Chaos Based Image Encryption and Decryption

Abhishek Bhagat[1], Abhishek Surve[2], Sanuj Kalgutkar[3], Apeksha Waghmare[4]

[1]*BE-CMPN (Pursuing), Atharva College of Engineering, Mumbai, Maharashtra, India*
[2]*BE-CMPN (Pursuing), Atharva College of Engineering, Mumbai, Maharashtra, India*
[3]*BE-CMPN (Pursuing), Atharva College of Engineering, Mumbai, Maharashtra, India*
[4]*Assistant Professor, Dept. of Computer Engineering, Atharva College of Engineering, Maharashtra, India*

---***---

Abstract - *In recent years, owing to frequent flow of digital images across the world over the transmission media, it has become essential to secure them from leakages. Due to the exceptionally desirable properties of mixing, sensitivity to initial conditions and parameters of chaotic maps; chaos-based encryption has recommended a new and efficient way to deal with the problem of fast and highly secure image encryption. The implemented image encryption scheme consists of an 80-bit secret key and uses chaotic map like Arnold Cat-Map and Logistic Map. The initial conditions for the chaotic maps are derived using the 80-bit secret key. In this cryptosystem, permutation-diffusion architecture followed by an efficient diffusion scheme is implemented. This scheme consists of two diffusion procedures, with a supplementary diffusion procedure padded after the normal diffusion. In the supplementary diffusion module, the control parameter of the selected chaotic map is altered by the resultant image produced after the normal diffusion operation. As a result, a slight difference in the plain image can be transferred to the chaotic iteration and bring about distinct key streams, and hence totally different cipher images will be produced. Therefore, this scheme can remarkably accelerate the diffusion effect of the cryptosystem and effectively resist differential attacks. Our project objective is to provide high level of security and satisfactory encryption speed for practical secure image applications.*

Key Words: **Arnold Cat-map, Logistic Map, Chaotic Map, Cipher, Permutation, Diffusion.**

1. INTRODUCTION

In this project a new way of image encryption scheme has been proposed using two chaotic maps which are Arnold Cat map for Permutation and Logistic Map for diffusion using a 80-bit randomly generated key. The initial condition for both chaotic maps is derived using the 80-bit randomly generated key. In this proposed encryption process, the traditional permutation-diffusion architecture is followed by an efficient diffusion scheme. Our diffusion scheme consists of two relevant diffusion procedures in one overall round encryption. The first one is the same as the normal diffusion module, whereas, in the supplementary diffusion procedure, the control parameter of the selected chaotic map i.e. Logistic map is altered by the resultant image generated after the first diffusion operation. Key sensitivity test is conducted to observe the effect of changing the different keys to encrypt slightly. Furthermore we calculate the NPCR and UACI values and perform the different statistical analysis such as histogram analysis, correlation of adjacent pixels and information entropy.

2. Literature Review

2.1 Block Image Encryption Algorithm by Fridrich, 1998

Fridrich proposed the first general architecture for chaos-based image cryptosystems. This architecture is composed of two stages: permutation and diffusion. In the first stage, pixels are permuted by a two-dimensional area-preserving chaotic map to erase the high correlation between adjacent pixels. Then, pixel values are modified sequentially using a certain discretized one-dimensional chaotic map in the diffusion procedure.[1]

2.2. Image Encryption using Chaotic Logistic Map, 2006

Patidar et al. proposed an image cipher in which an external secret key of 80-bit and two chaotic logistic maps are employed. The initial conditions for the both logistic maps are derived using the external secret key by providing different weightage to its bits. In the algorithm, the first logistic map is used to generate numbers ranging from 1 to 24. The initial condition of the second logistic map is modified from the numbers, generated by the first logistic map. By modifying the initial condition of the second logistic map in this way, its dynamics gets further randomized.

