ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Data Encryption Algorithm using Asymmetric Key Derived from Fingerprint Biometric Features

Prof. Dr. Tarik ZeyadIsmaeel[1], Ahmed Saad Names[2]

University of Baghdad, Electrical Engineering Department, Baghdad, Iraq[1,2]

Abstract: Security is a one of the major concerns in the present because of increasingtheinformation quantity and theft. Due to these causes, an efficient security system is more importantto protect the personal information. This leads to use password, keys, etc.to secure the information. Fingerprint Encryption is preferable biometric technique for securing text because of its parallelism, vast storage and fast computing quality. In this paper will use the features provided by the fingerprint of the information sender to extract a new encryption method depending on the distribution of the hells and valleys of the finger print since this distribution differs from one finger to another and from one person to another. The proposed method will be used for text data transmission. The types of encryption key generators which will be used through this research are the private key generators. Extracted the feature vector from fingerprint. Then the feature vector is converted to encryption key. In general, encryption algorithms use this fingerprint key to encrypt and decrypt the data. In encryption and decryption we use a new algorithm, which depend on look up table to encrypt and decrypt message. The security is enhanced in this paper by using fingerprint encryption technique.

Key Words: Encryption Algorithm, Asymmetric key, Fingerprint biometric, Decryption Algorithm.

1. INTRODUCTION

Data security is very much necessary fordatasecurity of the personal computer. Usedthe Cryptography techniques are using for secure data.

Cryptography is the ability for safe storage and transport sensitive data. Cryptography, to most persons, is concerned with preservation communications secret. Cryptography means “Hiding a information by first converting it into an unintelligible form by ciphering and then converting back to intelligible form by deciphering [1].

The technique of protecting data by converting an encrypted message into an unreadable format, called cipher textonly those who possess a privetkeycan decipher or decrypt the message into plain text. Encrypted messages cansometimes be broken by cryptanalysis and is also called code breaking. In, short using cryptography data is first encrypted into another form and then transmitted.

Thus, in Cryptography there are different steps which are as follows:

1. In First, encrypt the message.
2. In Second, Step Processing of message is done which contain a private key.
3. At last the encrypted message is decrypted by using private key [10].

There are two types of encryption methods: Symmetric Key or Private Key Cryptography and Asymmetric or Public Key Cryptography.

In ours algorithm will use a symmetric.

In general, symmetric encryption scheme has five ingredients.Plaintext, Encryption algorithm, Secret key, Cipher text and Decryption algorithm

In any encryption algorithm, there are two requirements [1]

1. We need a strong encryption algorithm and strong key.
2. Sender and receiver should have usedthe same key.

Fingerprint is a one of the most common physical biometric patterns analyzed that is used to purposes of information security.

A biometric is a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. A statistical analysis these biological characteristic is known as the biometrics science [3].

In present, fingerprint technologies are used to analyze characteristics of biometrics science for security purposes. Each fingerprint containtwo types of features. These features are called end ridge and bifurcation ridge.

The security is depended on the strong of the key [3]. In the traditional cryptographic algorithms, such as “advanced encryption standard” (AES), "data encryption standard" (DES) and “Rivest-Shamir-Adelman” (RSA) etc., data is encrypted using privet or public key. The short keys are easy to be remembered, but they are also easy to be broken. And the long keys are difficult to be broken, but they are also difficult to bememorized and have to be stored in somewhere, which can be stolen or lost. Biometric encryption, which use the features of biometric to encrypt data. Some biometric cryptographic algorithms have been developed based on fingerprints [7], iris [8], signature [9] and DNA [4] etc.

The fingerprint encryption offers a new mechanism for key security by using a fingerprint to secure the cryptographic key. Instead of entering a password to access the Cryptographic key, the use of this key is

DOI 10.17148/IJARCCE.2015.47133

guarded by fingerprint encryption. When a user wants to access a secured key, the user will be prompted to allow for the capture of a fingerprint sample.then the key is released and can be used to encrypt or decrypt the desired data. The fingerprint encryption will offer a both convenience, as the user not need to remember a key, and secure identity confirmation, since only the real user can release the key[3].

