Secure Exchange of Generated Key by Fingerprint Ridges Depend on Cubic Bezier Curve

Wesam Samier Bhaya
University of Babylon, Iraq
Information Networks Dep. IT College
wesambhaya@uobabylon.edu.iq

Wael Mahdi Brich
University of Babylon, Iraq
Information Networks Dep. IT College
Waal_555@yahoo.com

Abstract

Biometric science is one of the important tendencies which used in a human entity identification and security fields. Fingerprint is an important vital index in the field of security because it's unique for any individual and no change in its properties with time. Information security means protecting information from access illegal. This paper suggests a new approach for information secrecy and authentication on networks. This method used matching the features of fingerprints to ensure the sender authentication and generate the symmetry key depending on the ridges curvatures of fingerprint. Bezier curve equation is used to visualizing those ridges and store the result of control points which represent these curves in a matrix, then the algorithm will be selected randomly two curves when those curves have maximum degree of curvature to generate the symmetry key that used for encryption, authentication, and secured key exchange.

Key words: Biometric, Fingerprint, Cryptography, AES encryption algorithm, and Bezier curve.

الخلاصة

علم البايومتريه واحد من الاغراض المهمه التي تستخدم في تعريف كينونة الانسان وفي مجالات الامن. تعتبر البصمه مؤشر حيوي مهم في مجال الامنيه لانها فريده لاي فرد ولاتتغير خواصها عبر الزمن. امنية المعلومات تعني حماية المعلومات من الدخول غير المشروع. هذا البحث يقترح تقنيه جديده في مجال امن المعلومات والموثوقيه في الشبكات. هذه التقنيه تستخدم مطابقة ميزات البصمه لضمان التثبت من هوية الشخص المرسل وتوليد مفتاح تشفير متناظر وذلك بالاعتماد على انحناءات خطوط البصمه. تستخدم معادلة منحني بيزير لمحاكاة هذه الخطوط وخزن النقاط الناتجه لتمثيل هذه المنحنيات في مصفوفه حيث ستختار الخوارزميه عشوائيا منحنين يمتلكان اعلى درجة انحناء لتوليد المفتاح المتناظر لغرض تشفير البيانات والتثبت وتبادل المفتاح بصوره امنه.

الكلمات المفتاحية : البايومترية ، البصمة ، التشفير ، خوارزمية تشفير AES

1- Introduction

Biometric (fingerprint, hand, eyes, face, and voice) is one of the important fields in human identification and security. This science depends on the biological characteristic because the shape and location or behavioral of characteristic humans are different from one person to another (Anil *et al.,* 2007). Fingerprint is one of the famous biometric systems for identification, because it's unique for an individual and it's not change through the life, except the distortion may be happened on the skin by injuries or diseases (Peter *et al.,* 2005).

Fingerprint image is a pattern formed by a dark region called ridges and light region called valley which two trapped between ridges (Anil *et al.,* 2007). Global and local points are two types of features that used to recognize the fingerprint for identification and verification. Global features have two points on skin of fingerprint called core and delta points used for classify the fingerprints for five classes called (Whorl, left loop, right loop, arch, and tented arch**)**. Local features or (minutiae) have two common points distributed on the ridges lines; first point called ridge ending and the second called bifurcation point (Henry and Robert 2001).

Information security is the process of protecting the privacy and integrity of data and keeps it from any denial unauthorized access, for a high level of security there are a various cryptosystems have been used when data encrypted before transmission on network **(**Gunjan and Rama 2012).

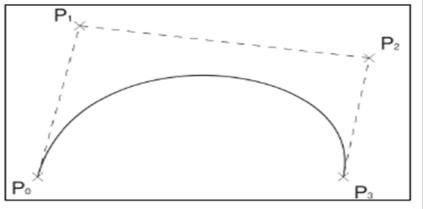
Cryptography is a science that providing level of security for storage information on our computers or when transmission it between parties on closed or open network. Today Cryptography is a cornerstone of modern electronic security technologies (William 2006). There are two types of cryptography the first called symmetric key when using the same key for encryption and decryption, and the second type called asymmetric key when there are two different keys mathematically related as one key which using for encryption and the other used for decryption. The security in the symmetric key depends on how well the sender and receiver can protect the key from broken. In symmetry key the level of security depends on the length of key and the type of algorithm that used as (AES, DES, blowfish, .etc), **(**Gunjan and Rama 2012).

