورة بصمة الإصبع بالاعتماد على خوارزميات معالجة الصور ثم استخدمت هذه الصفات لتوليد ارقام اولية طولها 1024 bit حيث تستخدم هذه الارقام في خوارزمية طريقة التشفير RSA لتوليد مفتايح تشفير بطول 2048 bi

1. Introduction

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. These days, 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, eye, face, and voice. Further there is explosion of information exchange and sensitive data across the network or internet and cryptography is becoming an increasingly important feature of computer security. Many cryptographic algorithms are available for securing information. However, the security is dependent on the secrecy of the secret key because larger the size of key, stronger will be security. But it would clearly not be feasible to remember the user so much big key. The biometrics traits e.g. fingerprint, hand, eye, face, and voice encrypt with original message to generate the encrypted data and further the same will be used to decrypt it.

Biometric cryptosystems combines cryptography and biometrics to afford the advantages of both for security. This technique will provide the advantages like better and modifiable security levels which are the advantages of cryptography and advantages like eliminating the must to memorize passwords or to carry tokens etc which are the advantages of using biometrics [1].

Agood biometric is characterized by use of a feature that is highly unique - so that the chance of any two people having the same characteristic will be minimal, stable so that the feature does not change over time, and be easily acquired - in order to provide convenience to the user, and prevent misrepresentation of the feature. Fingerprint recognition is the oldest method of biometric identification. In this time the fingerprint identification technique is used, with the name as dactyloscopy. The fingerprint is composed of ridges (lines across fingerprints) and valleys (spaces between ridges) [2].

2. Methodology

A. *Fingerprint characteristics*

In this approach fingerprint is used as a biometric parameter for generation of encryption key. Fingerprints have been used for over a century and are the most widely used form of biometric identification. The fingerprint of an individual is unique and remains unchanged over an individual's lifetime. A fingerprint is formed from an impression of the pattern of ridges on a finger. A ridge is valley is the region between two adjacent ridges. The set of minutiae types are restricted into only two types, ridge endings and bifurcations, ridge endings are the points where the ridge curve terminates, and bifurcations are where a ridge splits from a single path to two paths at a Y-junction. Fig. 1 illustrates an example of a ridge ending and a bifurcation. In this example, the white pixels correspond to the ridges, and the black pixels correspond to the valleys [3].

For each fingerprint of individual there are unique features as follow:

a) Each fingerprint is unique to individuals i.e. no two fingers have identical ridge characteristics.
b) They are highly universal as majority of the population have legible fingerprints.
c) They are very reliable as no two people have same fingerprint. Even identical twins having similar DNA, are believed to have different fingerprints.
d) Fingerprints are formed in the fetal stage and remain structurally unchanged throughout an individual's lifetime.
e) It is one of the most accurate forms of biometrics available.
f) Fingerprint acquisition is non-intrusive and hence is a good option.

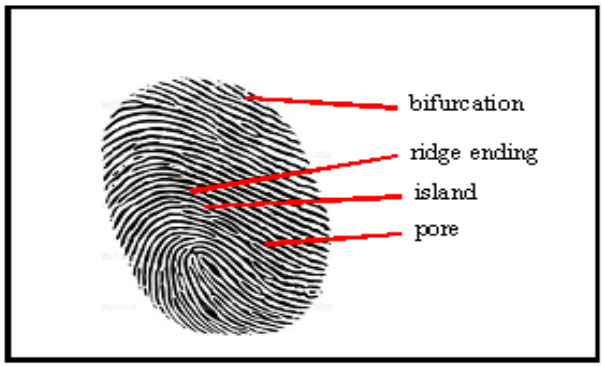

Figure 1: Fingerprint Image with different identifying points.

B. ***RSA encryption***

The user's biometric features were integrated into the key generation process based on the RSA algorithm, so that, the process is unpredictable for hackers and external users not having the same biometric traits. RSA is public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA) which supports encryption and digital signatures. It is most widely used public key algorithm and gets its security from integer factorization problem. It is relatively easy to understand and implement. RSA is used in security protocols such as IP data security, transport data security, email security, terminal connection security and many more. RSA use two different keys with a mathematical relationship to each other. Their protection relies on the premise that knowing one key will not help you figure out the other. The RSA algorithm uses the fact that it's easy to multiply two large prime numbers together and get a product. But you can't take that product and reasonably guess the two original numbers, or guess one of the original primes if only the other is known. The public key and private keys are carefully generated using the RSA algorithm; they can be used to encrypt information [4].

