ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol 2., Issue 7, July 2013

CRYPTOGRAPHIC SYSTEM FOR FINGERPRINT IMAGE USING CHAOTIC SEQUENCE GENERATOR

Bhavana S[1] Dr. Lalitha Y. S[2]

PG Student [LDE], Dept. of ECE, Appa Institute of Engineering and Technology, Gulbarga, Karnataka, India[1]

Professor, Dept. of ECE, Appa Institute of Engineering and Technology, Gulbarga, Karnataka, India [2]

ABSTRACT: Here we are going to achieve secure for the finger print images by using symmetric method. This symmetric finger print image encryption is a combination of scrambling and confusion process. It also include the chaotic map in which scrambling will be used to identify address of the finger print image pixels, and bit -level permutation is used for confusion process so it will enhance the security. Encryption scheme possesses large key space to resist brute force attack, malicious attack like cropping, noising and possesses good statistical properties to frustrate statistical analysis attacks**.**

Keywords: Image encryption, Fingerprint image, Chaotic map, Biometric authentication.

I.INTRODUCTION

In common usage chaos means a state of disorder. In chaos theory it is defined more precisely. In dynamical system chaos will be having property like sensitive to initial conditions. As there is a rapid development in a digital image processing and network communication, electronic publishing and wide spread dissemination of digital multimedia data has been communicated over the internet and wireless networks. Where to avoid the leakages from image/video attacker, we use two methods in biometric authentication.

Biometric authentication refers to verifying individuals based on their physiological and behavioural characteristics. The two methods which it includes are one is digital watermarking which is used for information hiding. And other is encryption which includes conventional encryption and others such as chaotic encryption. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. These above are helpful to avoid from leakages. As in the centralized matching scheme, finger print images are collected or captured at the local site and will be sent to the central point through the network. Where here we will expect the finger print which will be in biometric technologies should be unique across the individuals and across fingers of the same individuals. This biometric technology has come from recent years. Here even identical twins having similar DNA, are expected to have different finger prints. This central matching scheme is also using in ATM banking.

In recent years, a number of digital chaotic cryptographic schemes have been proposed. Fingerprint image encryption algorithm based on combination of scrambling and confusion processes was proposed. Chaotic map is used for the scrambling the addresses of the fingerprint image pixels while bit-level permutation is used to confuse the values of image pixels so as to enhance the security [1]. Several one-dimension chaotic maps are used to generate pseudo-random sequences, which are independent and approximate uniform. After a series of transformations, the sequences constitute a new pseudo-random sequence uniformly distributing in the value space, which covers the plaintext by executing Exclusive-OR and shifting operations some rounds to form the cipher.

II. THE PROPOSED ENCRYPTION AND DECRYPTIONOF ALGORITHM FOR FINGERPRINT IMAGES

Here there is a need to get the pixel information of the fingerprint image. The fingerprint image contains R,G,B pixels getting the information of the R,G,B is important. For the simplicity first only one colour is taken into account these pixel values of the RGB is converted into 8-bit binary form.

A. Encryption of fingerprint image

To encrypt the fingerprint image two times scrambling is done. One is address scrambling and other one is 2-D scrambling. Address scrambling is done by taking chaotic sequence generator 1 and 2-D scrambling is done by chaotic sequence generator 2.

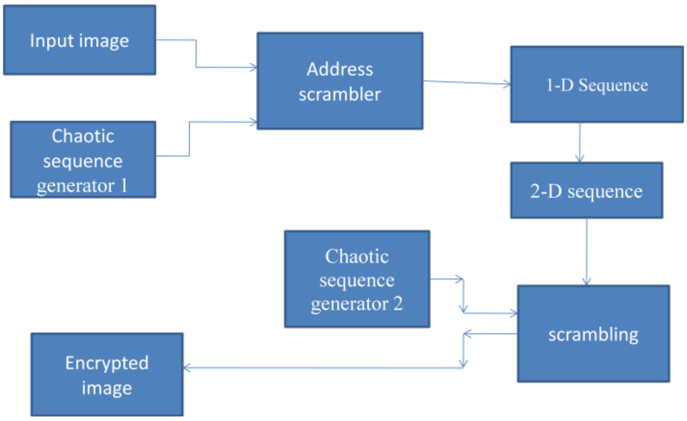


Figure 1: Encryption of finger print image

1] Chaotic sequence generation:

Chaos is a definite pseudo-random process produced in nonlinear dynamical systems. It is non-periodic extremely sensitive to the initial condition. In general, the chaotic system model is given as:

$$X(k+1) = f(\mu, X_K) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

f is the nonlinear function, μ is control parameter, X_k is real number.