Security of any encrypted data depend on the encryption algorithm and the encryption key. The keys management is often the weakest point for many encryption systems and thus need using suitable technique to keep the key in safe place. The biometric system is the solution for problem of key management, because the features in each type of biometric unique for any one can be used for identification (Zdenek 2000; Lukasz 2009).

Bezier curve was invented by Pierre Bezier in 1970**.** Bezier curve defined by four points, two points called the end points and the other points called control points, as shown in figure (1)**.** This curve passes through end points but does not pass through control points**.** When the location of control points has been changed, the shape of curve changes and that give the flexibility for drawing different shapes of curves and this suitable for visualizing the shapes of ridges in fingerprint images. Cubic Bezier curve equation is (David 2005):

$p(t)_{x,y}= (1-\mathrm{t})^3 p_0(\mathrm{x},\mathrm{y})+ 3(1-\mathrm{t})^2 \mathrm{t}\, p_1 (\mathrm{x},\mathrm{y}) + 3(1\text{-}\mathrm{t})\, t^2\, p_2(\mathrm{x},\mathrm{y}) + t^3\, p_3 (\mathrm{x},\mathrm{y})$.

Where (t) is ratio 0<= t <=1, p(x,y) is coordinates of control points of Bezier curve.



Fig(1) Cubic Bezier Curve

There are some related works about using Bezier curve and generate the secure key depend on biometric characters as:

- **Generation of biometric key for use in DES:** this method depends on the number of local features dotes in fingerprint image to generate the key**.** After remove false minutiae, the number of interested features represents the total key after taking the mod 64 for these points to generate the encryption key. This key is different from one to another because the unique property of fingerprint **(**Rupam 2012)**.** This method is more sensitivity for features points while our approach uses the features in fingerprint for authentication. In addition the our proposed method uses the ridges to generate symmetry key with 128 bits as length and using AES algorithm for encryption and decryption.
- **An innovative scheme for effectual fingerprint data compression using Bezier curve representations:** this system provides compact storage for fingerprint image through utilizes a cubic Bezier curve by visualizing each segment of ridge from fingerprint image and store the control points for each segment of curve for fingerprint image in database. This process reduces the size of memory that needed for storage (Vani and Jagannathan 2009)**.** Our proposed system is using cubic Bezier curve for

visualizing each segment of ridges from fingerprint and stored the control points for each segment with index number in a matrix, Then select randomly the control points for two curves which have maximum curvature degree from matrix, and substitute this control points for each curve in equation of Bezier curve. The initial value of parameter (t) which takes value between 0 and 1 substitute in Bezier equation to generate the encryption key from the random numbers of p(x ,y), that result from Bezier equation for each curve selected from the matrix of control points.

2. Fingerprint Security Proposed System

The proposed system consists of three stages: preprocessing of fingerprint and authentication, encryption and decryption. These stages explain in figure (2):

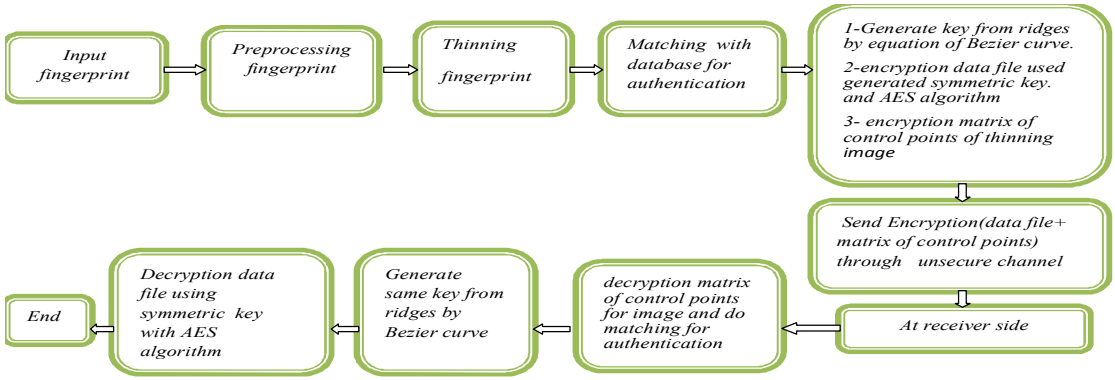


Figure.(2)A block diagram of the proposed fingerprint security system

2.1 Preprocessing of Fingerprint Image

This stage is very important to improve the quality of fingerprint image, because the system of matching depends on good quality of fingerprint image. Extraction the features for fingerprint matching and extract the ridges with its co-coordinates and store coordinates such as a control points in a matrix depend on the steps that used in a preprocessing for fingerprint image after acquisition fingerprint. Preprocessing for fingerprint image involves five stages as shown in figure (3) (Raymond 2003).

