Securing image using Chaotic System

Sunil Jaiswal, Supriya M.Gharat, Sankusu Sharma

Abstract*— Security of an image has become an essential part in communication and multimedia world. Cryptographic techniques are used to accomplish a certain level of security, integrity and confidentiality to prevent unauthorized access. In this paper, a colour image encryption and decryption technique is proposed, based on chaotic system. Image pixel scrambling is to divide the image into quadrants and then rotate them clockwise. After that a 2 dimensional Arnold cat map is applied to make more distortion to the adjacent pixel of the image. A Henon mapping system is then used to diffuse the correlation between the crypto-image and the original image. The encryption algorithm has been tested and analysis on several colour images showed significant security and validity to resist different attacks.

Index Terms*— Image Scrambling, Arnold cat map, Henon Chaotic map, Key generation, Encryption, image cryptography.

I. Introduction

Digital encryption is one of the essential techniques to provide secrecy to image and video data. Image encryption technique converts the image data from readable form to and illegible form in an open network so that the plain image is kept secret. Digital image encryption can be used in different application such medical imagery, archaeological applications, military field, video surveillance, confidential transmission and in daily life styles likes financial records. Because of the development in the multimedia technology, the transmission of image and video is used in real time data transmission. In order to provide the higher security image encryption algorithm needs to fulfil the concepts of confusion and diffusion. Confusion means shuffling the values and diffusion means changing the values. In [1], N. S. Raghava introduced a new symmetric image encryption algorithm which is based on Henon's chaotic system. A byte sequences is applied with a novel approach of pixel shuffling of an image which results in an effective and efficient encryption of images. Confusion is done by pixel movement form actual position to a new position and diffusion is done by applying byte sequence generated from Henon map. So both the processes of increasing confusion and diffusion resulted in increasing the security of cryptosystem. In [2], R. Kumar introduced a colour image encryption technique which is simple in implementation with high level of efficiency. Henon map is a discrete time dynamic system which exhibit chaotic behaviour which was used to produce a uniform distribution of pixels of image. In this method, a bit stream of RGB component of colour image is taken and is used as the input for the Encryption algorithm. The chaotic map takes the original image as initial value for the input, sequence of bit provided by user mapped as control parameter. Output chaotic sequence produces the cipher image. In [3], P. Gupta, S. Singh, I. Mangal have discussed a new algorithm for image encryption based on Arnold cat map. Arnold cat map is a 2 dimensional chaotic map which is used to shuffle the pixel position of the plain image Arnold cat map does not change the intensity value of the image, it only shuffle the data of the image. The relationship between the neighbouring is removed and the original image seems distorted and meaningless. The rest of paper is arranged as follows: Section 2 shows the related works of image encryption. In section 3, an image encryption method based on Image scrambling, 2D Arnold cat map and Henon chaotic mapping is proposed and discussed also. In Sections 4, experiment results are explained. Finally, Section 5 involved the conclusion of the paper.

II. RELATED WORK

Various technique and algorithm has been implemented to build a fast and secure image transmission system. In [5], Chen introduced a gray scale image encryption scheme which is used to scramble the position of image pixels using chaotic cat mapping. The experimental tests and analysis that carry out on various images of the proposed algorithm demonstrated the high level of security and also, it useful for encryption the real time images through transmission networks and internet. In [6], showed an image encryption technique based on Arnold cat map with Henon's chaotic system to encrypt image pixel by pixel. The experimental results and analysis of system shows that the gray-scale cipher image exhibits is spread in a random manner. An experimental analysis also shows that this method is more

***Sunil Jaiswal**, Department of Computer Engineering, University of Mumbai/ St. John College of Engineering & Technology. Mumbai, India/ Mobile No:+919503511094*

***Supriya M. Gharat Department** of Computer Engineering, University of Mumbai/ St. John College of Engineering & Technology. Mumbai, India.*

***Sankusu Sharma**, Department of Computer Engineering, University of Mumbai/ St. John College of Engineering & Technology., Mumbai, India.*

All Rights Reserved © 2016 IJARCET

suitable for image encryption application especially for wireless communication. In [4], the suggested system perform diffusion on the image data pixel by pixel by moving the original pixel location to a new pixel location and to hide the structure of the image, while confusion method was done by byte sequence generate by Henon map. The result shows that the increase in number of confusion and diffusion processing will increase the security of encryption method.