Sequence can be generated by using the multipliers. For the first multiplier one input is constant and other is iteration from 0 to 255.This multiplier output is given as the input for next multiplier. The other input will be random number between 0 and 1.after getting the multiplication it will produce long random sequence. As shown in figure2.

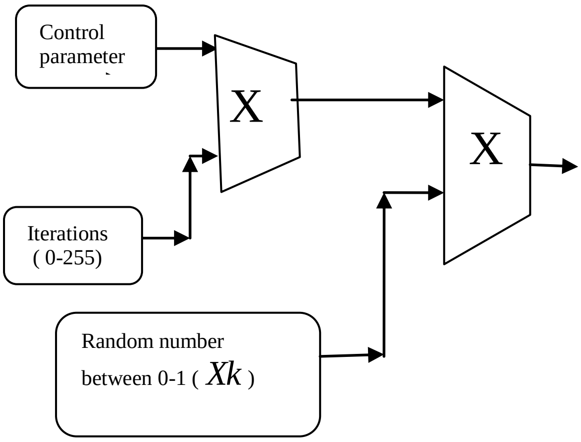


Figure 2: Block diagram of chaos generator

2] Address Scrambling:

Address scrambling is between chaotic sequence generator 1 and the input image. Input image will be fingerprint image this image pixel values are arranged according to the chaotic sequence generator 1.That is the position of image pixel are changed. This method of scrambling is called address scrambling.

3] Conversion of 2-D sequence:

Address scrambling output sequence will be in 1-D sequence so for the second scrambling the conversion of 1-D to 2-D is needed so conversion is done.

4] 2-D scrambling:

This scrambling is done between 2-D sequence and chaotic sequence 2.so that position of sequence is changed according to the chaotic sequence 2.

5] Encrypted image:

After scrambling the sequence what we will get is called encrypted image.

B. Decryption of Fingerprint Image

To get back the original image 2 times descrambling is done. One is 2-D descrambling and other is address descrambling.2-D scrambling is done by taking chaotic sequence 2 and address descrambling is done with the help of chaotic sequence generator 1as shown in figure 3.

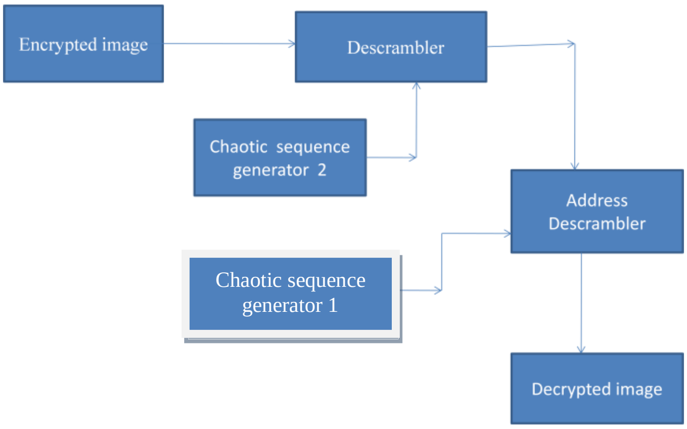


Figure 3: Decryption of Fingerprint Image

1] 2-D Descrambling

The input for this descrambling will be encrypted image and chaotic sequence generator 2.so gets back the input for address descrambling this 2-D sequence is rearranged according to the sequence generator 2.

2] Address descrambling:

After getting the descrambling output sequence that sequence is given as a input for address descrambler. Then according to the chaotic sequence generator 1 the position of the pixels are changed that sequence will be in 2-D.

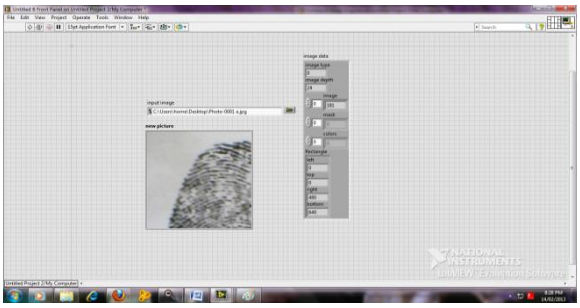
3] Decrypted image:

The output of the address descrambling is called the decrypted image. that will be in 2-D called original fingerprint Image.

III SYSTEM IMPLEMENTATION

Implementation is carried out in LABVIEW. Implementation of pixel value extraction, sequence generator, encrypted image, decrypted image.