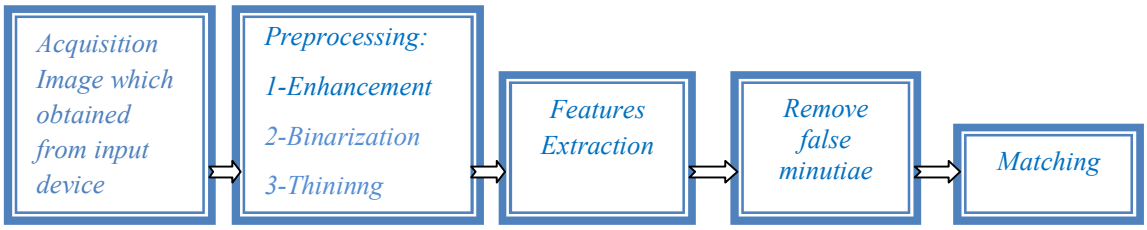


Figure.(3) Steps of preprocessing for finger print image.

2.1.1 Image acquisition

This stage represents the method which used to capture the fingerprint image**.** There are many methods which are used to capture fingerprint image, suchas the inked impression or by fingerprint scanner**.** There are many different factors take in to consideration when we choose the method of acquisition of fingerprint image **(**Nalini and Venu 2008**).**

2.1.2 Enhancement

This stage is very important for image after acquisition. Fingerprint images are generally obtained from the scanner or from other media. There is no guarantee of their good quality, because the image may be having some noise and distortion (Lukasz 2009). The enhancement stage is improving the contrast between ridges and valleys and

reduces the noise. This can be done by using suitable types of filtering like Gabor filter, median filter, etc. We need suitable threshold choice to keep the features of fingerprint image clear (Raymond 2003)**.**The description of the steps for enhancement is as followed:

- **Fingerprint image normalization**

Normalization is used to standardize the intensity of the pixels in fingerprint image**,** by using the variance in grey-level values along the ridges and valleys. The normalized image is defined as follows (Lukasz 2009)**:**

$$N(i,j)\begin{cases} M0+\sqrt{\left(\frac{v0}{v}\right)(I(i,j)-M)(I(i,j)-M)} & \text{if } I(i,j) > M \\ M0-\sqrt{\left(\frac{v0}{v}\right)(I(i,j)-M)(I(i,j)-M)} & \text{otherwise} \end{cases}$$

Where

Mean…M=$\frac{1}{h\times w}\sum_{i=0}^{w-1}\sum_{j=0}^{h-1}I(i,j)$ (h) and (w) height and width of fingerprint image. I(i, j) represents the intensity value of pixel.

Variance…v=$\frac{1}{h\times w}\sum_{i=0}^{w-1}\sum_{j=0}^{h-1}(I(i,j)-m)\text{^}2$

m0 and v0 are the desired mean and variance values.

Normalization does not change the valley and ridges structures.

- **Binarization**

This stage involves convert the grey image to binary image (0, 1) by using the suitable threshold. Figure (4.a) shows binary fingerprint image (Raymond 2003)**.**

- **Thinning**

This stage converts the thickness of ridge in fingerprint to width with one pixel wide without affect on the structure of fingerprint**.** The ridges in binary image are thinned to one pixel wide by examining the (8) neighborhoods of each pixel in the binary image by scanning and deciding, if the pixel can be thinned or not until one pixel wide as shown in figure(4.b**)** Lukasz 2009)**.**

(a) Binary image

(b) Thinning image

Figure(4) Thinning of Binarization image

- **Feature extraction**

Feature extraction is very important for matching of fingerprint images. After the fingerprint ridges thinning, we will determine the position (x, y) and the direction of the ridge (θ) of minutia points. The cross number (CN) is commonly employed method of feature extraction, this method used the skeleton image where the ridge flow pattern is eight-connected. The local features are extracted as in figure(6) by scanning the local neighborhood for each ridge pixel in the block of image. In general, for each block (3×3), the type of minutia is a bifurcation, if the central pixel of block is 1 and has exactly 3 one-values neighbor and the minutia is ending ridge if the central pixel is 1 and has one- value neighbor as shown in table(1). The CN value computed as half the

sum of the differences between pairs of adjacent pixels in the eight neighborhoods by using formula (Rupam 2012)**:**

CN=$\frac{1}{2}\sum_{i=1}^{8}|p_i - p_{i-1}|$, $p_9 = p_1$,where p_i is the pixel value in the neighborhoods of p as illustrated in Figure(5).

