ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Analysis of Chaotic Image Encryption based on DPFrFT and Biokeys

Jenny Joseph, Josy Elsa Varghese

Pursuing M.Tech, Dept. of CSE, Caarmel Engineering College, MG University, Kerala, India

Assistant Professor, Dept of CSE, Caarmel Engineering College, MG University, Kerala, India

ABSTRACT: A new biometric inspired chaotic image encryption technique is proposed. The idea behind the proposed technique is to capture the biometric image of the sender and then the image is pre-processed to estimate the initial seed of nonlinear chaotic map and feature vector. This feature vector is used to obtain the biometrically encoded bit stream. The original image is randomized using the random matrix generated by the iteration of Nonlinear Chaotic Map. Then the randomized image is encrypted using Dual Parameter Fractional Fourier Transform, Hessenberg Decomposition and the feature vector to get the randomized encrypted image. Then inverse Dual Parameter Fractional Fourier Transform is performed on the randomized encrypted image to get the encrypted image. The encrypted image can be decrypted by using the reverse process of encryption. To analyse the randomness of different chaotic maps, the above described method can be carried out using 1D, 2D and 3D chaotic maps and a comparative study on them is conducted. Theoretical analysis and computer simulations have shown that the proposed technique is efficient and secure.

KEYWORDS:Biometrics, Nonlinear Chaotic Map, Dual Parameter Fractional Fourier Transform (DPFrFT), Hessenberg Decomposition, 1D, 2D and 3D chaotic maps.

I. INTRODUCTION

Due to the recent developments in digital distribution networks, the security of multimedia data against different types of forgeries and attacks has become extremely important. The most possible solution is to use Cryptography. Generally Cryptography is used to protect the privacy of information which is communicated over open channels. The Cryptographic techniques are generally considered as the best method of data protection against passive and active fraud. Nowadays cryptographic techniques are based on number theoretic or algebraic concepts. The chaotic systems are nonlinear system, which can exhibit random behaviour and are considered to be complex. However, this random behaviour has no stochastic origin. It is considered as the result from the defining deterministic processes. Recent researches have been made to use chaotic systems for communication to increase security and privacy of the data. The highly unpredictable and random-look nature of chaotic signals makes it more suitable to use in novel (engineering) applications.

Chaotic algorithms and cryptographic algorithms have certain similar properties i.e. both are sensitive to a change in initial conditions and parameters, also they exhibits random behavior and has unstable periodic orbits having long periods. The encryption rounds of a cryptographic algorithm lead to the confusion and diffusion properties of the algorithm. But in the chaotic maps, the iterations of a chaotic map are used instead of encryption rounds.

However, the requirements for encrypting the multimedia data are different because it is highly redundant, has large volumes and has the characteristics of amplitude-frequency. Hence researchers try to develop specific encryption techniques considering the characteristics of multimedia data. So they make use of Biometrics along with Cryptography. Biometrics has the potential to uniquely identify a person based on his/her physical or behavioural characteristics. An example for cryptography combined with biometrics is a biometric-key system based on fingerprints reported earlier [3]. The system extract phase information from the fingerprint image using a Fourier transform and apply majority coding to reduce the feature variation. A method called biometric locking is used here, instead of generating a key directly from biometrics: A predefined random key is locked with a biometric sample by forming a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

phase-phase product. A genuine biometric sample can unlock this product. However, the biometric data is not very secret. People may leave their fingerprints everywhere. So in this proposed technique biometrics is combined with Dual Parameter Fractional Fourier Transform, Hessenberg Decomposition and Chaotic Map. Also to analyze the randomness of different chaotic maps, the basic method can be carried out using 1D, 2D and 3D chaotic maps.

The proposed technique allows a secure communication between two people, commonly known as Alice (owner) and Bob (receiver). First the biometric image of the sender is captured using an appropriate biometric scanner. The image is then pre-processed to estimate the initial seed for the Nonlinear Chaotic Map (1D/2D/3D) and to get the feature vector. For this purpose an efficient method is suggested. Now the keys in the proposed encryption technique, i.e. initial seed for Nonlinear Chaotic Map (1D/2D/3D), transform orders and angles are generated. Then the image is encrypted using DPFrFT, Hessenberg Decomposition and Feature Vector. The keys for the encryption are obtained from the biometrics of Alice and therefore Bob also need the same biometrics data to decrypt the image. The randomness of different chaotic maps can be analyzed using Lyapunov exponent and Entropy.

The rest of the paper is organized as follows. Section 2 formulates the motivation and overview. Section 3 shows the system architecture. Section4 describes the methodology for key generation, encryption and decryption. Section 5 concludes the work.