The public key consists of the value n, which is called the modulus, and the value e, which is called the public exponent. The private key consists of the modulus n and the value d, which is called the private exponent. An RSA public-key / private-key pair can be generated by the following steps:

1. Generate a pair of large, random prime's p and q.
2. Compute the modulus n as $n = p \times q$.
3. Select an odd public exponent e between 3 and n-1 that is relatively prime to p-1 and q-1.
4. Compute the private exponent d from e, p and q.
5. Output (n, e) as the public key and (n, d) as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the eth power modulo n:

$$c = \text{ENCRYPT}(m) = m^e \bmod n \qquad (1)$$

The input m is the message; the output c is the resulting cipher text. In practice, the message m is typically some kind of appropriately formatted key to be shared. The actual message is encrypted with the shared key using a traditional encryption algorithm.

This construction makes it possible to encrypt a message of any length with only one exponentiation.

The decryption operation is exponentiation to the dth power modulo n:

$$m = \text{DECRYPT}(c) = c^d \bmod n \qquad (2)$$

The relationship between the exponent's e and d ensures that encryption and decryption are inverses, so that the decryption operation recovers the original message m. Without the private key (n, d) (or equivalently the prime factors p and q), it's difficult to recover m from c. Consequently, n and e can be made public without compromising security, which is the basic requirement for a public-key cryptosystem.

3. Cryptographic Key Generation Based on Fingerprint Biometric

Biometric cryptosystems as shown in Fig. 2 combine both biometrics and cryptography to afford the advantages of both for security purposes. This technique provides the advantages like better security levels for data transmission and eliminating the must to memorize passwords or to carry tokens etc. In this approach for generating cryptographic key, fingerprint has been selected as the biometrics feature. Minutiae points have been extracted from the fingerprint image and that points set are used for generating cryptographic key. Several steps have been achieved in order to generate cryptographic key from fingerprint biometric as follow:

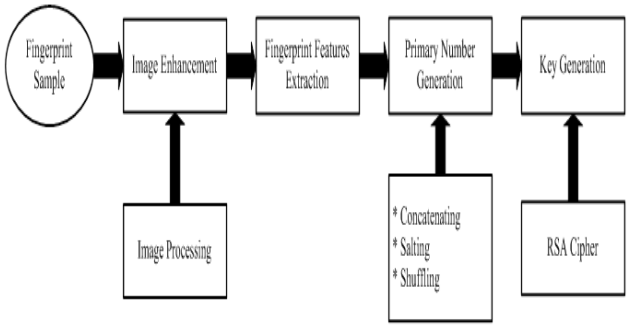

Figure 2: Biometric cryptosystem.

a) ***Image Enhancement***: The main reasons of performing image enhancement are to improve the contrast between ridges and valleys, reduce noise in the fingerprint image and protect the true configuration of them. The enhancement method is the modification of image brightness, contrast, and equalization.

b) ***Image Binarization***: It is the process that converts a grey scale image into a binary image. By using traditional threshold based methods to convert gray scale fingerprint image into black white shows low accuracy, so adaptive binarization algorithm has been used for high accuracy conversion. In this case there is no universal threshold value of whole image, but for each pixel its own threshold value is calculated separately depending on pixel location which the average value of intensity of neighborhood pixels block has been represented as threshold value. If the gray value of the pixel is greater than threshold, then it is set to white, otherwise it is black. This method is much more accurate, if the size of neighborhood pixels block for threshold calculation is selected appropriately. Analyses have shown that the optimum size of pixels block is depending on fingerprint image. The best results are obtained when block size is a little bigger than twice of the thickness of the ridge.

c) ***Morphological Operations*:** The most basic morphological operations are dilation and erosion. Dilation adds pixels to the boundaries of objects in an image, while erosion removes pixels from object boundaries. The number of pixels added or removed from the objects in an image depends on the size and shape of the structuring element used to process the image. In the morphological dilation and erosion operations, boundaries of objects inside fingerprint image have been modified for accurate recognition [5].

