Chaos Based Cryptosystem for Images

[1]Akash Singh, [2]Anshika Rathi, [3]Megha Chauhan
Student
[1]Department of Computer Science, Inderprastha Engineering College -IPEC, Ghaziabad-201010, India
[1] akashsingh.skyhorn @gmail.com, [2]anshirathi@gmail.com, [3]meghachauhan30@gmail.com

Abstract— **The utmost negative impact of advancement of technology is an exponential increase in security threats, due to which tremendous demand for effective electronic security is increasing importantly. Since chaos fundamentals such as ergodicity and high sensitivity to initial conditions are directly connected with two basic properties of good ciphers: confusion and diffusion, so chaos has emerged as a new promising candidate for cryptography. Although significant research has been done on chaos based cryptography still there are some of problems basically speed, that restrict the application of encoding/decoding algorithms. In the proposed technique Arnold cat map & Hénnon map have been employed during permutation substitution process to design a spatial domain based chaotic cryptosystem& only single iteration have been performed to make it faster. Thorough performance, security and comparative analysis ascertains efficacy of the proposed technique.**

Index Terms—**Arnold Catmap, Henon Map, Encryption, Decryption.**

I. Introduction

With the development in science & technology over last few years internet has also emerged & so is the need to protect data to insure the authenticity of the data and protect system from security based attacks. From thousands of years Cryptography play a central role in information security and is becoming increasingly important as a building block for information security. It has long been used by militaries and governments to facilitate secret communication. During world war-II allies got a significant advantage over German due to their robust cryptosystem .Cryptography is a study of design of technique to provide secret communication as it protects the information transmission from the influence of adversaries who may present a threat to information. Cryptography is generally acknowledged the best method of data protection against passive and active fraud.

II. Related Work

Chaotic maps have properties like pseudorandom behavior, ergodicity, topological transitivity and sensitive dependence on initial conditions. Owing to these properties, different chaos based maps have been extensively used for the development of numerous block and stream cipher based cryptosystems. Ljupco Kocarev proposed public-key encryption algorithms based on iteration of one-dimensional Chebyshev chaotic maps and two-dimensional of torus auto Orphism chaotic map [1].Roy teeny introduced a public key encryption scheme based on an additive mixing with a chaotic nonlinear dynamics system [2]. Further Shuichi Aono presented a new cryptosystem by using iterations of an expansion chaotic map [3].Bi Dayuan added one more milestone when a public-key cryptosystems based on a defined feature of Chebyshev polynomials was proposed [4].LI Zhi-huimodified the existing algorithms on the Chebyshev polynomial chaotic to make them faster [5]. Mazen Tawfik introduced a new system, which can be implementing using the modified three beta-transform maps as a key exchange and three logistic maps as a private key and the Lorenz system for encryption and decryption process, for public key cryptosystem based on chaotic key management [6].

Guan et al. proposed to encrypt an image using confusion-diffusion mechanism using two distinct chaotic maps [7]. For an enhanced security level, Chen et al. generalized 2D Arnold cat map into 3D map before encrypting the image [8].Wong et al. proposed sequential add and shift operation to introduce diffusion into substitution process [9]. In contrast, Wang et al. proposed the use of multiple chaotic systems to generate a dynamic sequence and consequently encrypt the image [10].Sun et al. proposed the use of spatial chaos map to encrypt an image pixel by pixel, and permute the pixels in multiple directions of space [11].

III. Basic Concepts

Arnold cat map & Hénnon map have been employed during permutation substitution process to design a robust and fast, spatial domain based chaotic cryptosystem. The used techniques have been described in this section.

1) Arnold cat map

Arnold's cat map [12] is a chaotic map from the torus into itself.

Thinking of the torus T2as the quotient space R2/Z2Arnold's cat map is the transformation given by the formula

$$f:(x,y)\rightarrow(2x+y,x+y)\mathrm{mod}1 \qquad (1)$$

Equivalently, in matrix notation, this is

$$f\left(\begin{bmatrix}x\\y\end{bmatrix}\right)=\begin{bmatrix}2&1\\0&1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\mathrm{mod}1=\begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\1&1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}\mathrm{mod}1 \qquad (2)$$

That is, with a unit size equal to the width of the square image, the image is sheared one unit up, then one unit to the right, and all that lies outside that unit square is shifted back by the unit until it's within the square. Because digital image is composed of a set of finite gray values, the result that the transformation has periodicity can be obtained. The image becomes disordered after several cycles, but because of the inherited features of discrete dynamical system, the image will be transformed to the original state ultimately.