II. MOTIVATION & OVERVIEW

Cryptography is considered to be a powerful solution against security attacks and it is the science of protecting the confidentiality of data that is transmitted over channels. However, cryptographic security has an authentication step that requires long pseudo-random keys, which are nearly impossible to keep in mind. Also many people may use identical keys or password for a number of applications and as a result attacking one system lead to the breaching of many others. This makes the work of an attacker easy thereby reducing the general security of the data being protected.

In order to provide security for the keys associated with the encryption process, many biometrics inspired multimedia encryption techniques has been proposed. The combination of biometrics and cryptography might have the ability to connect a person with a digital signature that he had created. Hao et al. [5] presented a realistic and secure way to incorporate the iris biometric into cryptographic applications. It focused on the error patterns within iris codes i.e. burst errors and random errors and developed a two-layer error correction codes namely, Hadamard and Reed-Solomon codes. Through the auxiliary error correction data the key was produced from the iris image of the subject and can be saved in a tamper-resistant token like a smart card.

The social acceptance of biometric data is an important factor for the success of biometric inspired cryptography. Many people feared that the biometric data has been misused so they become reluctant to use such systems. So the proposed technique tries to strengthen the security by combining biometrics with DPFrFT and chaotic cryptography.

Chaotic cryptography describes the use of chaos theory, which is a dynamical phenomenon, in a cryptographic system to perform different cryptographic tasks. An efficient way for the fast and highly secure image encryption has been suggested by Chaos based algorithms. A remarkable characteristic of chaotic systems is their randomness, unpredictability and capability of producing quite complex patterns of behavior. Chaotic dynamical systems can provide simple mechanisms to generate deterministic pseudo randomness. They can use deterministic NLDS to produce the deterministic pseudo-randomness which is required in cryptography. Moreover, NLDS are able to produce complex patterns of evolution. This gives the algorithmic complexity to chaotic systems.

Motivated by the application of chaos combined with biometrics a biometric inspired multimedia encryption technique using Dual Parameter Fractional Fourier Transform, Hessenberg Decomposition and Nonlinear Chaotic Map is proposed here. Dual Parameter Fractional Fourier Transform is a new technique in the definition of Fractional Fourier Transform. DP-FrFT is more time efficient than FrFT. DP-FrFT provides better results for the applications that needs randomness. Hessenberg decomposition is the factorization of a general matrix A by orthogonal similarity transformations into the form

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

$$A=QHQ^T \quad (1)$$

where Q is an orthogonal matrix, Q^T is the transpose of Orthogonal matrix Q and *H* is an upper Hessenberg matrix, meaning thereby hij = 0 whenever i > j + 1.

A chaotic map is a discrete-time dynamical system running in the chaotic state. The chaotic sequence $\{x_n: n = 0, 1, 2,\}$ can be used as a random number sequence and can be used to randomize the image. Here a nonlinear chaotic map is used to create digital sequence. The nonlinear chaotic map can be 1D, 2D and 3D chaotic maps.An example for 1D chaotic map [7] is the simple logistic map. The logistic map is defined as:

$$x_{n+1} = \lambda x_n(1 - x_n) \quad (2)$$

$\lambda \in [0,4], n = 0,1,$ .....The parameter λ and x_0 may represent the key.
An example for 2D chaotic map [7] is 2D Arnold's cat map. The 2D Arnold's cat map is given by:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n[5] \quad (3)$$

q is the position variable (0 < q < N) and p is the momentum variable, where $p_t = q_t - q_{t-1}$and n is dimension of image. Here $\begin{bmatrix} x \\ y \end{bmatrix}$ represents location of pixels before transform and $\begin{bmatrix} x' \\ y' \end{bmatrix}$ represents location of pixels after transform.
An example for 3D chaotic map is 3D Arnold's cat map. The 3D Arnold's cat map is defined as:

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} 1 & a & 0 \\ b & ab + 1 & 0 \\ c & d & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \bmod n[2] \quad (4)$$

Here $\begin{bmatrix} x \\ y \end{bmatrix}$ represents location of pixels before transform and $\begin{bmatrix} x' \\ y' \end{bmatrix}$ represents location of pixels after transform. The third parameter inserted is z which is given by z = (c*x + d* y + z) mod M. The randomness of these chaotic maps can be measured using Lyapunov exponent and entropy.

This method increases the security in such a way that the encryption keys in the proposed technique, i.e., initial condition for nonlinear chaotic map, transform orders, and angles for the Dual Parameter Fractional Fourier Transform are obtained from the biometrically encoded bit stream, which is generated from the biometrics of the sender. So the receiver also requires the same biometric data of the sender to decrypt the message.