Table(1): properties of crossing number(CN).

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure.(5):pixel in image using 3×*3 window*

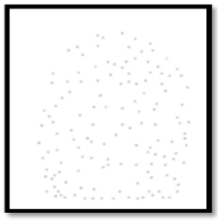


Figure.(6): Extracted features

- **Matching**

This stage used for verification and identification. After minutiae extraction and remove false minutiae from thinned image, the matching stage is start. This operation is complete the comparative between the features of online acquisition image with features of fingerprint image in database**.** There are many factors effect on the result of matching as the noise, extraction error, displacement and rotation. The highest similarity between the input and stored image means the acceptance (Raymond, 2003) **.**

2.2 Encryption stage

This stage includes the steps for generate the encryption key which uses to encryption data file and the steps of encryption the thinning image is shown in figure(7).

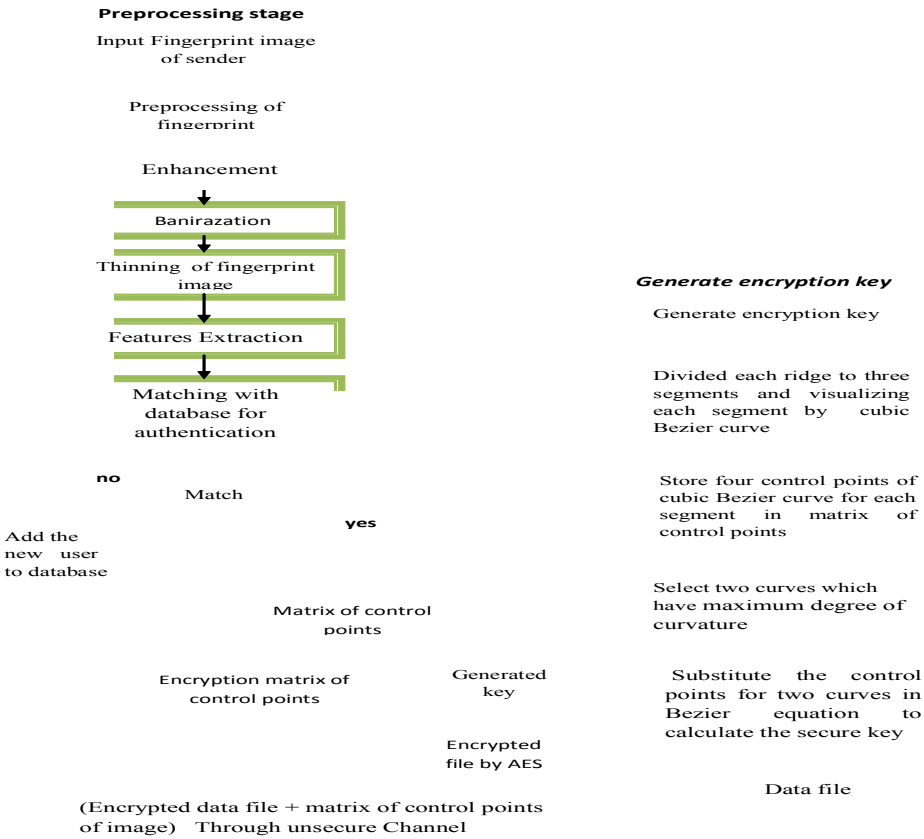


Fig (7) Block diagram explain generate encryption key, preprocessing and encryption fingerprint image and data file.

2.2.1 Generate the Encryption Key from the Ridge of Fingerprint

This approach used fingerprint to generate the symmetry key for encryption data file and exchange this key in the same file on networks. The generated key depends on the shape and location of ridges of fingerprints.

After complete preprocessing stage on fingerprint image and do matching for authentication**,** the encryption stage is begin, if the result of authentication is true the first step to generate the encryption key is begin, this step includes extracted the coordinates of control points for each segment for all ridges, and store these points with index number in matrix of control points.

The second step the algorithm is begin to check the curvature degree for all these curves and select two curves which have maximum value of curvature degree of ridge line, then substitute these control points for two curves in cubic Bezier curve equations.