In the proposed encryption process, eight different types of operations are used to encrypt the pixels of an image and which operation will be used for a particular pixel is decided by the outcome of the second logistic map. Thus, the second chaotic map further increases the confusion in the relationship between the encrypted and its original image. To make the cipher more robust against any attack, after each encryption of a block of sixteen pixels, the secret key is modified.[2]

2.3. A Novel Image Encryption using Arnold Cat Map, 2013

Pan Tian-gong and Li Da-yong proposed an algorithm of image encryption based on 3D Arnold cat map, combined with logistic chaotic map to image encrypt. In this paper, 3D

Arnold cat map is applied in image encryption, and it has more security and better effect. However, its period is fixed. The original image will be returned to itself if iterating some times. On the basis of 3D Arnold cat map, it presented an algorithm of image encryption which separates the original image to many same blocks and no period.[3]

2.4. Chaotic Image Scrambling Algorithm Based on S-DES, 2006

X Y Yu, J Zhang, H E Ren, G S Xu and X Y Luo proposed a dual image encryption algorithm based on S-DES and Logistic map. The encryption structure which combined the Logistic map with S-DES system is showed as Fig. 2.1.[4]

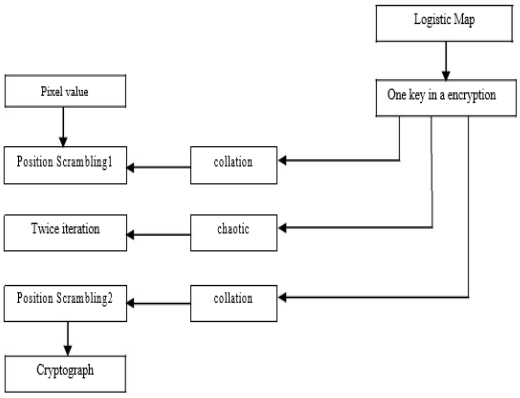

Fig. 2.1. The encryption structure of Logistic map and S-DES

2.5. Chaos based Image Encryption, 2014

Jun-xinChen, Zhi-liangZhu, Li-boZhang, ChongFu, and HaiYu proposed an Efficient Diffusion Scheme for Chaos-Based Digital Image Encryption. In the proposed scheme the plain image is permuted using Arnold Cat map. The permuted image undergoes diffusion procedure using Logistic Map. A supplementary diffusion is padded after normal diffusion to accelerate the spreading scale remarkably. In this project we will be referring to the technique proposed by Jun-xinChen, Zhi-liangZhu, Li-boZhang, ChongFu, and HaiYu.[5]

2.6. Communication Theory of Secrecy Systems, 1949

C. E. Shannon proposed a solution on problems of cryptography and secrecy systems by furnishing an interesting application of communication theory. In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography. There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.[6]

3. System Implementation

3.1. Architecture of Permutation-Diffusion Type Image Cryptosystems

The traditional architecture of permutation-diffusion type chaos-based image cryptosystems is shown in Fig. 3.1. There are two stages in this type of cryptosystems, namely, the permutation stage and diffusion stage.

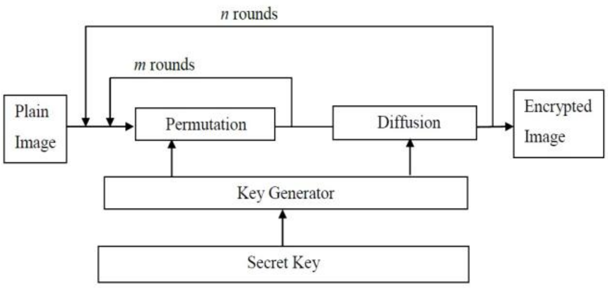

Fig. 3.1 Fridrich's permutation-diffusion architecture

3.2. Permutation

In the permutation stage, image pixels are generally shuffled by a two-dimensional area-preserving chaotic map, without any modification to their values. Arnold Cat Map is applied to the Plain Image to achieve permutation (pixel position substitution). All pixels are scanned sequentially from left to right and top to bottom.

3.3. Arnold Cat Map

Arnold's Cat Map was discovered by Russian mathematician Vladimir Arnold in 1960. This mapping is a simple illustration of some of the principles of chaos theory – specifically, showing the underlying order to an apparently random evolution of a system. In this example an image is hit with a transformation that apparently randomizes the original organization of its pixels. However, if iterated enough times, the original image reappears.