d) ***Thinning*:** Before the minutiae extraction stage, a thinning process is used to on skeletonize the binary image by reducing all lines to a single pixel thickness.

e) ***Minutiae Extraction*:** For each 3x3 window inside fingerprint image, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window, so the two pixels will be marked as branches too. But actually only one branch is located in the small region, so a check routine requiring that none of the neighbors of a branch are branches is added [6].

f) ***Feature Representation***: Every trivia purpose extracted from a fingerprint image is represented as (x, y) coordinates. Here, we tend to store those extracted minutiae points in two totally different vectors: Vector F_1 contains all the x coordinate values and Vector F_2 contains all the y coordinate values.

$$F_1 = [x_1\ x_2\ x_3 \dots x_n];\ |F_1| = n \quad (3a)$$
$$F_2 = [y_1\ y_2\ y_3 \dots y_n];\ |F_2| = n \quad (3b)$$

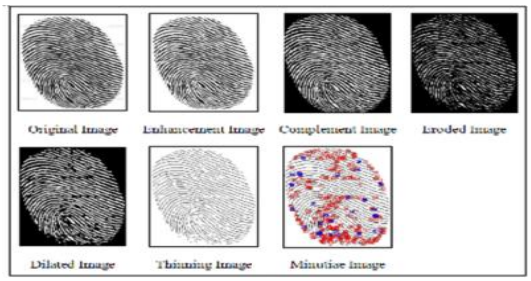

Figure 3: Extracting fingereprint features.

g) ***Prime Number Generation*:** F_1 and F_2 vectors have been used to generate unique prime number (p) based on three processes:

I. Concatenating process: In this step the features of F_1 and F_2 have been concatenating in order to generate single vector S as follow:

$$S = [x_1\ x_2\ x_3 \dots x_n\ y_1\ y_2\ y_3 \dots y_n];\ |S| = 2n \quad (4)$$

For example shown in Fig. 3 which (x,y) is the coordinates of x- bifurcation and y- bifurcation respectively, the values of F_1, F_2, and S as follow:

F_1 = [99 100 101 73 100 162 163 73 72 70 73 72 30 31 31 209 210 149 150 226 227 226 224 225 200 201 225 201 178 178 178 192 193 228 229 193 219 220 75 75 229 230 133 134 168 168 61 61 61 39 40 226 226 227 138 139 139 164 164 179 179 180 219 220 182 182 97 98 218]

F_2 = [14 14 15 16 16 16 16 17 28 29 30 31 36 36 37 38 38 55 55 64 64 65 66 66 67 67 67 68 77 78 79 86 86 86 86 87 95 95 98 99 100 100 117 117 124 125 133 134 135 137 137 137 138 138 148 148 149 165 166 166 167 167 167 167 168 169 177 177 178]

S = [99 100 101 73 100 162 163 73 72 70 73 72 30 31 31 209 210 149 150 226 227 226 224 225 200 201 225 201 178 178 178 192 193 228 229 193 219 220 75 75 229 230 133 134 168 168 61 61 61 39 40 226 226 227 138 139 139 164 164 179 179 180 219 220 182 182 97 98 218 14 14 15 16 16 16 16 17 28 29 30 31 36 36 37 38 38 55 55 64 64 65 66 66 67 67 67 68 77 78 79 86 86 86 86 87 95 95 98 99

100 100 117 117 124 125 133 134 135 137 137 137 138 138 148 148 149 165 166 166 167 167 167 167 168 169 177 177 178]

II. *Salting process*: In this process, the vector S has been salted to 1024 bit number which a vector R of random numbers has been generated and concatenated with vector S to generate vector U of 1024 bit.
If the number of bits of all numbers in vector S are greater than 1024 bit then remove the numbers in the top of S vector to reduce number of bits less than 1024 and then salting process will be performed.
The overall number of bits of the individuals in vector S of example in part I is 991 bits then the overall number of bits must be added as random numbers is (1024-991 = 33 bit). The vector U will be as follow