$P(t) = (1-t)^2 p_0 (x,y) + 3(1-t)^2 t\, p_2 (x,y) + 3(1-t)\, t^2\, p_2 (x,y) + t^3\, p_3 (x,y)$ when $0 <= t <= 1$

Then the algorithm selects the initial value of parameter (t) when ($0 < t < 1$) there are many values of $[p(t)_{x,y}]$ result from Bezier equation for values.

The number of these result points depends on the value of (t) and the curvature degree of ridge, from the list of random numbers of values x and y which generated from Bezier equation the algorithm selected (12) numbers for each value for (x) and (y) and trunk four digits at most right from these numbers and convert each two values from four digits to binary form. Then the algorithm stores 128 bit is represent the key encryption which is using in encryption stage with AES algorithm after put the key in hexadecimal form as 128 bit in matrix 4×4 called the matrix of key

- **Algorithm for generate encryption key**

The steps of algorithm for generate encryption key explain as below:

At sender:-

Input: *thinning fingerprint image .*

Output : *symmetry key with length of 128 bits .*

Begin

index=0

Dividing *each ridge to three segments and visualizing each segment by cubic Bezier curve .*

Index=index+1

Store *the result of control points for each segment with number index in vector matrix.*

Calculate *the curvature degree for each curve and order the control points for these curves ascending depending on the curvature degree.*

Select *control points for two curves which have more curvature degree from matrix of control points depends on curvature degree of curve.*

Substitute *the control points of two curves in cubic Bezier equation.*

T= any initial value selected by sender between 0 and 1

I=0

Begin

$P(t) = (1-t)^3 p0(x,y) + 3(1-t)^2 t\, p1(x,y) + 3(1-t)\, t^2\, p2(x,y) + t^3\, p3(x,y)$

while t < 1

t = t + T

calculate *the value of p(t) for two curves*

B[i]=p(t)

I=i+1

End while

j=0

While j <= I

Select *4 digits at right most from B[i] which result one integer number of 4 digit length.*

Store *the result integer number in matrix C[j].*

j=j+1

End while

J=0

J=J+1

Convert *each two digits of integer number in C[j] to binary form and store the result in matrix A(J).*

J=0

While Q[j]<128

Q[j]=A[j]

J=j+1

End while

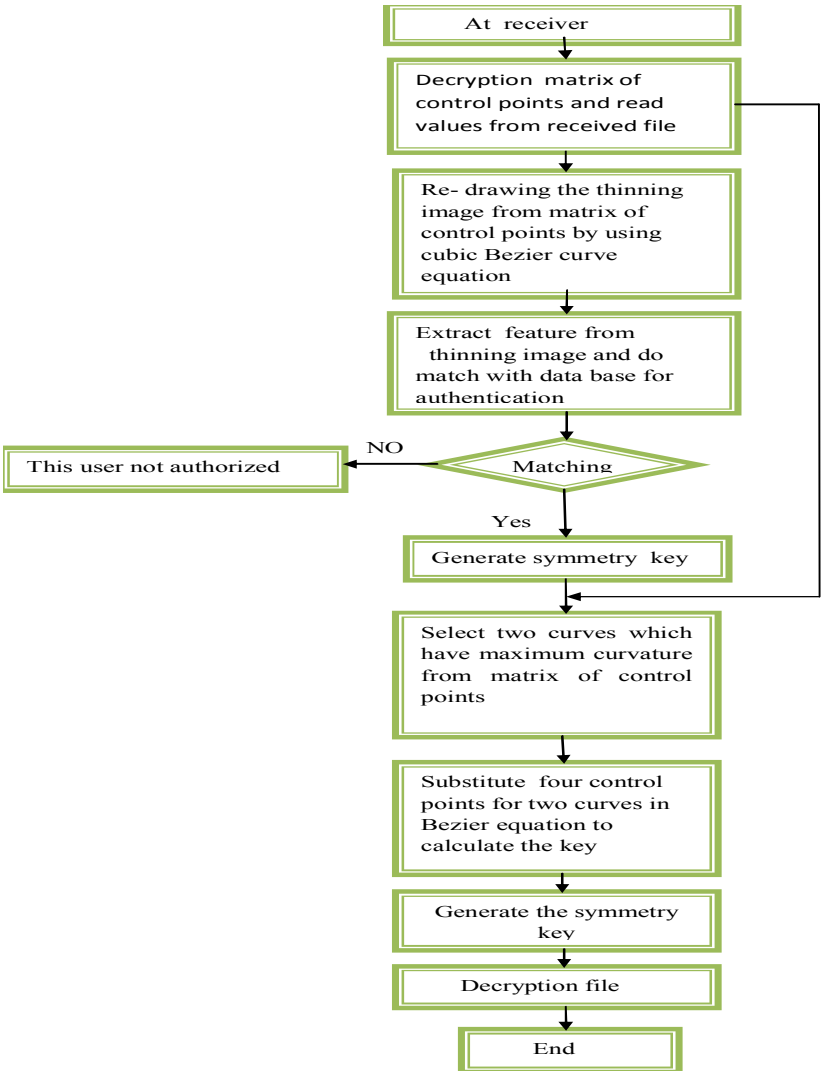
convert *binary number of the key in Q[j] to hexadecimal form and put the key in 4×4 matrix that consider as key.*