2) **Hénnon map**

The Hénon map [13] is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behavior. The Hénon map takes a point (xn, yn) in the plane and maps it to a new point

$$x_{n+1} = 1 - ax_n^2 + y_n \tag{3}$$

$$y_{n+1} = bx_n \tag{4}$$

The map depends on two parameters, a & b, which for the classical Hénon map have values of a=1.4 and b=0.3. For the classical values the Hénon map is chaotic. For other values of a & b the map may be chaotic, intermittent, or converge to a periodic orbit. An overview of the type of behavior of the map at different parameter values may be obtained from its orbit diagram

IV. THE IMAGE ENCRYPTION SCHEME

The proposed cryptosystem is based on permutation-substitution architecture, where the permutation operation is performed using Arnold cat map, while substitution is performed using Hénon map. The Arnold iterations (ni) and the initial condition of Hénon map (ti) form the security keys. The proposed encryption technique is illustrated in Fig. 1, and is described hereafter & decryption technique is illustrated in Fig. 2.

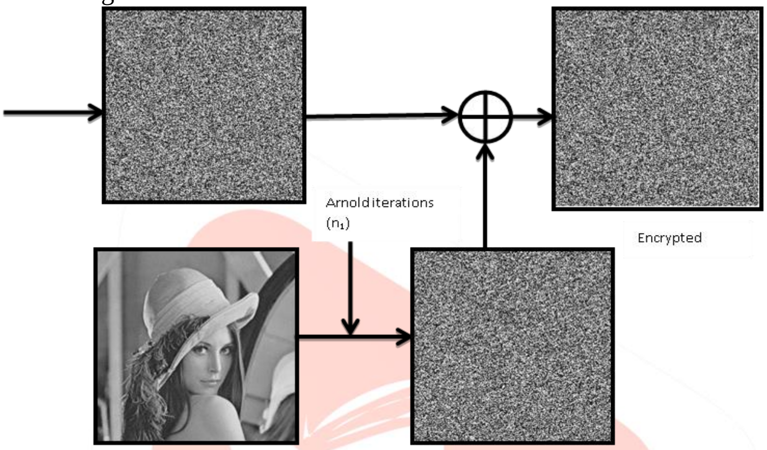


Figure 1 Encryption Process on Lena Image

ENCRYPTION TECHNIQUE

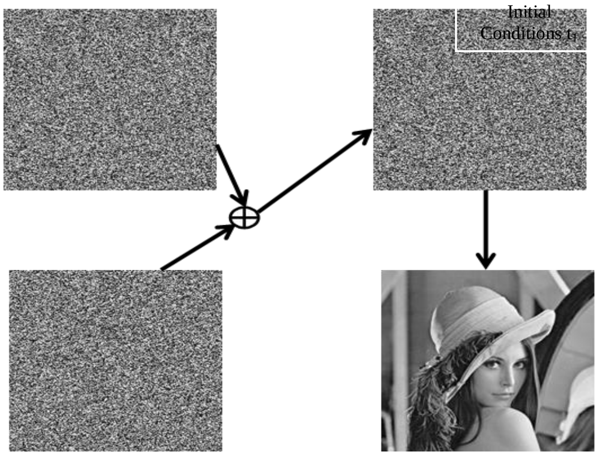
Let I (i, j) represents the original image of size N × N,

1. Apply $n_1$iterations of Arnold Cat map on the original image matrix I (i, j) to generate a completely scrambled image matrix S_1 (i, j).
2. Perform several iterations of the Hénon map, with initial condition t_1, to generate a chaotic matrix R_1 *(i, j)* of size $N \times N$. R_1 is formed by assembling the generated *x* and *y*, as alternate elements of the matrix.
3. XOR the scrambled image matrix S_1 (i, j) with the chaotic matrix R_1 (i, j), to obtain partially encrypted image matrix PC_1 (i, j).

