Journal of Information Engineering and Applications www.iiste.org
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.3, No.6, 2013- Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications

A New Approach of Colour Image Encryption Based on Henon like Chaotic Map

Ramesh Kumar yadava[#], Dr. B. K.singh*, S.K.sinha*, K. K.pandey[*], [#]
[#] Department of computer science and engineering, AISECT University BHOPAL
[1]mailramesh28@gmail.com
[3]third.author@first-third.edu
[*]AISECT UNIVERSITY
Mendua, Bhojpur Raisen Bhopal INDIA
[2]skrishna24it@gmail.com

Abstract
In modern era of digital world, exchange of information in form of image often very frequently over communication channel, the secrecy of multimedia data like images becomes very important, The issue of secrecy for image resolved In many digital applications such as sensitive visual aids, broadcasting, military services, rare satellites images and confidential medical images etc. To reduce the processing overhead with the concern of Real-time data transmission application, to reduce such a huge file processing cost, we needs to enhance our encryption/decryption techniques. This paper proposed a novel image encryption technique based on Hannon like chaotic map. Chaos-based image encryption technique is one of the more promising encryption algorithms that provide very efficient and fast way of image encryption due to its ubiquitous phenomenon in deterministic nonlinear systems that exhibit extreme sensitivity to initial condition and random like behaviours.
Keywords— Image RGB colour component, image encryption, *Henon* map, chaotic system.

I. INTRODUCTION

Encryption is a common technique to uphold multimedia image security in storage and transmission over the network due to some inherent features of image like high data redundancy and bulk data capacity. The encryption of image differs from that of text. With the development of multimedia technology the transmission of information as image and video is extensively used in real time data transmission. The digital image is widely used in our lives to resolve in many applications such as Geoinformation system, military image database, medical imaging system etc. for secure transmission of data, there is prime concern to provide security to these multimedia data, resulting in encryption of data. Most of conventional algorithm does not have the efficient capability for securing multimedia data containing image due to the complexity of algorithm and perfect correlation between pixel values of image. Several reviews has been proposed on multimedia data protection such as information hiding which include steganography, anonymity, watermarking. The other is encryption which includes conventional encryption technique. Last some decade relatively new approach has been extensively used, namely chaos based selective image encryption which provides relatively sufficient security and confidentiality. A symmetric block encryption algorithm creates a chaotic map used for permuting and diffusing multimedia image data. In permutation the pixel of image are replaced by another value and in the process of diffusion the pixel values are shuffled within the image. This paper proposed a colour image encryption technique which is very simple in implementation with high level of efficiency, which is based on *Henon* chaotic system. Henon map is a discrete time dynamic system which exhibit chaotic behaviour which we used to produce a uniform distribution of pixels of image. In proposed method we take a bit stream of *RGB* component of colour image which is the input for the Encryption algorithm. The rest or this paper is organized as follows. Section 2 describes the feature of chaos. Section 3 explains Henon map and its implementation. Section 4 present Encryption and decryption algorithm. Section 5 describes the experimental result to show the proof of robust algorithm. Section 6 shows the simulation analysis of security through Mat Lab. Section 7 concludes the paper.

II. FEATURE OF CHAOS

Chaos is a ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit sensitivity to initial conditio and have random like behaviour. Mathematically one dimensional chaos map can be represented as:

$$Xp+1 = f(\mathrm{Xp}),\quad f: I \rightarrow I, Xo\ \varepsilon\ I,$$

Where f is a continuous map on the interval $I = [0, 1]$.

With the following propriety:

1. Sensitive to initial condition this sensitivity property is utilized for the keys of cryptosystems..

2. Topological transitivity which linked to the diffusion feature of cryptosystem.
3. Density of periodic points in *I*.

Above two properties often used to construct stream cipher and block cipher in chaotic cryptography. Because the property of sensitivity of initial condition make the encryption very complicated. Sequence is also sensitive to control parameter. For image encryption chaotic system can be represented by Fig 1. The initial value of chaotic map takes the original image as input, sequence of bit provided by user mapped as control parameter. Output chaotic sequence produces the cipher image.

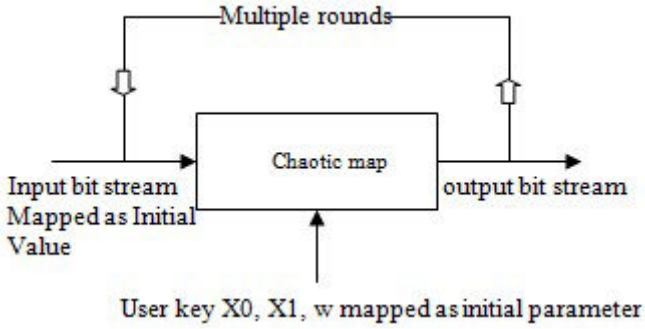

Fig. 1. Basic architecture of chaotic map

Small change in input bit stream produce a huge change in output bit stream after multiple round. Slight change of user key also produces totally different output sequence of bit stream.