III. PROPOSED CRYPTOSYSTEM

The main aim of the proposed system is to provide a easy and secure scheme for encryption and decryption of a digital image to all valid user, Fig. 1.a. shows how to encryption and Fig.1.b. shows decryption of the image will be done. It uses a RGB matrix of width*height*3 stored as a three dimensional matrix of pixels.

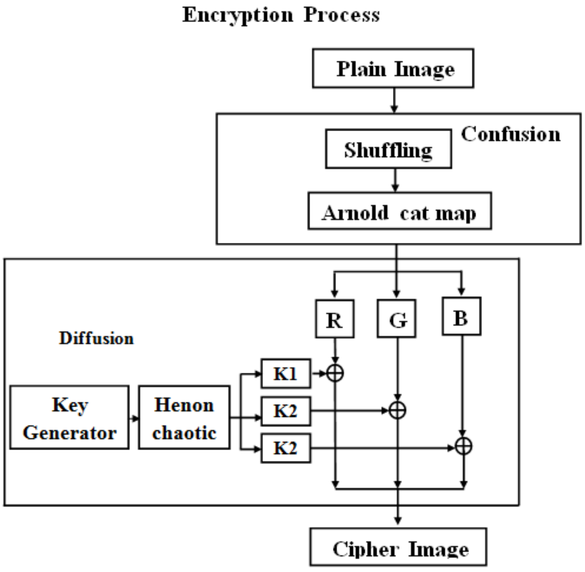


Fig.1.a. Encryption process

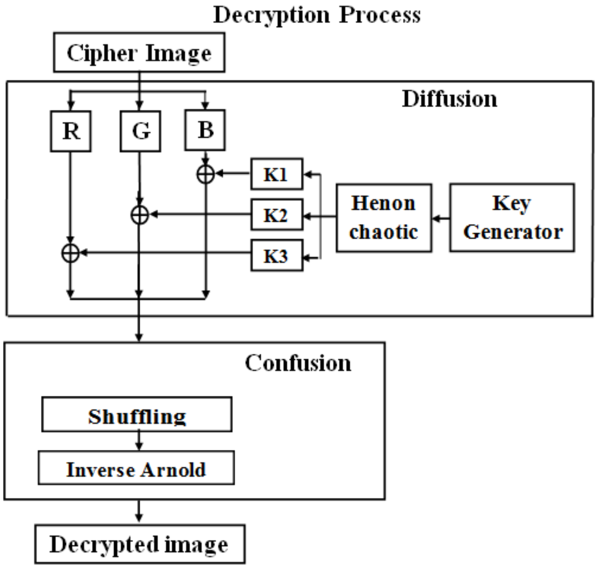


Fig.1. b. Decryption process

A. Image Scrambling

Image scrambling is used to disturb the correlation between the neighbouring pixels. We only change the position of the pixels, so that the histogram of the image is same at the beginning of the encryption and decryption process

Scrambling of the image is done in three steps

1st step: Divide the image into 4 quadrants and rotate each one with 90^0 in anticlockwise direction.

2nd step: Divide each quadrant into 4 sub-quadrants and rotate them with 90^0.

3rd step: Divide each block again to four sub-quadrants and rotate each one with 90^0. The result is 64 block of the image.

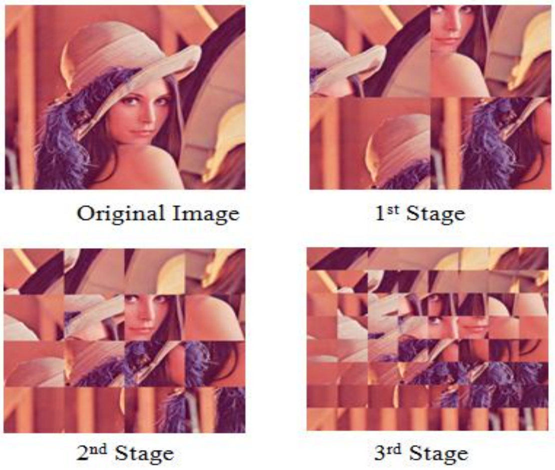


Fig.2. Example of Image Scrambling

B. Arnold Cat Map

Arnold cat map is a 2 dimensional chaotic map which is used to shuffle the pixel position of the plain image. Using Arnold cat map, the intensity value of the image is not changed, only the data of the image is shuffled.