2. FINGERPRINT IMAGE ENHANCEMENT, PREPROCESSING AND FEATURE EXTRACTION

To can use the image of fingerprint in encryption algorithm must be applied many of intermediate steps. In These steps, will enhance the fingerprint image by apply some of mathematical equation on original image to get on the enhanced image. And then will extract feature from Enhanced image [6]. All intermediate steps in respectively are.

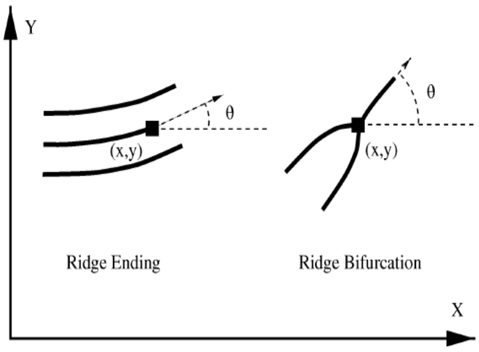
1. Segmentation.
2. Image enhancement.
3. Binarization. [2].
4. Region of Interest [5].
5. Thinning [2].
6. Feature extraction

Will use the Crossing Number (CN) concept to extract the feature from thinnedimage.

In this method, a window of 3x3 pixels is used to check each pixel neighborhood in the image and the CN value is determined as half the sum of the differences between two neighbor pixels in eight pixels which is Surrounding of this window.

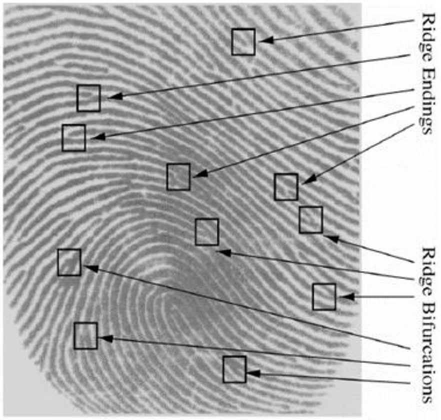
The most stableridges, which called minutiae, are:
1) _ ending
2) _ bifurcation.

Where a ridge ends suddenly. This point calls ending. And where the ridge branches in to two ridges. this point calls bifurcation.CN for ridge ending equal to one and CN for ridge bifurcation equal to three [2]. Examples of minutiae are shown in Fig. 1[6].



(a)

Figure 1. Minutiae. (a) A minutiae can be characterized by its position and its orientation.



(b) Minutiae overlaid on a fingerprint image.

3. ENCRYPTION AND DECRYPTION

A. Code generation

Step 1 .find average point of minutiae (ridge ending and ridge bifurcations), (X', Y')

$X'=\frac{\sum_1^i Xi}{i}$ $Y'= \frac{\sum_1^i Yi}{i}$ (1). When i is equal to number of minutiae.

Step 2.Convert that minutiae (ridge ending and ridge bifurcations) to polar form i.e. (magnitude and theta) by calculate the length (LE) and angle (θ) between each minutiae and average point.

$LEi=\sqrt{(Xi-X')^2+(Yi-Y')^2}$ (2).$\Theta i=\tan^{-1}\frac{Yi-Y'}{Xi-X'}$ (3)

Step 3. Find the maximum value of length from this length

Step 4 normalize this lengths by divided each value on the maximum value.

Lei norm=$\frac{LEi}{\max(LEi)}$ (4).

Step 5. Write the codewhich represented the vector of (Lei norm and Θi).

Note. We can derive the fingerprint's code from minutiae ending or minutiae bifurcation or merge between them

B. Create look up table

Create look up table (M*N) where M is the number of rows which depend on the number of symbols that wont to encrypt and N is the number of columns which depend on the code i.e.(each range of length and angle of fingerprint code will refer to one column).as shown in table (1)

C. Encryption

Step1. Select the same sequence for key and message. I.e.(first key to first letter). If the length of key is shorter than letters of message will repeat that code.

Step2. Select the column from look up table depends on the first number of fingerprints' keys (norm Lei and θ).