This is mathematically expressed as

$$PC_1(i, j) = R_1(i, j) \oplus S_1(i, j).$$

DECRYPTING TECHNIQUE



Encrypted Image Decrypted Image

Figure 2 Decryption Process on Lena Image

For decryption of image process was carried out in reverse direction it required as many steps as for encrypting the image. Decrypting steps are:

1. Iterate the Hénon map with initial conditions t_1 to generate a chaotic output. Arrange the randomly generated data in an $N \times N$ matrix form, denoted by $R_1 (i, j)$.
2. XOR the chaotic matrix R_1 (i, j) with original encrypted image matrix EC (i, j), to generate the matrix E_2 (i, j).
$$E_2 (i, j) = R_2 (i, j) \oplus EC (i, j)$$
3. Scramble the obtained matrix E2 (i, j) with (y – n1) Arnold iterations to obtain decrypted image matrix PC (i, j). Here, y denotes the periodicity of Arnold cat map for the chosen image size.

It is very clear that the proposed algorithm is quite simple & provides good encryption as discusses further in result & discussion section.

V. Results & Discussions

Chaos based watermarking helps in achieving dual purpose of cryptography which is Cryptography security & perceptual similarity. Cryptography similarity includes security against various cryptanalytic attacks such as differential attacks, statistical attacks, key-related attacks etc., whereas perceptual security means that the human perception is not able to perceive the encrypted content. In this section, these evaluation metrics have been employed to analyze the performance and security level attained by the proposed encryption technique.

1. Perceptual security analysis and peak signal to noise ratio

The perceptual security of an encryption technique measures the amount of detail lost or retained in the encrypted image data. Subjective analysis of obtained results reveals completely incomprehensible images, as shown in Fig. 3 which indicates a high perceptual security level.

Objective evaluation is performed using peak signal to noise ratio, where original image and encrypted image are considered as signal and noise, respectively. It can be calculated using

$$PSNR = 20 \times log10255/\sqrt{MSE}\ dB$$

Where, MSE is Mean Square Error, given by

$$MSE = \frac{1}{MN \sum\sum(|I\ (i,j) - I'\ (i,j)|^2)}$$

I(i, j) and I’(i, j) denotes intensity of original image and encrypted image at pixel position (i, j), respectively. PSNR obtained for different test images is indicated in Table 1. Lower PSNR value obtained by all test images reflects the difficulty in retrieving the original image from its encrypted counterpart, without the knowledge of correct decryption key.

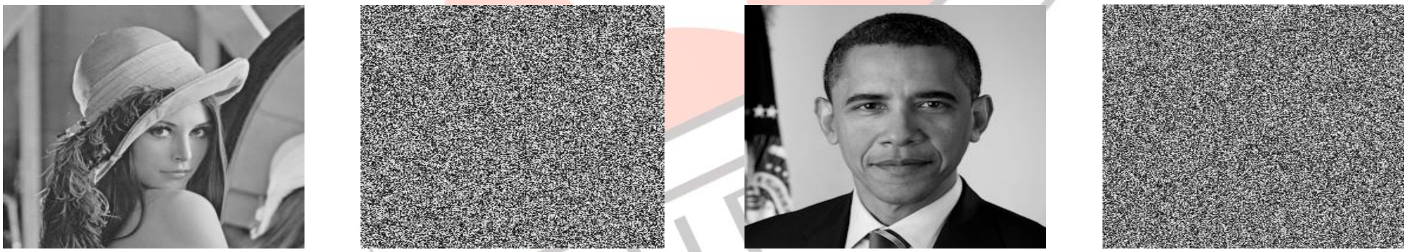


Figure 3 Encrypted Images for original images

Table 1 Table showing PSNR values for various images

Image	PSNR Value (dB)
Lenna	5.56
Obama	4.62
Pepper	5.61

2. Statistical attack analysis

In order to see the relationship between the data elements of original bit-stream & cipher code-stream, which is used in cryptanalysis to determine plaintext without the knowledge of decryption key or to substantially reduce the search space such that a brute force attack is feasible, and correlation coefficient of the original image and its encrypted counterpart has been analyzed.