Consider a N × N image and x and y be the row and column number of the pixels in the image. Thus x and y both ranges from 1 to N. Arnold's Cat Map transformation of the image is obtained by implementing the below formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Where, p and q are positive integers, and determinant of matrix A is 1.The value of p and q depends on the key size. When Arnold cat map algorithm is executed once, the original pixel positions coordinate will be transferred from the (x, y) to a new pixel position (x', y'); then the process is repeated with the A matrix multiplied. The pixels will continue to move until they return back to their original position; the number of moves is T and the size of the pixel space is n = 0, 1, 2… N−1. Pixels move with periodicity, and T, p, q and the original image's size N are correlated; thus, whenever the values change, it generates a completely different Arnold cat map. After being multiplied few times, the correlation between the pixels will be completely chaotic.

However, Arnold cat map encryption algorithm has periodicity, which reduces its encryption security. This is why we add the Logistic map into the chaos system to enhance security.

Below is an example where the mapping is applied repeatedly onto a 124× 124 pixel image of a tiger, which results in a surprising thing.

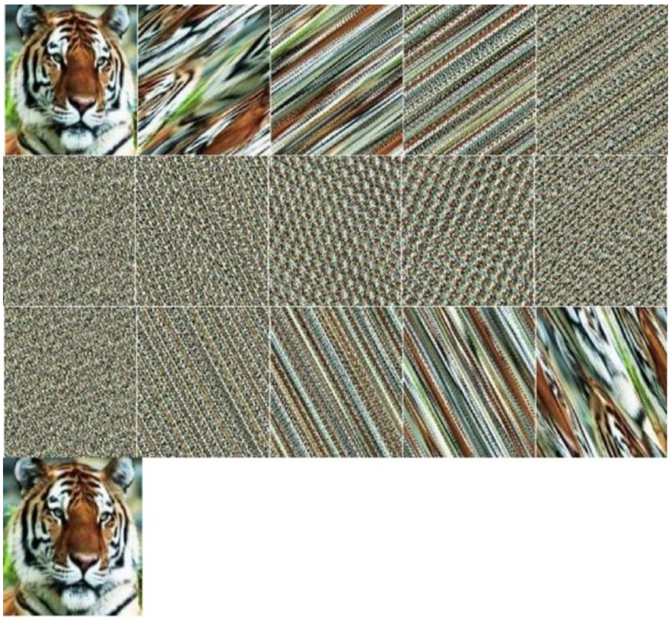

Fig. 3.2 Image is encrypted using Arnold's Cat map

Initially the image dissolves into a television-static like state, and then eventually on the fifteenth iteration it reforms back into the original image.

3.4. Diffusion

In the diffusion stage, pixel values are modified sequentially by mixing with the key stream elements that are generated by a one-dimensional chaotic map. Logistic Map is used for performing diffusion of the permuted image. Generally, the modification to one particular pixel depends not only on the corresponding key stream element but also on the accumulated effect of all the previous pixel values, as described by:

$$C(n) = X(n) \oplus p(n) \oplus C(n-1)$$

where p(n), X(n), C(n), and (n−1) represent the current plain pixel, key stream element, output cipher-pixel and the previous cipher-pixel, respectively. Such diffusion algorithm can spread a slight difference in the plain image to large scale pixels in the ciphered image and thus differential attack may be practically useless. Additionally, to cipher the first pixel, c (−1) has to be set as a seed. In this project, chaotic logistic map is employed as the key stream generators.

3.5. Logistic Map

The logistic map is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. The map was popularized in a seminal 1976 paper by the biologist Robert May, in part as a discrete-time demographic model analogous to the logistic equation first created by Pierre François Verhulst. Mathematically, the logistic map is written as:

$$x(n+1) = \mu \times x(n) \times (1 - x(n))$$

where, μ and Xo is the control parameter and state value respectively. If one choose μ∈ [3.57,4], the system is chaotic.