Step3.Choose the row depend on the location of this litter at first column

Step4.intersection between that column and row to choose cipher letter

Step 5.repeat that four steps above to encrypt another letter.

DOI 10.17148/IJARCCE.2015.47133

number of column number of row	**1**	**2**	**3**	**4**	**5**
	At ORIGINAL MESSAGE	LEnorm (0 - 0.7.) θ<180	LEnorm (0.7-1). θ<180	LEnorm (0 - 0.7.) Θ>180	LEnorm (0.7 - 1) Θ>180
1	A	X	N	H	J
2	B	C	Q	Y	I
3	C	F	W	U	K
4	D	G	E	C	Z
5	E	D	T	%	O
6	F	A	B	G	P
7	G	M	C	A	V
8	H	R	F	M	E
9	I	N	G	R	T
10	J	Q	X	N	B
11	K	W	L	X	D
12	L	E	O	Q	5
13	M	Z	P	W	R
14	N	2	*	S	N
15	O	T	D	E	2
16	P	#	A	T	Q
17	Q	H	M	B	W
18	R	Y	R	D	S
19	S	&	J	L	F
20	T	J	I	O	G
21	U	K	K	P	+
22	V	I	Z	V	M
23	W	L	H	J	H
24	X	O		I	Y
25	Y	P	U	K	U
26	Z	V	S	Z	C
27	space	U	Y	!	L

Table (1) show how generate look up table

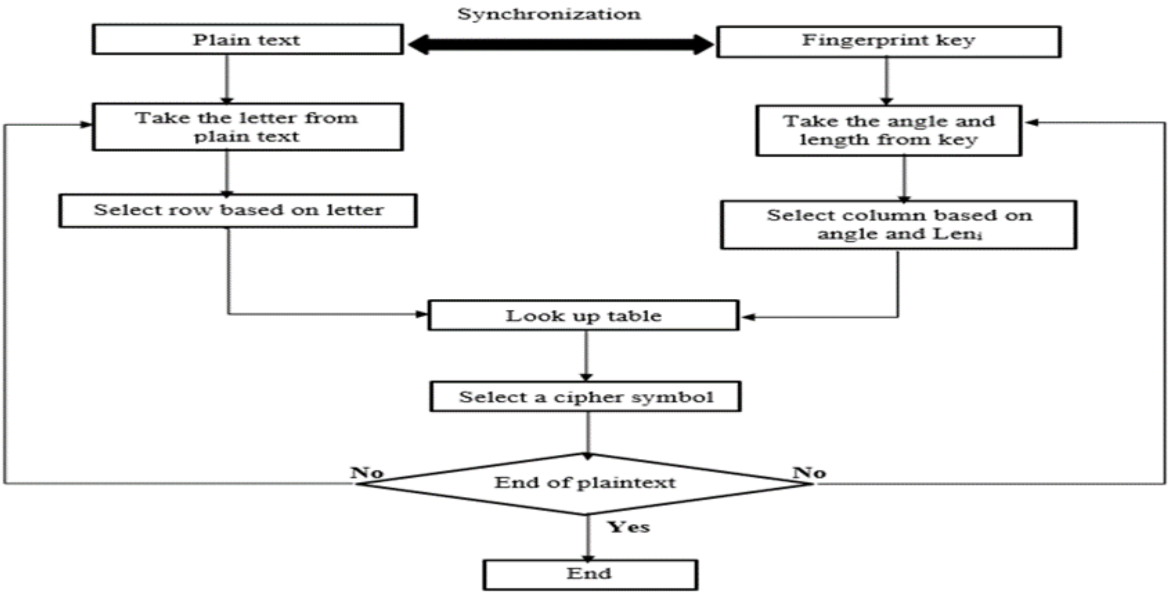

Synchronization
Plain text
Fingerprint key
Take the letter from plain text
Take the angle and length from key
Select row based on letter
Select column based on angle and Lenᵢ
Look up table
Select a cipher symbol
No
End of plaintext
No
Yes
End

Figure (2): block diagram illustrates encryption steps

DOI 10.17148/IJARCCE.2015.47133

For example: to our encryption algorithm. Took asample of minutiae from fingerprint's image
X= [82, 125, 201, 222, 281, 6, 225, 201] y= [7, 9, 14, 250, 251, 252, 253, 10].
At first generated code by apply generated code algorithm. Equation (1, 2, 3, 4)
And get to code as shown in table (2). And then generated lock up table (for our example contain 4 columns and 27 rows) as shown in table 1. If wont to increase encryption strength take moor rows and columns.