III. *HENON* CHAOTIC MAP

The map was introduced by Michel Henon as a simplified model of the Poincare section of the *Lorenz* model. For the canonical map, an initial point of the plane will either approach a set of points known as the *Henon* strange attractor, or diverge to infinity. Two dimensional *Henon* map takes a point (Xn, Yn) in the plane and maps it to a new point:

$$X_{n+1} = Y_{n+1} - aX_n^2$$

$$Y_{n+1} = bX_n \quad \text{where } a > 0 \text{ and } |b| < 1,\ n = 0, 1, 2\ldots$$

Henon Map depends on two parameter a and b. these parameter values determine the chaotic behaviour of map. The

Most representative form of *Henon* map for canonical constant values a = 1.4 and b = 0.3 as we can see in Fig. 2. In which The *Henon* map reflects as chaotic attractor. The propose colour image encryption is based on *Henon* chaotic map, *Henon* like mapping used sin function which include a frequency control parameter w for maintaining their chaotic behaviour . The *Henon* like mapping equation which used in our present image encryption technique is a mathematical concept, where time dependency of any point determines by the fixed prescribed rule in geometrical space. In our proposed encryption technique we used Henon like chaotic map mathematically defined as

$$X_{n+2} = 1 - aX_{n+1}^2 + b\sin(wx_n)$$

Which contain frequency control parameter w to control the *Henon* like chaotic signal. Encrypted *Henon* chaotic signal looks like distortion to unauthorized users ignoring to decrypt it, due to some specific characteristic such as nonperiodicity, ergodicity, randomicity.

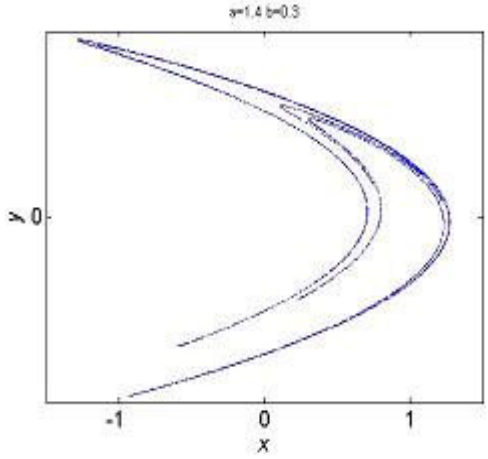

Fig. 2. Chaotic nature of the *Henon* map

IV. Encryption and Decryption Algorithm

The proposed encryption algorithm is based on *Henon* like mapping. Our algorithm is based on fully layered encryption technique to provide higher level of confidentiality. We used colour image for the encryption process in our proposed technique we can also used same technique for Gray scale image. We perform the colour transformation to separate the RGB colour in its component matrix. For Gray scale image there is no need of colour transformation. Then we select any one of the component (RGB) matrix for encryption to reduce the computational overhead. The encryption process perform in the study can be seen in Fig. 3.

(1) Encryption process:

Step 1. The *Henon* like chaotic system is converted in to one-dimensional chaotic map. One dimensional *Henon* chaotic map mathematically is defined as:

$$X_{n+2} = 1 - aX^2_{n+1} + b\sin(wxn) \quad \text{.....(1)}$$

Step 2. Transform the colour image in to its (RGB) 3 pieces of component matrix.

Step 3. One dimensional *Henon* chaotic map obtain in (1) takes R component of colour image to generate the random bit stream.

Step 4. The bit vales obtained in previous step is bit XOR with the original pixel values of R component of original transform matrix.

Step 5. The vector result of G and B component of transform colour image with the matrix after bit XOR obtained from the previous stage produce the cipher image.

Deterministic behaviour of chaotic map able us to reproduce the original image by providing the secret key component such as initial condition, system parameter, and number of iteration.

(2) *Decryption process:*

Step 1. The *Henon* like chaotic system is converted into one-dimensional chaotic map. One dimensional *Henon* chaotic map mathematically defined as

$X_{n+2} = 1 - X^2_{n+1} + b\sin(wXn)$ which is same as during encryption process.

Step 2. Perform colour transformation so that the colour image component RGB has been separated as in encryption process.

Step 3. Select the secret key and parameter as used in encryption with the Henon chaotic map function same as (1). This process generates the transform matrix of pixel values of R component of image.