Equation.1. used for shuffling pixel within the image.

$$x' = (x+y)\text{mod width.} \quad (1)$$
$$y' = (x+2*y)\text{mod width.}$$

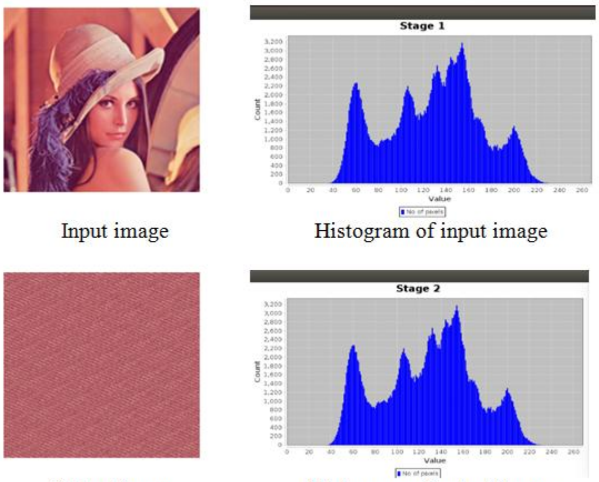
where,

x', y' represent the new location of the image pixel.
x, y represent the original location of the image.
width represent the width of the input image.

After applying Arnold for a specific no of times on the plain image, the relation between the neighbouring pixels is distorted and the original image seems meaningless. For iterating it too many times it will return the original look, which means that Arnold cap map is periodic transform.

After image shuffling, the histogram are same for encrypt image and original image to improve the security of the encryption System. After the confusion process, we use Henon chaotic system for diffusion and for improving the security.

All Rights Reserved © 2016 IJARCET



Input image Histogram of input image

Output image Histogram of output image

Fig.3. Example of Arnold Cat Map

C. Henon Chaotic Map

Henon chaotic is the most known and commonly used dynamic system that reveals chaotic behaviour. Henon map introduces uniform distribution of pixel of digital image. A Henon key is provided by the user which will be used to calculate the initial points. It take initial conditions (x_0, y_0) as a secret value in a 2D plane and map it to next point by using Equation.2.

$$x_{[i+1]}=1-a*(x_{[i]}*x_{[i]})+y_{[i].} \qquad (2)$$

$$y_{[i+1]}=b*x_{[i].}$$

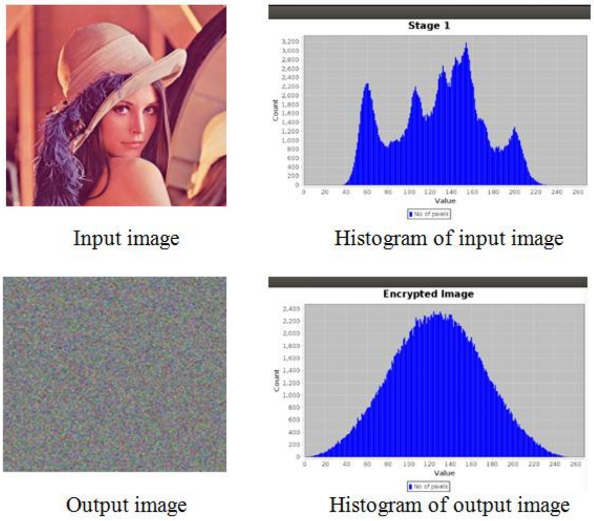
where,

a, b - represent the control parameter.

x_i, y_i - represent the initial secrete key.

$x_{[i+1],}$ $y_{[i+1]}$ - represent the sequence of the other key.

The Henon chaotic system is designed to diffuse the relationship among encrypt image and the original image. The histogram of the encrypted is in uniform distribution which make difficult for the cryptanalyst to find the encryption system.



Input image Histogram of input image

Output image Histogram of output image

Fig.4. Example of Henon Chaotic Map

D. Key generation

Algorithm:

1. Separate the RGB matrix of an image.
2. Convert the matrix of each R, G, B component into a single array with (width*height) elements.
3. Generate the sequence of keys with (height*width*3) elements using Equation.3.

$$x_{i+1}=1-ax^2_i+y_i \qquad (3)$$

$$y_{i+1}=bx_i \qquad i=1,2,3,....$$

where,

a, b represents the control parameters given by user.

x_0, y_0 represents the initial secret keys.

x_{i+1}, y_{i+1} represents new sequence of keys.

Providing a=1.4, b=0.3 and initial parameters x0=0.0100, y0=0.0200. The values of key sequence lie between the interval of [-1 1]. Some samples are shown in Table.I.