A] Pixel Value Extraction:


Untitled 6 Front Panel on Untitled Project 2/My Computer *

input image
C:\Users\home\Desktop\Photo-0001 a.jpg

new picture

image data
image type 0
image depth 24
image 0 181
mask 0
colors 0
Rectangle
left 0
top 0
right 480
bottom 640

Untitled Project 2/My Computer

1] Address Scrambling:

Address scrambling is between chaotic sequence generator 1 and the input image. Input image will be fingerprint image this image pixel values are arranged according to the chaotic sequence generator 1.That is the position of image pixel are changed. This method of scrambling is called address scrambling.

2] Conversion of 2-D sequence:

Address scrambling output sequence will be in 1-D sequence so for the second scrambling the conversion of 1-D to 2-D is needed so conversion is done.

3] 2-D scrambling:

This scrambling is done between 2-D sequence and chaotic sequence 2.so that position of sequence is changed according to the chaotic sequence 2.

4] Encrypted image:

After scrambling the sequence what we will get is called encrypted image.

.

B. Decryption of Fingerprint Image:

To get back the original image 2 times descrambling is done. One is 2-D descrambling and other is address descrambling. 2-D scrambling is done by taking chaotic sequence 2 and address descrambling is done with the help of chaotic sequence generator 1as shown in figure 3.

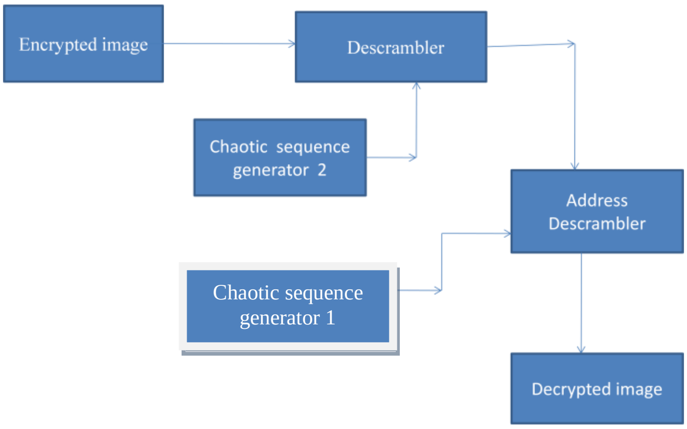


Figure 3: Decryption of Fingerprint Image

1] 2-D Descrambling

The input for this descrambling will be encrypted image and chaotic sequence generator 2. so get back the input for address descrambling this 2-D sequence is rearranged according to the sequence generator 2.

2] Address descrambling:

After getting the descrambling output sequence that sequence is given as a input for address descrambler. Then according to the chaotic sequence generator 1 the position of the pixels are changed that sequence will be in 2-D.

3] Decrypted image:

The output of the address descrambling is called the decrypted image, that will be in 2-D called original fingerprint image.

III SYSTEM IMPLEMENTATION

Implementation is carried out in LABVIEW. Implementation of pixel value extraction, sequence generator, encrypted image, decrypted image.

A. Pixel Value Extraction:

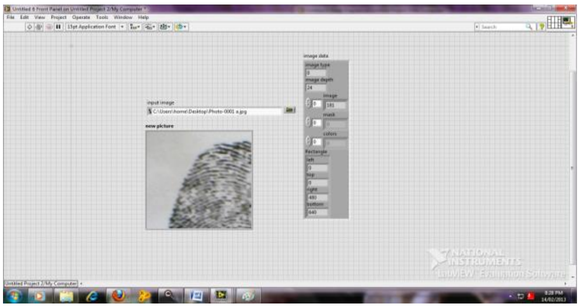

input image
C:\Users\home\Desktop\Photo-0001 a.jpg
new picture
image data
image type
0
image depth
24
image
0
181
mask
0
0
colors
0
0
Rectangle
left
0
top
0
right
480
bottom
640

Figure 4. Front panel for pixel value extraction

The front panel for pixel value extraction is shown in figure 3 which shows the pixel value of the fingerprint image. The input for this is fingerprint image .The JPEG block reads a JPEG file and creates the data necessary to display in a picture control.

B. Sequence generator:

The front panel for sequence generator is shown in figure 5. which shows the long sequence which will be in random in nature. The input for this will be random value between 0 and 1.and other will be control parameter.