Encryption *file information by using the key generated from fingerprint image by using AES algorithm and sends the encryption file with encrypted matrix of control points for thinning image in the same file on network.*
End algorithm

2.3 Decryption Stage

When receiver receives file that contains encrypted matrix of control points for thinning fingerprint image and encrypted information from sender. The first step at receiver is decryption matrix of control points using AES algorithm with key generated from random generator which take the input(seed) from the first character and last character from encrypted file and re-drawing the thinning image of sender from matrix of control points using cubic Bezier curve equation .

The second step do matching if the result of matching was true receiver repeat the same steps of algorithm for generated same key to decryption information file, but if the result of matching is false the program send message for sender to tell him re-send the file once more. Figure(8) explains decryption steps.



Fig(8) Block diagram explain steps of decryption stage

- ***Algorithm of decryption stage***

A- R- drawing thinning of fingerprint image
Input: *encrypted matrix of control points.*
Output: *thinning of fingerprint image.*
Begin
Decryption *matrix of control points.*
Read *the matrix of control points.*
Using *Bezier curve to drawing ridges of image from matrix of points.*
Matching *the result image with data base for authentication.*
End
B*-generate symmetry key*
Using same steps in encryption stage to generate the same key.
C-*decryption data file.*
By using AES encryption algorithm with same key generated from stage B to decryption data file.
End

3-The Results and Evaluation

After proposed system is applied on, for example, fingerprint image with size (401× 473) which shown in Figure(11), we get the following results as shown in table(2) and Figures 9 and 10 respectively. The example below explains the steps of proposed system applied on the input fingerprint to generate the encryption key. After doing preprocessing and get on thinning of fingerprint, we will visualizing the segments of ridges by cubic Bezier curve and store the result of control points in matrix. The algorithm randomly selects the control points for two curves which have maximum degree of curvature from matrix of control points.

The index number of four control points for first curve in matrix is (155).

The coordinates of control points for first curve selected depend on degree of curvature are:

[p_0=(146,186), p_1=(180,172) , p_2=(218,177) , p_3=(252,190)].

These points Substitute in cubic Bezier curve equation, as below:

$p(t)_x$= $(1-t)^3$ 146+ 3$(1-t^2$ t 180 + 3(1-t) t^2 218 + $t^3$252 ,

equation after substitute x values.

$p(t)_y$=$(1-t)^3$ 186+ 3$(1-t)^2$ t 172+ 3(1-t) t^2 177+ $t^3$190 ,

equation after substitute y values.

Index number of four control points for second curve in matrix is (142).

The coordinates of control points for second curve selected depends on degree of curvature are:[p_0 =(106,311),

p_1 =(120,284), p_2 =(155,255) , p_3=(180,243)].

These points substitute in cubic Bezier curve equation, as below:

$p(t)_x = (1-t)^3\ 106 + 3(1-t)^2\ t\ 120 + 3(1-t)\ t^2\ 155 + t^3\ 180$,

equation after substitute x values.

$p(t)_y = (1-t)^3\ 311 + 3(1-t)^2\ t\ 284 + 3(1-t)\ t^2\ 255 + t^3\ 243$,

equation after substitute y values.

When we select the initial value of parameter (t= 0.017), we got the random values of p(t) for x and y as depicted in table(2).

Table (2) Shows the random values of (x) and (y) for two Bezier curves selected from matrix.