III. SYSTEM ARCHITECTURE

The Fig 1 depicts the system model of the proposed technique. Here, first the sender takes the biometric image of the fingerprint, using an appropriate biometric scanner. The pre-processing of the image will give the initial parameter for iterating the chaotic maps and also the feature vector. The Iteration of the chaotic maps will generate a random matrix, which can be used to randomize the original image that he/she want to send. Using Dual Parameter Fractional Fourier Transform, Hessenberg Decomposition and the Feature Vector the randomized image is then encrypted to get the randomized encrypted image. Then inverse DPFrFT is performed on the randomized encrypted image to get the encrypted image.

At the receiver side perform Dual Parameter Fractional Fourier Transform on the encrypted image. Then apply Hessenberg Decomposition on the biometric image to get two orthogonal matrices. With the two orthogonal matrices the partially decrypted image can be generated. Apply inverse DPFrFT on the partially decrypted image to get the randomized decrypted image. Iterate the chaotic maps to get the random matrix. Undo the randomization of the randomized decrypted image to get the decrypted image.

.

The chaotic maps can be 1D/2D/3D maps. The randomness of the chaotic maps can be measured using two components Lyapunov exponent and Entropy. Entropy (H(m)) is a statistical measure of randomness. It measures the complexity of the chaotic system. It can be measured using the following formula:

$$H(m)= \sum_{i=0}^{2^N-1} p(mi)\log_2 1/p(mi) \quad (5)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

where p(mi) is the probability of message.

The Lyapunov exponent is a measure of sensitive dependence on initial condition. For a map to be chaotic, the Lyapunov exponent should be positive. It is calculated as:

$$\lambda(f, x) = \lim_{n\to\infty} \frac{1}{n} \log\left((f^n)'(x)\right) \quad (6)$$

where $(f^n)'$ is the derivative of nth iterate f^n. Using Lyapunov exponent and Entropy we can analyse the efficient chaotic map.

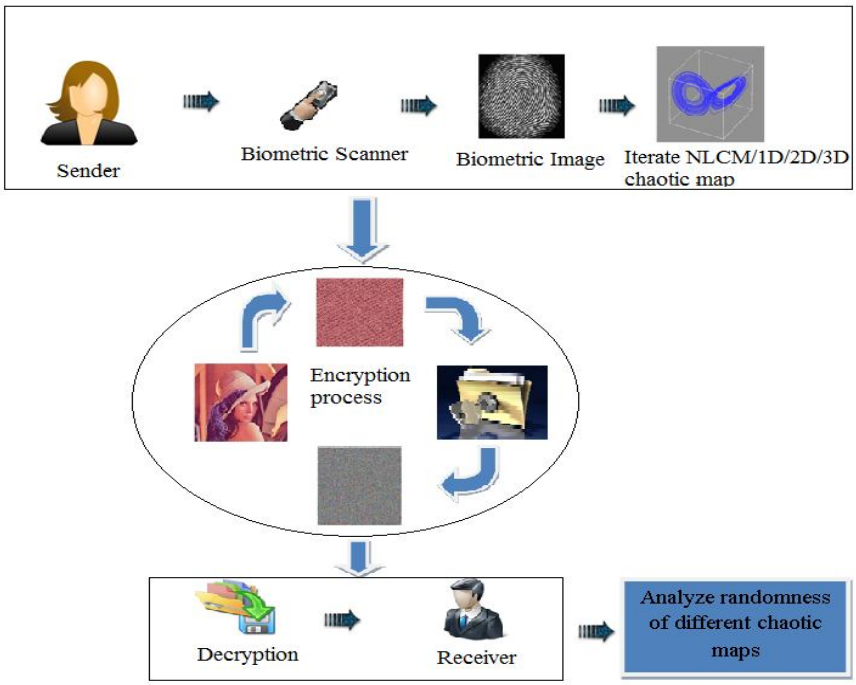

Fig 1: System Architecture

IV. METHODOLOGY

A. KEY GENERATION FROM BIOMETRICS

Let B=[b(i,j) ;b(i,j) $\epsilon\{0,1,\ldots,2^L-1\}$ be the biometric image having size M_1*N_1.The key generation process is as follows.First,randomly select two pixel values say p_x and p_y from B. Then take the difference between the two and divide it with total number of grey levels in the biometric image, i.e.