X	Y	Le_i	Len_i	θ
82	7	150.6273	0.7448	235.2417
125	9	129.0788	0.6382	250.6000
201	14	121.3583	0.6000	285.8400
222	250	130.9583	0.6475	65.5877
281	251	165.0979	0.8163	46.7487
6	252	202.2500	1.0000	143.1655
225	253	134.9382	0.6672	64.9542
201	10	125.2111	0.6191	285.3404

Table (2) show generated code

To encrypt message (HELLO WORLD).
Step 1.The first letter of message is H and also look to first number of a code vector (LEi norm =0.7448 and θ= 235.2417).
Step 2. Due to LN_1 =0.7448 >0.7 and θ_1= 235.2417>180 so will choose5th column in table (1).
Step 3Letter H locate at 8th row in the first column at table (1).
Step 4 intersection between 5th column and 8th row will get to letter E
Step 5.The second liter is E which located in 5th row in the table and the second code is LN_2 is 0.6382 andθ_2= 250.6000 so will choose 4th column and intersection with 5th row will get to letter (F)
And so on to encrypt all messages and get to this message (E%QEDYLESQC)

D. Decryption

Note: Decryption must use same thefingerprints' codes and table in encryption.

Step1. Choose the samesequence for cod and message. I.e. (first code to first letter). If the length of cod is shorter than letters of message will repeat that code.
Step2. Depend on the fingerprint's code choose the column from table (1).
Step3.In this column will find a location of the symbol that wrote in the encrypted message.
Step4.Depending on the rows' location of that symbol will choose the letters from the first column.
Step5.repeat three steps above to decrypt all messages

To decrypt (E%QEDYLESQC) at first depend on code vector will choose 5thcolumn and find the row of letter E which located in 8th row and then take the 8thletter from first column which refer to(H).
And then take second code and second letter and so on to decrypt all messages and get to original message (HELLO WORLD).

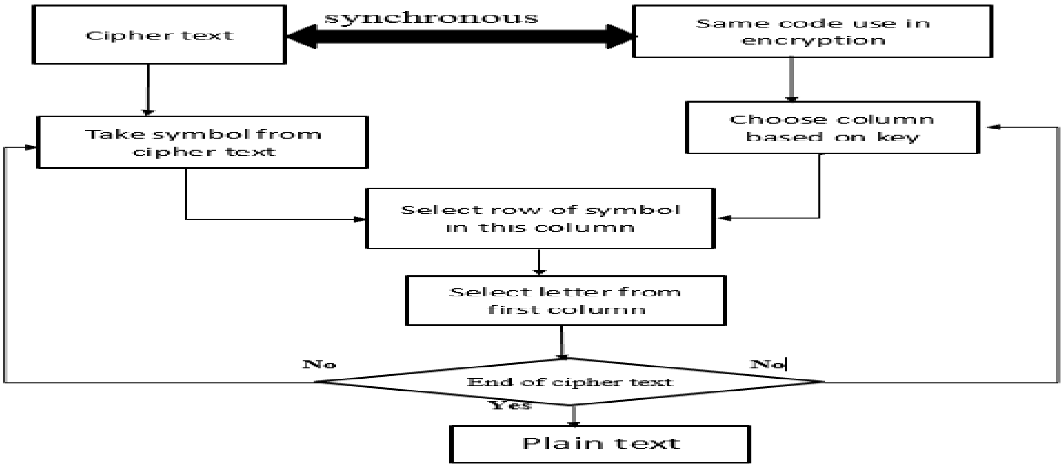
4. Security strength

An attack is a most threat to anysecurity system. For a fingerprint encryption system, not only the encryption information, e.g. the password, but also the fingerprint data must be protected against attacks. In this section, will list some of typical attacks and analyze how the proposed protocol defends against

A. Biometric template attack

In this algorithm, Key generates from fingerprint feature, i.e. length and angle between average point and minutiae. It is noticeable that one fingerprint can only contain limited number of minutia points, approximately between 20--40. If attackers acquire minutiae information successfully, they can narrow down the search range of Key. In other words, the cryptographic key space created by 20--40 minutiae points is small [7].