Random values of p(t) for x and y for two segments of ridge	Select four digits at most right of decimal number	Convert each two digit of decimal number to binary form	No of Bits
• X= 147.737428696 Y=185.302418957 • X =149.4815577568 Y= 184.6374599656 • X=151.2321500792 Y=184.0047977839	8696 8957 7568 9656 0792 7839	10101101100000 1011001111001 101011100100 1100000111000 01111011100 101110100110	64 bits
• X =106.7320544697 Y=309.6213593347 • X =107.4996095576 Y=308.2398100776 • X=108.3017500819 Y=306.8559144369	4697 9347 9576 0776 0819 4369	1011101100001 1011101101111 10111111001100 01111001100 100010011 1010111000101	64bits

10101101100000101100111100110101110010011000001110000111011011001101110110000011011101101111101111110011000111001100100010011101

Figure(9): Total length of Key (128) bits in binary form

AD	82	CF	35
C9	83	87	B9
BB	0D	DB	EF
CC	79	91	3A

Figure(10): The key in hexadecimal form

Fig (11.a) represents the original fingerprint, Fig(11.b) refers to apply Gabor filter, Fig(11.c) represents feature extraction and Fig(11.d) illustrates the locations of two curves in image.

a-Original fingerprint *b- After apply Gabor filter* *c- Features extraction* *d- Locations of two curves*

Fig(11):Four images illustrate do preprocessing for fingerprint and select two curves using cubic Bezier curve.

3.1 The Key Randomness test

The randomness of key which generated by this method is pass the randomness statistical testes as (Arderw *et al.,* 2001):

1-The Frequency test.

2-The Serial test.

3-The run test.

To calculate the P-value for the generated (128) bits key in figure(9), we apply the steps below:

1-For **frequency test** we are use the formula: $X^2=\frac{(n_0 - n_1)^2}{n}$. Good sequence must be $0< X^2< 3.84$

Where n_0 = number of zeros in key sequence, n = total number of key sequence

n_1 =number of ones in key sequence.

From figure(9), n_0 =57 , n_1 = 71

$X^2=\frac{(n_0 - n_1)^2}{n} = \frac{(57-71)^2}{128} = 1.531$, p-value= $1.531< 3.84$ (pass).

- **For frequency Mono bit test,** we do the following:

1-convert the zeros to(-1) and the ones to(+1) in key sequence and added together to produce S_n=x1+x2……xn.

2- compute the $S_{obs}=\frac{S_n}{\sqrt{n}}$.

3-compute P-value= erfc ($\frac{S_{obs}}{\sqrt{S_n}}$) .

When apply the steps above on the key sequence we get on the result as bleow:

S_n= 11 , $S_{obs}=\frac{S_n}{\sqrt{n}}=\frac{11}{\sqrt{128}}$ =0.972 , P-value= erfc ($\frac{S_{obs}}{\sqrt{S_n}}$) =$\frac{0.9723}{\sqrt{11}}$ = 0.29 > 0.01 (pass).

- **For frequency test within block** frequency(M ,n), where:(M) the length of each block, (n) the length of key sequence, N number of blocks, and S_n key sequence**,** we do the following:

N=$\frac{n}{M}$ if M=8 that mean N = $\frac{128}{8}$ =16 , divided the sequence of key for 16 block each block have 8bits.

1- Determine the proportion π_i of ones in each M-bit block where π_i =$\frac{number\ of\ ones\ in\ block\ i}{M}$
2- Compute the X^2(obs) = 4 M$\sum_{i=1}^{N}(\pi_i-\frac{1}{2})^2$ when substitute M=8 , N=16 and calculate π_i for each block the value of X^2(obs)=15.5
3- Compute p-value= igamc ($\frac{N}{2}$,$\frac{X^2(\text{obs}}{2}$) , p-value= igamc ($\frac{16}{2}$,$\frac{15.5}{2}$) (pass).

2- The Serial test

the following steps explain this test:

1- Calculate the number of occurrences of 00,01,10,11 and number of ones and zeros in key sequence.
2- Apply the formula : $X^2=\frac{4}{n-1}(n00^2+n01^2+n10^2+n11^2)-\frac{2}{n}(n1^2+n0^2)+1$, for good sequence X^2 <=5.99

Where n =total length of key sequence = 128bits

When apply this steps on the key generated above in fig(9) we get on the result as below:

$n00$= 27, $n11$= 41 , $n01$=29 , $n10$= 30 , $n0=57$, $n1=71$.

$X^2=\frac{4}{128-1}(27^2+29^2+30^2+41^2)-\frac{2}{128}(57^2+71^2)+1$ = **2.21 < 5.99** (pass).