As can be seen from the figure 4 that the histogram of cipher image is more or less uniform making it different from the pixels at each gray level of original image. This signifies the dissimilarity between the two images.

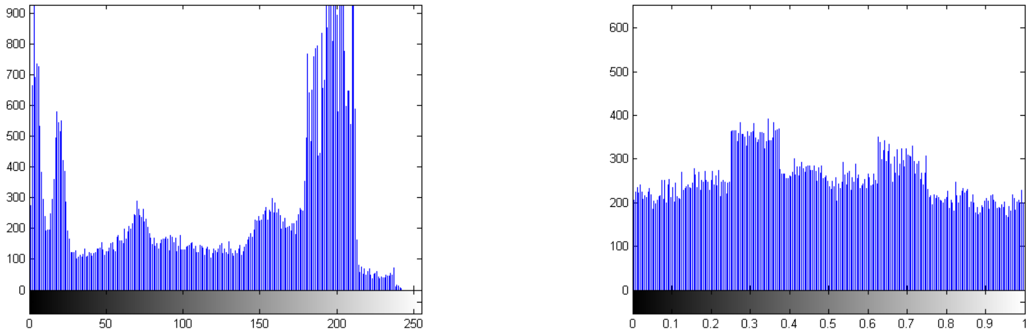


Figure 4 The left side picture represents the histogram of original Obama image meanwhile right side picture represents histogram of encrypted image

REFERENCES

[1] Ljupco Kocarev, Marjan Sterjev, Attila Fekete, Gabor Vattay, "Public-key encryption with chaos," American Institute of Physics, Vol. 14, No. 4, 1078-1082, 2004

[2] Roy Tenny, Lev S. Tsimring, "Additive Mixing Modulation for Public Key Encryption Based on Distributed Dynamics", IEEE Transactions on circuits and systems, Vol. 52, NO. 3, 672-679, 2005.

[3] Shuichi Aono, Yoshifumi Nishio, "A Cryptosystem Based on Iterations of Chaotic Map," IEICE Technical Report, Vol.107, No.87, 2007.

[4] Dayuan, B. Dahu, W.," A Chaos Public-Key Cryptosystem Based on Semi-Group Features," International Conference on Biomedical Engineering and Informatics, BMEI, 1-3, 2009.

[5] LI Zhi-hui, CUI Yi-dong, XU Hui-min, "Fast algorithms of public key cryptosystem based on Chebyshev polynomials over finite field‖", The Journal of China Universities of Posts and Telecommunications, Volume 18, Issue 2, 86–93, 2011.

[6] Mazen Tawfik Mohammed, Alaa Eldin Rohiem, Ali El-moghazy, A. Z. Ghalwash, "Chaotic Based Key Management and Public-key Cryptosystem‖," International Journal of Computer Science and Telecommunications, Volume 3, Issue 11, 35- 42, 2012.

[7] Guan Z-H, Huang F, Guan W "Chaos-based image encryption algorithm," PhysLett A346:153–157, 2005.

[8] Chen G, Mao YB, Chui CK "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons Fractals 12:749–761, 2004.

[9] Wong K-W, Sin-Hung Kwok B, Law W-S "A fast image encryption scheme based on chaotic standard map," PhysLett A 372(15):2645–2652, 2008.

[10] Xing-Yuan W, Qing Y "A block encryption algorithm based on dynamic sequences of multiple chaotic systems," Commun Nonlinear Sci Numer Simul 14(2):574–581, 2009.

[11] Sun F, Liu S, Li Z Lu Z "A novel image encryption scheme based on spatial chaos map," Chaos Solitons Fractals 38:631–640, 2008.

[12] Pan Tian-gong and Li Da-yong "A Novel Image Encryption Using Arnold Cat," International Journal of Security and Its Applications Vol.7, No.5: 377-386, 2013

[13] Sun X., Zheng K.,Wang L., Zhao W., Sun X. "Choas of Henon Map Based on the Coupled Networks," Journal of Theoretical and Applied Information Technology, Vol. 47 No.1: 349-354, 2013