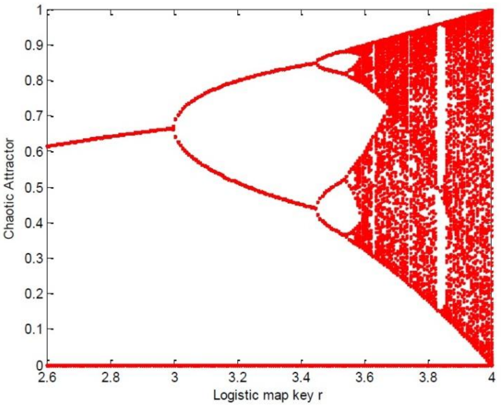

Fig. 3.3 Bifurcation Diagram of Logistic Map

By varying the system parameter μ, following behaviors are observed:

- When the value of μ lies between 0 and 1, the iterative values ultimately die, which are sovereign of the initial conditions.
- When the value of μ lies between 2 and 3, the iterative values first oscillate around some value and then finally stabilize on the same value.
- When the value of μ lies between 3 and 3.45 (approximately), the iterative values oscillate between two values forever, which are dependent on μ.
- When the value of μ lies between 3.45 and 3.56 (approximately), the iterative values oscillate between four values.
- As the value of μ becomes greater than or equal to 3.57, this logistic map is converted into chaotic map because a slight variation in the initial condition produces dramatically different iterative values over time, exhibit chaotic behavior and trajectory of these iterative values is called chaotic attractor, which is suitable condition for image encryption.

3.6. Key Generation

- The proposed image encryption process utilizes a randomly generated 80-bit key (binary). Further, the secret key is divided into 5 sub keys 16-bit each.
- The main secret key K is 80-bit and the subkeys K_1, K_2, K_3, K_4, K_5 are 16-bit each. The subkeys K_1, K_2 are assigned to secret parameters p and q of Arnold Catmap. The subkeys K_3,
- $K_4$and $K_5$are assigned to Logistic map parameters μ, $X_0$and C (-1). K_1, K_2 K_3, K_4, K_5areconverted from binary to decimal value (0-1) using Eqn.3.12 and Eqn.3.13 which is specified according to IEEE 754 standard.

$$K_n = \sum_{i=1}^{16} K_n\,(i) \times 2^{-i}$$

- From decimal values $K1$, $K2$ *and* $K5$ are converted to positive integers in the range (1-255) using Eqn.

$$K_n = mod\left(\left(\frac{K_n + 1}{2}\right) \times 10^{14}\right) 255$$

- μ is brought in range (3.57,4) by adding decimal value of k_3 with 3.57 and if it exceedes 4 then setting it as 4.

In this way all keys are brought to their ranges as shown in Table:

	Subkeys	Key Parameter	Range
Arnold Cat Map parameters	K1	*p*	(1-255)
	K2	*q*	(1-255)
Logistic Map parameters	K3	*μ*	(3.57-4)
	K4	*X0*	(0-1)
	K5	*C* (-1)	(1-255)

3.7. Traditional diffusion scheme

- In the traditional diffusion stage, pixel values are modified by mixing with the key stream elements that are generated by a one-dimensional logistic map. Logistic Map is used for performing diffusion of the permuted image. The modification to one particular pixel depends not only on the corresponding key stream element but also on the effect of all the previous pixel values.

- Such diffusion algorithm can spread a slight difference in the plain image to large scale pixels in the encrypted image and thus differential attack may be practically useless. Additionally, to encrypt the first pixel,*C* (-1) has to be set as a seed.

3.8. Efficient Diffusion Scheme

The implemented efficient diffusion scheme consists of permutation and two diffusion procedures with the normal diffusion module being unchanged and supplementary diffusion procedure. In the normal diffusion stage, plain pixel values are modified sequentially by the logistic map with the chosen parameters (X0, μ). So, the difference will spread out to all the pixels from (x', y') to the last pixel, the same as the spreading process in the traditional diffusion procedure. Then, in the supplementary diffusion stage, the control parameter μ of the logistic map is altered by C1(N-1,N-1), the last pixel of the resultant image produced by the first diffusion stage.

Through this mechanism, the slight spreading effect produced in the normal diffusion procedure will be introduced to the chaotic map, and hence result in totally different key streams due to its high sensitivity to the control parameter. Therefore, the difference will spread out to the whole cipher image and bring about totally different cipher images, and hence a satisfactory diffusion effect is obtained, as shown in Fig. 9.5 In our scheme, the control parameter of the logistic map is altered according to

$$\mu' = \mu \pm L \times \Delta \text{ (Eqn. 1)}$$

Where L is the gray-scale value of C1(N-1,N-1),and Δ is the basic perturbation unit.