3-The Run test

$\pi=\frac{71}{128}=0.515$,$\tau=\frac{2}{\sqrt{n}}=\frac{2}{\sqrt{128}}$ =0.176

$|\pi-\frac{1}{2}|=|\frac{71}{128}-\frac{1}{2}|$=0.054< τ= 0.176

$$\text{p-value}=\left[\frac{v_{n(obs)}-2n\pi(1-\pi)}{2\sqrt{2n}\times\pi(1-\pi)}\right]$$

$$=\left[\frac{75-2\times128\times\frac{71}{128}(1-\frac{71}{128})}{2\times\sqrt{2\times128}\times\frac{71}{128}\times(1-\frac{71}{128})}=\frac{11.84}{7.88}=1.5\right]$$

p-value = 1.5 > 0.01 (pass).

4- Conclusion

This approach use the biometric features of fingerprint with cryptography for information secrecy and authentication on networks. This method overcomes on several problems that associated with traditional cryptography, because it provides a practical and secure method to integrate the fingerprint biometric into cryptographic applications. The key generation by this method depends on the ridges shape of fingerprint and on the flexibility of Bezier curve to visualizing these ridges. The proposed key is generated depends on the curvature degree of ridge which increases the randomly distribution of bits in key sequence. The algorithm can update this key periodically via a re-change the parameter of (t) when the ratio (t) takes value between zero and one. This approach is using AES algorithm with key 128 bit as length to encryption blocks of data before send it with encrypted matrix of control points for fingerprint image on network. Key exchange is a weak point in AES algorithm, this method uses efficient and secure method to exchange the key and overcome on this problem. There are No need to store the key in database, the symmetry key generated randomly and directly from fingerprint. This work can used in many applications which need level of security in our life such as bank transfer.

References

Anil.K.Jain, Patrick Flynn, Arun A. Ross, 2007. "**Handbook of biometrics**" . USA. ISBN13:978-0-387-71040-2, pp:12.

Arderw *et al.,* 2001. NIST, " **Astatistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Application**". http://csrc.nist.gov/publications/pubsSps.html#800-22 (Accessed on April 2010) .

David .S, 2005. "**Curves and Surfaces for Computer Graphics**". Springer - Verlag . ISBN: 0-387-24196-5, pp: 176.

Gunjan. G, Rama. C, 2012. "**Review on Encryption Ciphers of Cryptography in Network Security**". International journal of advanced research in computer science and software engineering, 2(7):211-213. www.ijarcsse.com.

Henry. C. lee, R.E.Gaensslen, 2001. "**Advances in Fingerprint Technology**" .2nd Ed. crc. press, USA. pp:299-300. ISBN:978-1-4200-4134-7.

Lukasz Wieclaw, 2009. "**A Minutiae-based Matching Algorithms in Fingerprint Recognition System**". Journal of medical informatics and technologies, 13: 65-72. http://www.academia.edu/2508970.

Nalini K. Ratha, Venu Govindaraju, 2008. "**Advances in Biometrics Sensors, Algorithm and Systems**". Springer-verlag London.ISBN:978-1-84628-920-0, pp:17.

Peter *et al.,* 2005. "**Automated Fingerprint Identification System(AFIS)",** Elsevier Academic press .USA. ISBN 13:978-0-12-418351-3, pp:84.

Rupam K. S , 2012 . "**Generation of Biometric Key for use in DES**" . International Journal of Computer Science Issues, 9(6):312-315. http://ijcsi.org/papers/IJCSI-9-6-1-312-315.

Raymond Thai, 2003. "**Fingerprint Image Enhancement and Minutiae Extraction**". Technical Report, the university of western Australia, pp:38-40.

Vani perumal, Jagannathan Ramaswamy, 2009. "**An Innovative Scheme For Effectual Fingerprint Data Compression Using Bezier Curve Representations**". International journal of Computer Science and Information Security, 6(1):149-157. http://arxiv.org/ftp/arxiv/papers/0911/0911.0499 .

William Stallings, 2006. "**Cryptography and Network Security: Principles and Practice**" . Prentice Hall ,pp:411-415. ISBN 10:0-13-609704-9.

Wesam Bhaya, Wael Mahdi, 2014. "**Fingerprint Security Approach for Information Exchange on Networks**". In Publishing.European Journal of Scientific Research.

Zdenek. R , Vaclav. M, 2000. "**Biometric Authentication Systems. Technical Report, Faculty of Informatics**" , Masaryk university, pp:44. http://www.fi.muni.cz/reports/files/older/FIMU-RS-2000-08.pdf.