TABLE.I. Sequence keys between[-1 1]

0.01	1.019	-0.453	-1.018	-0.588
1.225	-1.140	-0.453	0.370	0.671

4. Convert the sequence from [-1 1] to [1 256] using Equation.4.

newkey=((key*1000)%256) (4)

Sample key values in interval of [1 256] are shown in Table.II.

TABLE.II. Sequence keys between [1 256]

10	252	197	250	76
53	121	202	116	197

E. Encryption

The Encryption of the image is performed by changing the value of each R, G, B pixel through exclusive OR operation with the sequence value dedicated for each components.

F. Decryption

For reconstructing the original image, reverse operation of encryption is performed. the Chaotic system is deterministic in nature, the sequence key is XORed with the cipher image to get the shuffled image. Then we apply inverse of Arnold mapping to get the rotating image block. Using the Equation.5.

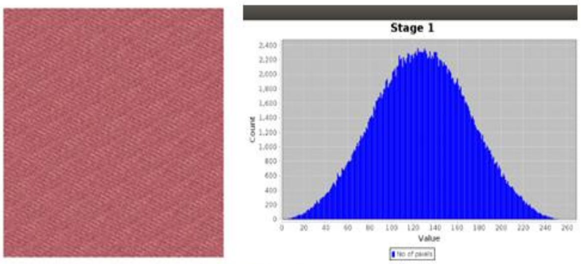
$$x = (x'+y')\text{mod width} \qquad (5)$$

$$y = (x'+2*y')\text{mod width}$$

All Rights Reserved © 2016 IJARCET

The shuffled blocks of image are then rearranged by rotating it Clockwise by 90 degree to obtain the original image. Fig. 5 shows the output and histogram of stage 1 of decryption process. Fig. 6 shows the output and histogram of stage 2 of decryption process. Fig. 7 shows the output and histogram of stage 3 of decryption process.

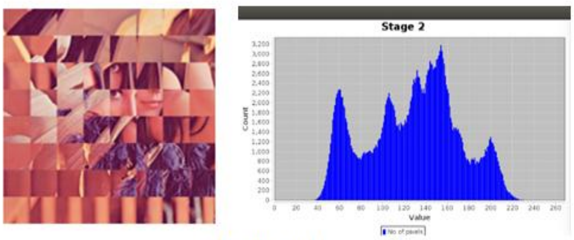
Step 1:



After Henon

Fig.5. Decryption stage 1

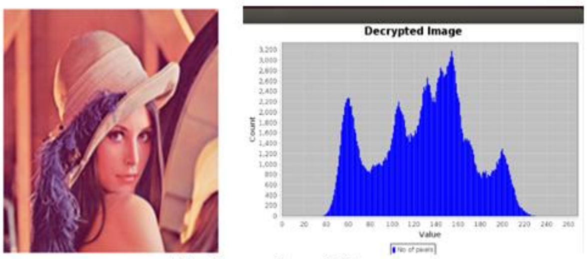
Step 2:



After Arnold

Fig.6. Decryption stage 2

Stage3:



After Image Scrambling

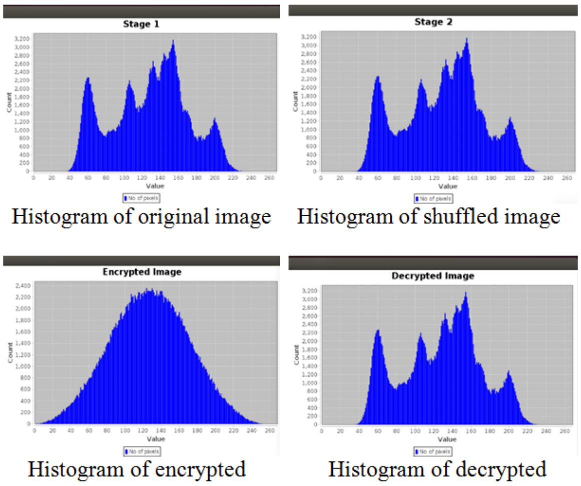
Fig.7. Decryption stage 3.

IV. Experimental Analysis

To check the effectiveness of the SCA system, we have performed several tests on different image. A plain image with the size 300X300 is taken as input and the histogram that image is shown in the Fig. 3 .The key and number of iteration to be done is taken from the user. Using key= 324 and number of iteration= 46, the encrypted image and the histogram of the encrypted image is shown in Fig.4

A. Histogram Analysis

A histogram is graphical representation of pixel intensity value of an image. There are 256 intensity of a greyscale image, so the histogram will display 256 intensities and the distribution of pixel among the intensity value. Histogram analysis is done at all the stage of the encryption and decryption process. In the original image some gray scale value are not present in the range of 0 to 255 but in the encrypted image, there are certain value which are in the encrypted image. The encrypted image does not help the intruder to employ statistical attack on the encryption process.