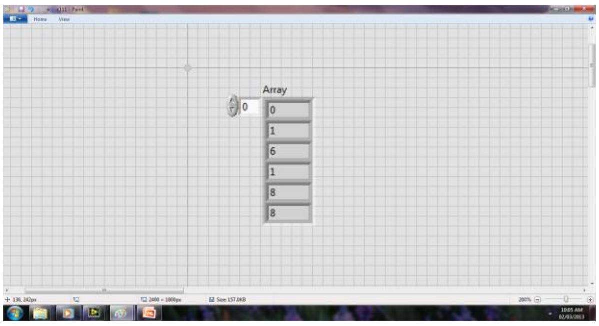

Array
0
0
1
6
1
8
8

Figure 5. front panel for Sequence generator

C. Encrypted image:

The Figure 6 shows the output for the encrypted image. After doing two times scrambling with chaotic sequence generators the original image is converted into encrypted image.

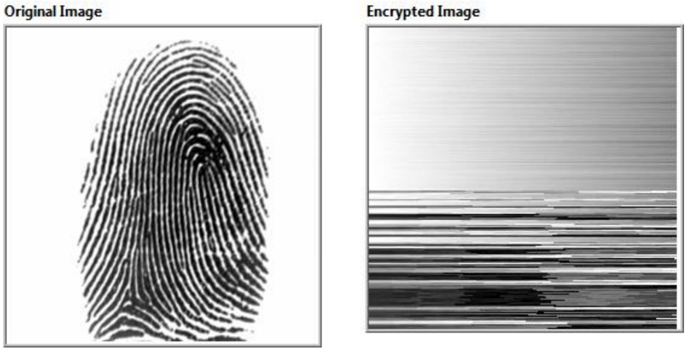
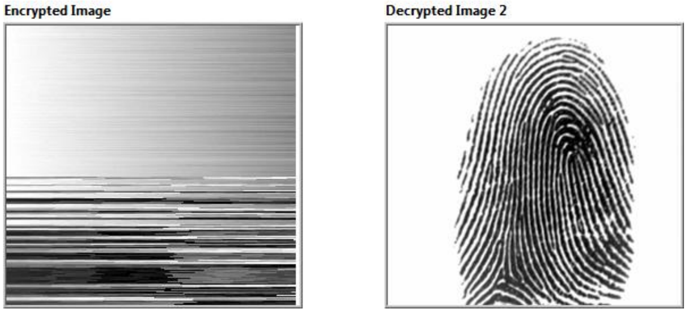


Figure 6: Front panel for encrypted image.

D. *Decrypted image:*


Encrypted Image

Decrypted Image 2

Figure 7 Front panel for decrypted image

Figure 7 shows Front panel for decrypted image. After doing 2-D descrambling and address scrambling with the help of chaotic sequence generators the decrypted image is taken.

IV CONCLUSION

For the fingerprint image encryption and decryption the pixel value of image can be taken. Here the algorithm is based on combination of scrambling and confusion process. For Chaotic map chaotic sequence generation is done and it is used for the scrambling the addresses of the fingerprint image pixels.

REFERENCES

[1] Ginni Chawla *FPGA Implementation of Chaotic State Sequence Generator for Secure Communication* Department of Electronics Engineering, Aligarh Muslim University, Aligarh 202 002, India.
[2]. Zhijie Jerry Shi and Ruby B. *Implementation Complexity of Bit Permutation Instructions* Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA.
[3] Behnia S, Akhshani A, Mahmodi H, and Akhavan *A novel algorithm for image encryption based on mixture of chaotic maps*, Chaos, Solutions & Fractals, vol. 35, pp. 408-419, 2008.

[4] Wang XY, and Yu Q, *A block encryption algorithm based on dynamic sequences of multiple chaotic systems*, Common Nonlinear Sci Numer Simul. vol. 14, pp. 574-581, 2009.Chaos, Solutions & Fractals, vol. 35, pp. 408-419, 2008.

[5] LIU Xiangdong, Zhang Junxing, Zhang Jinhai, He Xiqin *Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation*. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008.

BIOGRAPHY

Dr. Lalitha Y. S was born on July 7, 1969 in India. She **received** B.E degree in Electronics and Communication Engineering and M.E. degree in Power Electronics from Gulbarga University Gulbarga, India, in 1991 and 2002 respectively. She is working as Professor in Appa Institute of Engineering & Technology, Gulbarga, India. Her research interests include image Processing, Wavelet Transform coding. She attended Eight National Conferences and three International Conferences. She has published eight International Journal papers.

Bhavana S. Was born on December 5, 1989 in India. She completed B.E degree in Information Science and Engineering under VTU University in 2007-2011. Submitted dissertation in M. Tech (Digital Electronics) in Appa Institute of Engineering &Technology, Gulbarga under VTU Belgaum University. This is the first Journal paper on “**Cryptographic System For Fingerprint Image Using Chaotic Sequence Generator**