$$T = p_x - p_y / (2^L - 1) \quad (7)$$

Then from T the key for the chaotic map is calculated as follows:

$$K = (2^L * T) \bmod 1 \quad (8)$$

Then normalize the biometric image and then generate the feature matrix from it by the following equation:

$$F_B(i, j) = \begin{cases} 1, \text{ if } B(i, j) \geq T \\ 0, \text{ if } B(i, j) < T. \end{cases} \quad (9)$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Then arrange the feature matrix into the feature vector. To get the transform orders and angles for DPFrFT, partition feature vector into two equal segments F_{v1} and F_{v2}.The transform orders and angles can be calculated as follows:

$$\alpha_x=1/M_1\left(\sum_{i=1}^{\frac{l}{2}} F_{v1}(i)\right) \bmod (2^L-1) \quad (10)$$

$$\alpha_y=1/N_1\left(\sum_{i=1}^{\frac{l}{2}} F_{v2}(i)\right) \bmod (2^L-1) \quad (11)$$

$$\theta_x=\left(\sum_{i=1}^{\frac{l}{2}} F_{v1}(i)\right) \bmod 180 \quad (12)$$

$$\theta_y=\left(\sum_{i=1}^{\frac{l}{2}} F_{v2}(i)\right) \bmod 180 \quad (13)$$

B.MESSAGE ENCRYPTION

First, iterate the chaotic map (1D/2D/3D) using the key K generated from the above process. Then stack the chaotic sequence generated to get the random matrix (R_k). Using the random matrix randomizes the image by applying the following formula:

$$I_r(i,j) = \ln R_k(i,j) / \ln I(i,j) \quad (14)$$

Then perform DPFrFT on I_r as follows:

$$x_\theta^\alpha = R_N^\theta E^\alpha R_N^{\theta^T} x \quad (15)$$

Then distribute feature vector repeatedly into two arrays A_1 and A_2 of size M*M and N*N. Apply Hessenberg Decomposition on two arrays to get two orthogonal matrices Q_1 and Q_2 using the following formula:

$$A_1=Q_1HQ_1^T \text{ and } A_2=Q_2HQ_2^T \quad (16)$$

Then I_r is encrypted using the formula: $I_r^e = Q_1 I_r Q_2^T$ (17)

Then perform inverse DPFrFT on I_r^e to get the encrypted image as follows:

$$x = R_N^\theta E^{-\alpha} R_N^{\theta^T} x_\theta^\alpha \quad (18)$$

C.MESSAGE DECRYPTION

First, apply DPFrFT on the encrypted image. Then distribute the feature vector repeatedly into two arrays and apply Hessenberg Decomposition into it to get Q_1 and Q_2.Then the image is decrypted as follows:

$$J^d=Q_1^T J Q_2 \quad (19)$$

Then apply inverse DPFrFT on it. Then iterate the chaotic maps to get the random matrix (R_k).Then using R_k undo the randomization and decrypt the image using the following formula:

$$I^d(i,j)=e^{(\ln R_k(i,j)/J_d^r(i,j))} \quad (20)$$

V. CONCLUSION

To improve the security of multimedia data transmitted over open channels, a novel multimedia encryption technique is proposed, in which biometric and chaos are combined to increase the complexity and ensure better security. The keys are generated from the biometrics of the sender using an efficient process. Since a person will not lose his biometrics, the key become unique and more secure. The random sequence of chaotic map which is more complex and unpredictable also increases security. Also, the application of DPFrFT increases the randomness of the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

transformed signal. The randomness of different chaotic maps can also be measured. It is expected that 3D chaotic map has more randomness than 1D and 2D chaotic maps.Moreover; still the system may contain some loopholes that an efficient and skilled eavesdropper can exploit. So an efficient encryption technique with more and more complexity using the emerging technologies can be considered as a future work.

ACKNOWLEDGEMENT

We would like to thank reviewers for their helpful and constructive comments. We would also like to thank the faculties, the resource providers and the system administrator for the useful feedback and constant support.

REFERENCES

1. H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," Chaos, Solitons and Fractals, vol. 29, no. 2, pp. 393–399, Jul. 2006.
2. T. Gaoa and Z. Chen, "A new image encryption algorithm based on hyper-chaos," Phys. Lett. A, vol. 372, no. 4, pp. 394–400, Jan. 2008
3. F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Trans. Comput., vol. 55, no. 9, pp. 1081–1088, Sep. 2006
4. B. Chen and V. Chandran, "Biometric based cryptographic key generation from faces," in Proc. Digital Image Comput. Tech. Applicat., 2007,pp. 394–401.
5. S. V. K. Gaddam and M. Lal, "Efficient cancellable biometric key generation scheme for cryptography," Int. J. Netw. Security, vol. 11,no. 2, pp. 57–65, 2010
6. Gaurav Bhatnagar, and Q. M. Jonathan Wu," Biometric Inspired Multimedia Encryption Based on Dual Parameter Fractional Fourier Transform", Systems, Man, And Cybernetics: Systems, Vol. 44, No. 9, September 2014
7. Pawan N. Khade and Prof. Manish Narnaware, 3D Chaotic Functions for Image Encryption, IJCSI International Journal of Computer Science Issues, Vol. 9,Issue 3, No 1, May 2012