Histogram of original image Histogram of shuffled image

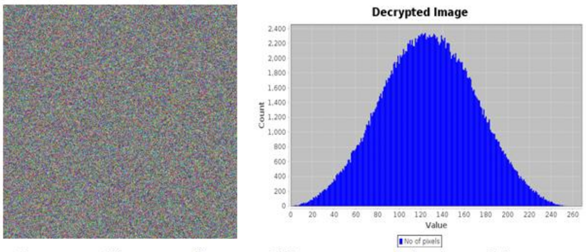
Histogram of encrypted image Histogram of decrypted image

Fig.8. Histogram Analysis

From Fig. 8, it is analyzed that the pixel distribution of the image is uniform in cipher image and totally different from the histogram of the original image.

B. Key Sensitive analysis

For secure encryption, the key should be sensitive with large no of key size to resist all kind of brute force attack. Randomness is important point in Henon Map. If we change the value of key from 324 to 325 the resultant encrypted will become entirely different from the original image. It is not possible to obtain the original image at the receiver end.



Decrypted image after slight variation in key Histogram of decrypted image

Fig.9. Key Sensitive analysis

All Rights Reserved © 2016 IJARCET

V. Conclusion

In this paper, the SCA encryption algorithm is given secure and effective way for encrypting the image. Image is encrypted using different encryption algorithm. The image is processed at different stages. At Stage 1 the image is scrambled to remove the correlation between the images, than an Arnold cat map is applied to shuffle the image, after that Henon chaotic system is used to change the intensity value of the image. The encrypted image is a scrambled image. Several images have been used to test the SC algorithm. The resultant image provides high level of security of images. SCA system has multi-dimensional large key space to resist all kind of brute force attack. Many experiments were carried out with key sensitive analysis, to check the robustness of the SC algorithm. The cryptosystem provides an effective way for image encryption and achieve more reliable flexible and higher quality encryption. The SCA works only on colour PNG image. Future work focuses on Encrypting JPEG colour and Greyscale images.

REFERENCES

[1] N. S. Raghava, A. Kumar,"Image Encryption Using Henon Chaotic Map With Byte Sequence",International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol.3, Issue 5, Dec 2013.

[2] R. K. yadava, B. K. Singh , S. K. sinha, K. K. Pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", Journal of Information Engineering and Applications, Vol.3, No. 6, 2013.

[3] P. Gupta, S. Singh, I. Mangal, “Image Encryption Based On Arnold Cat Map and S-box”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 4,Issue 8,2014.

[4] C. Wei-bin, Z. Xin, "Image encryption algorithm based on Henon chaotic system" , Image Analysis and Signal Processing IEEE explore, pages 94 - 97,11-12 April 2009.

[5] G. Chen, Y. Mao , C. K. Chui ,"A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals 21 ,pages 79–761, Elsevier Ltd 2004.

[6] C.Wei-bin, Z. Xin ,"Image encryption algorithm based on Henon chaotic system",Image Analysis and Signal Processing IEEE xplore,pages 94 - 97,11-12 April 2009.

[7] M. Prasad, K. L. Sudha, “Chaos image encryption using pixel shuffling with henon map”, Manjunath Prasad et al./ Elixir Elec. Engg. 38, pp4492-4495, August.2011.\

Sunil Jaiswal is an Under Graduate student pursuing his Bachelor's Degree in Computer Science and Engineering from St. John College of Engineering & Technology, Palghar. He is working on the current project mentioned in this paper under guidance of Sankusu Sharma, Assistant Professor in Computer Department.

Supriya M. Gharat is an Under Graduate student pursuing her Bachelor’s Degree in Computer Science and Engineering from St. John College of Engineering & Technology. She is working on the current project mentioned in this paper under the guidance of Sankusu Sharma, Assistant Professor in Computer Department.

Asst. Sankusu Sharma has completed his ME from VIT, India. He has completed BE in Computer Science and Engineering from St. John College of Engineering & Technology, Palghar, India. He has more than 3 years of teaching experience.

All Rights Reserved © 2016 IJARCET