- For decryption, $N \times N+1$ key stream elements are generated from μ' and the final encrypted image is decrypted using key stream elements of μ'which is then followed by normal decryption using key stream elements of μ. Here, μ is generated from μ', L and Δ.

- The detailed procedure of efficient diffusion scheme is as follows:

Encryption process:

- Step 1: Load the plain image.
- Step 2: Perform permutation using Arnold Cap Map for 3 rounds with keys p and q.
- Step 3: Perform diffusion using Logistic Map for 1 round on permuted image with keys μ,X_0 *and* C.
- Step 4: Calculate μ' Eqn. 1.
- Step 5: Perform diffusion by using Logistic map for 1 round on previously diffused image with keys μ',X_0 and C.

Decryption process

- Step 1: Perform inverse diffusion using Logistic map for 1 round on encrypted image with keys μ',X_0*and* C.
- Step 2: Calculate μ from μ', L and Δ.
- Step 3: Perform inverse diffusion by using Logistic map for one round on the previously diffused image with keys μ,X_0 and C.

Step 4: Perform inverse permutation by using Arnold Cat Map for three rounds on the previously diffused image with keys p and q.

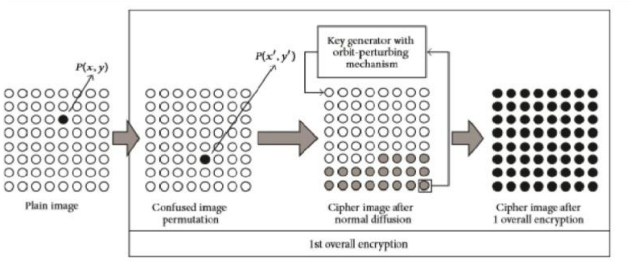
P(x, y)
P(x′, y′)
Key generator with orbit-perturbing mechanism
Plain image
Confused image permutation
Cipher image after normal diffusion
Cipher image after 1 overall encryption
1st overall encryption

Fig. 3.4 Diagram of Efficient Diffusion Scheme

4. CONCLUSIONS

In the project, an efficient diffusion scheme will be implemented to address the efficiency and security flaws of the traditional permutation-diffusion type image cryptosystems. The diffusion scheme consists of two relevant diffusion procedures in one overall round encryption. The first one is the same as the normal diffusion module, whereas, in the supplementary diffusion procedure, the control parameter of the selected chaotic map is altered by the resultant image generated after the first diffusion operation. This scheme makes full use of the sensitivity property of the chaotic systems, and a slight difference in the image can be transferred to the chaotic map iteration and then brings about totally different key stream elements. Through this mechanism, the spreading effect of the cryptosystem can be significantly accelerated in the supplementary diffusion procedure and the cryptosystem can resist chosen/known plaintext attacks effectively. Experimental results will prove the higher efficiency and the security level of the proposed scheme, as given in the reference paper. These improvements can motivate the practical applications of permutation-diffusion architecture chaos-based image cryptosystems.

REFERENCES

1) J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps, ”International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, vol. 8, no. 6, pp. 1259–1284, 1998.

2) V. Patidar, N. K. Pareek, and K. K. Sud, “A new substitution- diffusion based image cipher using chaotic standard and logistic maps,” Communications in Nonlinear Science andNumerical Simulation,vol.14,no.7,pp.3056–3075,2009.

3) A Novel Image Encryption Using Arnold Cat proposed by Pan Tian-gong and Li Da-yong College of Measurement-Control Tech & Communications Engineering, International Journal of Security and Its Applications Vol.7, No.5 (2013).

4) Chaotic Image Scrambling Algorithm Based on S-DES By X Y Yu1, J Zhang1,2 ,H E Ren2 ,G S Xu1 and X Y Luo1.

5) Jun-xinChen,Zhi-liangZhu, Li-boZhang, ChongFu, andHaiYu An Efficient Diffusion Scheme for Chaos-Based Digital Image Encryption, Volume 2014, Article ID 427349, 13 pages http://dx.doi.org/10.1155/2014/427349.

6) C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal, vol.28, no.4, pp.656–715, 1949.