Step 4. The XOR operation is computed bit- by- bit between the transform matrix of pixel values of R component of image and the bit values of the R component of cipher image as (2).

Step 5. Vector of the decryption result is returned as the value of RGB using the image transformation to produce the original image.

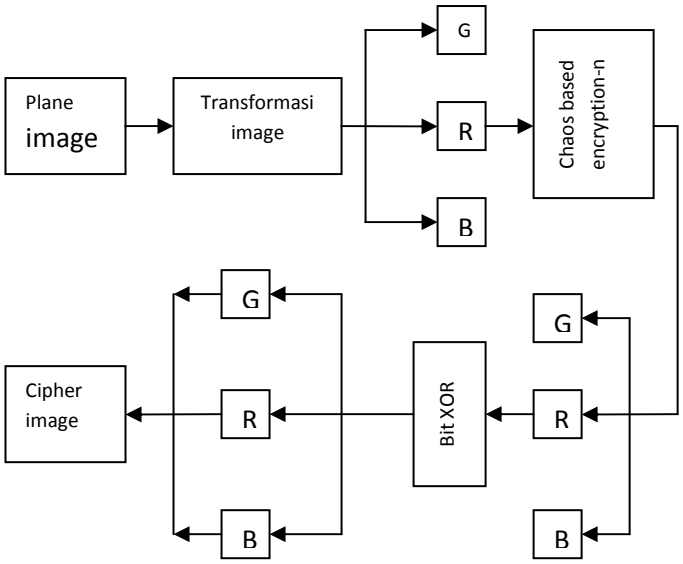

Fig. 3. Encryption process

V. EXPERIMENTAL RESULT

The experimental analysis of proposed technique is based on Histogram analysis through Mat Lab. Histogram analysis show the distribution of pixel values between plane image and cipher image, if Histogram of plane image and cipher image has significant diversity then we can say cipher image does not give any clue to perform brute force or cryptanalysis attack on the encryption algorithm. We take Lena plane image with the size 256*256 as shown in Fig 4. The histogram of this plane image is shown in Fig. 5. We use frequency parameter w and X0, X1 as the keys. Using X0 = 0.011, X1 = 0.021 and w = 08071982, the encrypted image is shown in Fig. 6 and corresponding histogram of encrypted image is shown Fig. 7. Chaos system is reversible in nature after Decryption we get back the original Lena image as shown in Fig. 7. Proposed technique is based on single channel encryption. We encrypt only R component of the plane image and leave other G and B component as such after combining these component we get the cipher image. Fig. 7 shows the Histogram of 'Original R component and Fig. 8 shown the Histogram of corresponding encrypted R component.

Fig. 4. Original Plane Lena image

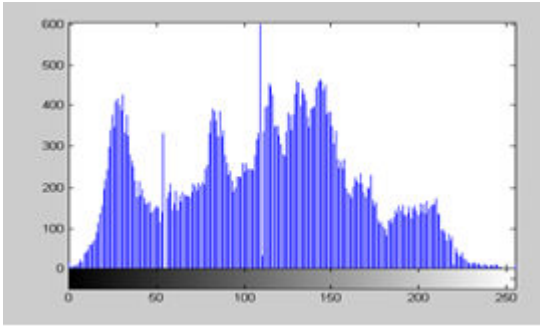

Fig. 5. Histogram of Plane Lena image

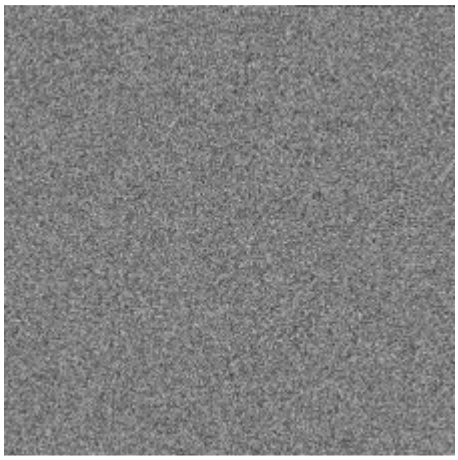

Fig. 6. Encrypted Lena Image

VI. SIMULATION ANALYSIS OF SECURITY

To determine the proposed technique is robust, we use to perform analysis and testing of the encryption algorithm sues different parameter, like Histogram analysis is used to decide the colour distribution between the plane image and cipher image. Both the Histogram gives the significant difference to decide the robustness of encrypted algorithm.