S = [99 100 101 73 100 162 163 73 72 70 73 72 30 31 31 209 210 149 150 226 227 226 224 225 200 201 225 201 178 178 178 192 193 228 229 193 219 220 75 75 229 230 133 134 168 168 61 61 61 39 40 226 226 227 138 139 139 164 164 179 179 180 219 220 182 182 97 98 218 14 14 15 16 16 16 16 17 28 29 30 31 36 36 37 38 38 55 55 64 64 65 66 66 67 67 67 68 77 78 79 86 86 86 86 87 95 95 98 99 100 100 117 117 124 125 133 134 135 137 137 137 138 138 148 148 149 165 166 166 167 167 167 167 168 169 177 177 178 46 65 87 31 202]

III. Shuffling process: The Mongean shuffle algorithm has been used for shuffling of vector U, which is the principle of algorithm as follows (by a right-handed person): Start with the unshuffled deck in the left hand and transfer the top card to the right. Then repeatedly take the top card from the left hand and transfer it to the right, putting the second card at the top of the new deck, the third at the bottom, the fourth at the top, the fifth at the bottom, etc. The result, if one started with cards numbered consecutively 1, 2, 3, 4, 5, 6, … , 2n, would be a deck with the cards in the following order: 2n, 2n-2, 2n-4, … , 4, 2, 1, 3, … , 2n-3, 2n-1.

U = [31 65 178 177 168 167 167 166 149 148 138 137 135 133 124 117 100 98 95 86 86 79 77 67 67 66 64 55 38 37 36 30 28 16 16 15 14 98 182 220 180 179 164 139 227 226 39 61 168 134 230 75 220 193 228 192 178 201 201 225 226 226 149 209 31 72 70 73 162 73 100 99 101 100 163 72 73 30 31 210 150 227 224 200 225 178 178 193 229 219 75 229 133 168 61 61 40 226 138 139 164 179 219 182 97 218 14 16 16 17 29 31 36 38 55 64 65 66 67 68 78 86 86 87 95 99 100 117 125 134 137 137 138 148 165 166 167 167 169 177 46 87 202]

Final step is all numbers in vector U have been concatenated. If the result number is odd and not prime number then 2 will be added until arriving to prime number while if the result number is even and not prime number at first step 1 will be added and tested for prime number if not then 2 will be added at next steps.

Conclusions

In this paper, a unique key generation using fingerprint minutiae has been achieved in order to perform high security for network systems. The challenge that has been solved in this approach is using fingerprint minutiae for generating 1024 bit prime numbers that were used in RSA cipher method for generating 2048 bit key. The minutiae of fingerprint extracted from fingerprint image by using image processing algorithms which the resolution, brightness, contrast of fingerprint image has been modified also unwanted pieces (noise) has been removed. This method is simple and can be implemented by different types of processors like microcontroller, ARM, FPGA, etc.

References

[1] Kamini H Solanki, Chandni Patel, "Biometric Key Generation In Digital Signature Of Asymmetric Key Cryptographic To Enhance Security Of Digital Data", International Journal of Engineering Research & Technology (IJERT), Vol. 2, Issue 2, pp. 1-8, Feb. 2013.

[2] Dr. Manish Manoria, Ajit Kumar Shrivastava, Satyendra Singh Thakur, DebuSinha, "Exploring the Prospect of Secure BiometricCryptosystem using RSA for Blind Authentication", International Journal of Wisdom Based Computing, Vol. 1 (2), pp. 24-27, August 2011.

[3] Priyanka Patel, "Secure Fingerprint Identification System and Matching by UsingImage Registration and Key Matching Techniques", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 6, pp. 2012-2017, June 2013.

[4] A. Jaya Lakshmi, I. Ramesh Babu, "Design of Secured Key Generation Algorithm using Fingerprint Based Biometric Modality", IOSR Journal of Engineering (IOSRJEN), Vol. 2 Issue 2, pp. 325-330, Feb. 2012.

[5] Mohammed Tajuddin, C. Nandini, "Cryptographic Key Generation using Retina Biometric Parameter", International Journal of Engineering and Innovative Technology (IJEIT),Volume 3, Issue 1, pp. 53-56, July 2013.

[6] Kim Seonjoo, Lee Dongjae, Kim Jaihie, "Algorithm for Detection and Elimination of False Minutiae in Fingerprint Images", 3rd International Conference on Audio- and Video- based Biometric Person Authentication, 2001.