The proposed solution to solve this problem by increasing the total number of minutiae by add noise through image enhancement and this noise will increasing the number of minutiae and also will increase the key strength.


Cipher text
synchronous
Same code use in encryption
Take symbol from cipher text
Choose column based on key
Select row of symbol in this column
Select letter from first column
No
No
End of cipher text
Yes
Plain text

All decryption steps illustrates in figure (4)

DOI 10.17148/IJARCCE.2015.47133

B. Brute force attack

Involves trying every possible key until an intelligible translation of the cipher text into plaintext is obtained. On average, half of all possible keys must be tried to achieve success [1]. The security strength of an algorithm cannot exceed its key length. In our protocol, Key is generated from a set of minutia points and number of rows and columns in table
To break a key by the brute force attack for a given key length

Time needed to break the fingerprint key in second = $\frac{Nc^{lk}}{2*1000000}$(5)
NC=number of column in table.
Lk=length of fingerprint key.
Divided by 2, for averaging
Divided by1000000, assuming that it takes 1µS to perform a single decryption, [1]
To calculate the time that need to break a table, which used for encryption, will use equation (6)
Time need to break a table=Nc*(Nr!) (6)
When Nr is number of rows i.e. (number of symbol that use in encryption algorithm).
NC is the number of columns.

5. EXPERIMENTAL RESULTS AND ANALYSIS

A. Encrypted message by fingerprint code and using Mat lab environment

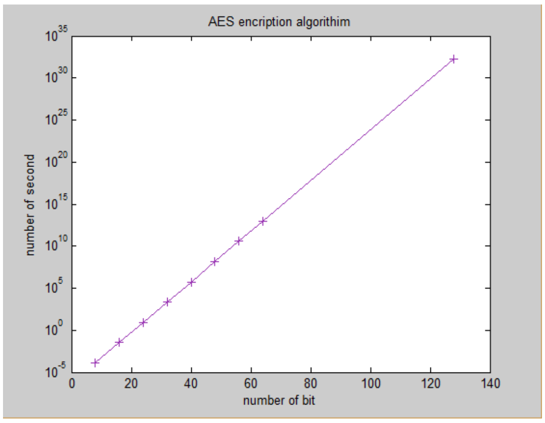
- At first derive the fingerprints code from minutiae that represent ridge ending to encrypt this message (HELLO WORLD). And get to this cipher (R3&T@M9@X91)
- Then derive the fingerprints code from minutiae that represent ridge bifurcation to encrypt this message (HELLO WORLD). And get to this cipher (VDX#F7YYX ;?)
- At last derive the fingerprints code by using combination of two minutiae (ridge bifurcation and ridge ending) to encrypt this message (HELLO WORLD). And get to this cipher (G9XLF7YYXBP)

B. Comparison between fingerprint encryption and AES algorithm

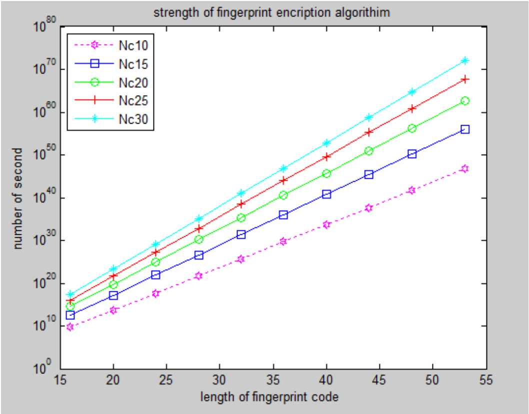
AES proves to be a better security algorithm than DES and Triple DES [11].due to this reason will compare the performance of our algorithm with AES
Shown in figure (4) the Comparison between fingerprint encryption and AES algorithm:

At first, test performance of AES by compute half of all possible keys divided by (1000000) in figure (4a). Then Test the performance and measure security against brute force attack of our algorithm and get to the result that shown in figure (4 b).