Fig. 4. Represent the Histogram of original lena image and Fig. 5. Represent the histogram of corresponding encrypted image. Both Histograms has significant difference which shows there is no possibility of brute-force attack. Similarly from the Fig. and Fig. shows the Histogram of original R channel and encrypted R channel, both the Histogram shows the significant amount of difference due to their pixel distribution. In our proposed algorithm we used w and the initial value X0,X1 as a secret key. *Henon* like chaotic system is very sensitive to initial condition and parameter. The experimental result demonstrates the encryption algorithm is very sensitive to the secret key. In our experiment if we change the secret

Fig. 7. Decrypted Lena Image

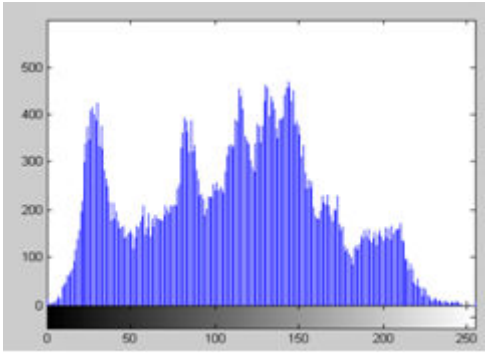

Fig. 8. Histogram of original R component

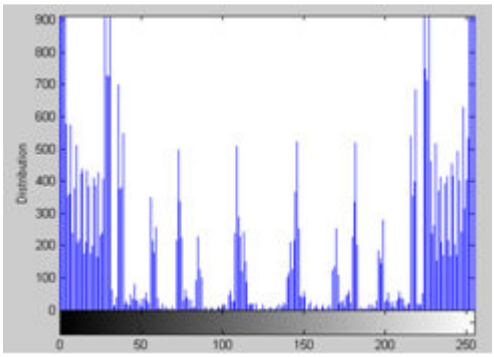

Fig. 9. Histogram of Encrypted R component

Key X0 from X0= 0.001 to X0= 0.0000000001 the resultant encrypted image become entirely changed form original image. We take the different value of secret key for calculating the correlation coefficient between plane image and cipher image and also find the Entropy of encrypted image for different key value, and then we find the average correlation coefficient 0.000014 and average entropy 7.85200. The average Calculation of correlation and entropy determine the quality of encrypted image. The higher value of entropy and lower correlation between pixel values of encrypted image determine the safe encryption algorithm. The average result of correlation coefficient and Entropy shows the guarantees of security of proposed scheme under any cryptanalysis.

VII. CONCLUSION

this paper proposed a new colour image encryption algorithm based on *Henon* like chaotic map. The encryption process applied on any RGB channel. The selected channel goes through the one dimensional *Henon* like chaotic map to produce the random bit stream. This random bit stream bit XOR with the original pixel value of selected channel to produce the encrypted image. The proposed scheme has multi-dimensional large key space to resist the all possible type of brut-force attack. Several Experiments were carried out with numerical analysis, to shows the robustness of proposed scheme. In the future work we intend to make our system to achieve more flexible, reliable and higher level of quality performance in real time system.

ACKNOWLEDGEMENT

The study taken up during perusing M.Tech (computer science & Engineering) in partially supported by IT infrastructure development project, Department of Information Technology, Govt of India.

REFERENCES

1. Chen Wei-bin, Zhang Xin, *Image Encryption Algorithm Based on Henon chaotic System*, International Conference on image Analysis and Signal Processing, 2009, pp. 94-97.
2. Li Chuanmu, Hong Lianxi, *A New Image encryption scheme based on Hyper chaotic Sequence,* IEEE International Workshop on Ant counterfeiting, Security, Identification, IEEE 2007, pp. 237-240.
3. Long Min, Huang Lu*, Design and Analysis of a novel Chaotic Image Encryption*. International conference on Computer Modeling and Simulation(ICCMS' 10), Vol 1,2010.pp. 517-520.
4. S. Behnia, A. Akhshani, H. Mahmodi and A. Akhavan, *A novel Algorithm for image Encryption based on Mixture of Chaotic Maps*, Chaos, Solutions and Fractals, Vol. 35, 2008, pp. 408-419.

5. Kocarev L, Chaos-based Cryptography, a brief overview. IEEE Circ Syst2001,1.6-21.
6. D. Xiao, X. Liao and P. Wei, *Analysis and Improvement of a Chaos-Based Image Encryption Algorithm*, "Chaos Solution & Fractials, Vol.pp.40,2007.
7. Y. Wanga, K.W. Wanga, X. F. Liao and G. R. Chen, *A New Chaos-Based Fast Image Encryption Algorithm,* Applied Soft Computing, Vol. 11, No. 1, 2011, pp. 514-522.