By observing the results in Figure 3 we compare between our algorithm and AES algorithm.
1-The security of AES algorithm depended on a key length while in our method the security depended on two parameters (key length and number of rows in table).
2-our method takes much more time to break by the brute force attack for a given key length.



(a)



(b)

Figure (4); the Comparison between fingerprint encryption and AES algorithm. (a) AES algorithm (b) Fingerprint encryption

C. Speed of fingerprint encryption

The speed of encryption system is measured by size of encrypted data, in kilo byte, peer one second.
The result of this test shown in figure (5)

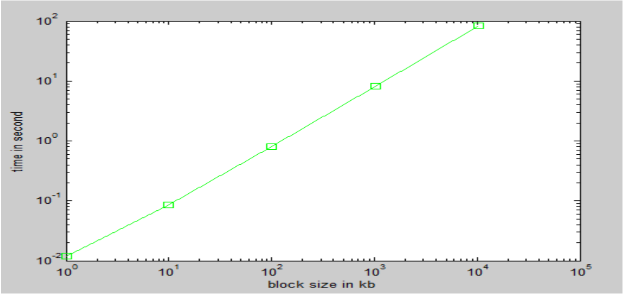


Figure (5). Fingerprint encryption speed

DOI 10.17148/IJARCCE.2015.47133

6. CONCLUSIONS

This paper proposed a novel fingerprint cryptosystem. The system extracted vector feature from fingerprint and used the modified algorithm to encrypt and decrypt messages. Experimental results show that the proposed fingerprint cryptosystem can work effectively, and observe that can encrypt message using three fingerprint's code derive from minutiae (ending, bifurcation and merge between them) and get to three different message. The result shows that our algorithm is very strong and it is almost impossible to be cracked.

REFERENCES

[1] William Stallings, "Cryptography and Network Security: Principles and Practice 5th Edition", Prentice Hall, 2010.

[2] Azad Noor, "A New Algorithm for Minutiae Extraction and Matching in Fingerprint", Ph.D Dissertation, School of Engineering and Design, Brunel University, 2012.

[3] Colin Soutar, Alex Stoianov, Rene Gilroy, and B.V.K Vijaya Kumar, "Biometric EncryptionTM", Proc. SPIE 3314, pp. 178-188, 1998.

[4] Anupryia Agrawal, and Praveen Kanth, "Secure Data Transmission Using DNA ENCRYPTION", IISTE Journal of Computer Engineering and Intelligent Systems, Vol.5, No.7, 2014.

[5] RajuRajkumar , and K Hemachandran, "A Secondary Fingerprint Enhancement and Minutiae Extraction", Signal & Image Processing : An International Journal (SIPIJ), Vol.3, No.2, 2012.

[6] Lin Hong, Yifei Wan, and Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, No. 8, 1998.

[7] Kai Xi, Tohari Ahmad, Fengling Han and Jiankun Hu, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment", Wiley Online Library, Vol.4, Issue.5, 2010.

[8] Xiangqian Wu, Ning Qi, Kuanquan Wang, and David Zhang, "A Novel Cryptosystem based on Iris Key Generation", Fourth International Conference on Natural Computation, Vol.4, pp. 53-56, Jinan, 2008.

[9] SanaulHoque, Michael Fairhurst, and Gareth Howells, "Evaluating Biometric Encryption Key Generation using Handwritten Signatures", Symposium on Bio-inspired, Learning Intelligent Systems for Security, pp. 17-22, Edinburgh, 2008.

[10] Ms. Priyanka, P. Palsaniya, and Mr. Pravin D. Soni "CryptoSteganography:Security Enhancement by using Efficient Data Hiding Techniques", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2**,** 2014.

[11] Mona Mudaliar, and L K Bhaiya, "Analysis of Symmetric Algorithms in MPLS Network", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 4, 2012.

DOI 10.17148/IJARCCE.2015.47133