iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Image Encryption Algorithm for Bulk of Image Data Using Henon Chaotic Approach

Divya Aarushi[1], Sunil Ahuja[2]
[1]Research Scholar, [2]Assistant Professor, Department Of Computer Engineering
Doon Valley Institute of Engineering & Technology, Karnal

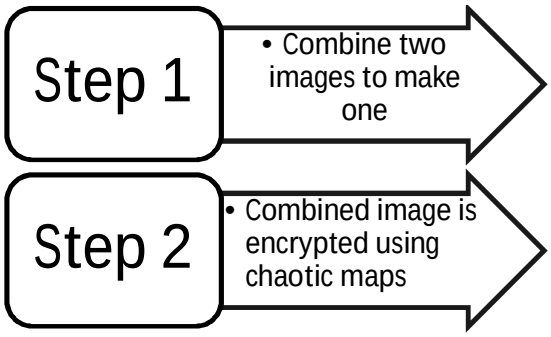
Abstract--In this paper deals with encryption using algorithm which is very efficient in case of bulk of image data. The idea for proposing the algorithm is to provide more security. Proposed algorithm for combining two images with the help of Henon Chaotic Approach.
Keywords: Image Encryption, henon chaotic Algorithm, bulk data, Arnold cat map.

I. INTRODUCTION

To transmit image data securely, various encryption algorithm have been made. The exchange of data in electronic form, information safety is becoming important in storage of data and transmission. In industrial process, widely using image, it is necessary to protect data from unauthorized access. For transmitting the secret or important data over the internet have become the need for fast and safe communication network to achieve the security integrity of information exchanged.
Digital images are exchanged over various types of networks. Sometimes, large part of information is either confidential or private. So, for this Encryption Process is preferred for transmitting the data safely. There are various encryption systems for encrypt and decrypt image data, however it can be argued that there is no single algorithm that satisfies the different image types. Image data have special features like bulk capacity, high redundancy and correlation among pixels, even they are huge in size, which together create difficulty in processing traditional algorithm methods and results in slow down the process. For transmission, an image have their own requirements such as: real-time processing, fidelity reservation, image format consistence and data compression. Simultaneously, fulfillments of these above requirements along with high security, high quality demands, have presented great challenges to real-time imaging practice. Many research work has been done on image encryption techniques to achieve more efficient performance and for increasing the security of transmission. Considering, that it is not sufficient to achieve secure data with performance. This paper explores the bulk of image data using henon chaotic. The rest of the paper is organized as follows: Section II provides description of proposed algorithm. Section III includes experimental results, followed by conclusions in Section IV. Finally references in Section V.

II. PROPOSED IMAGE ENCRYPTION ALGORITHM

We have designed a new image encryption algorithm for bulk of image data. It has 2 steps:



Step 1 Take two images and combine them to make one using most significant bit each image. One pixel of image takes 8 bits for storage. This combination image seems to be encrypted. Nobody can identify whether it is one image or combination of two using visual detection. So, we require next step.
Step 2 Combined images from last step is encrypted using chaotic maps. In our algorithm, we have used Henon chaotic map[11]

for encryption.

A. Henon Chaotic Encryption Algorithm

It includes two steps. First, the positions of the pixels of original image are shuffled by Arnold cat map. Second, pixel values of the shuffled image are encrypted by Henon's chaotic system.

1) Encryption By Arnold Cat Map: To disturb the high correlation among pixels, we adopt Arnold cat map to shuffle the positions of pixel of original image. The Arnold cat map is a two-dimensional invertible chaotic map. Without loss of generality, we assume the dimension of the original grayscale image I is M × M. It is described as:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(M) \qquad (1)$$

Where c & d are positive integers. The (x_{n+1}, y_{n+1}) is the new position of original image, and the (x_n, y_n) is the original position of the original image. where $n = 0,1,2,\ldots$. After iterating N times, there exist positive integers T, such that $(x_{n+1}, y_{n+1}) = (x_n, y_n)$. The period T depends on the parameters c , d and the size M of the original image. After several iterations, the correlation among the adjacent pixels can re-disturbed completely. However, the periodicity of Arnold cat map should degrade the security the encryption, because the possible attacks may iterate the Arnold cat map continuously to reappear the original image. There are no differences between the original-image and cipher-image on the statistical properties. At the same time, the key space of positive integers is limited. Therefore, we adopt Henon chaotic system to change the pixel values next to improve the security.

2) Encryption By Henon Chaotic System: Henon chaotic map is first discovered in 1978, which is described as following:

$$\begin{aligned} x_{i+1} &= 1 - ax_i^2 + y_i \\ y_{i+1} &= bx_i, i = 0,1,2,\cdots \end{aligned} \qquad (2)$$

In our scheme, two variables of the Henon chaotic map are adopted to encrypt the shuffled-image. The encryption process consists of three steps of operations.

Step1: The Henon chaotic system is converted into one-dimensional chaotic map. The one-dimensional Henon chaotic map is defined as:

$$x_{i+2} = 1 - ax_{I+1}^2 + bx_i \qquad (3)$$

Where a =0.3 , b € [1.07,1.4] .The parameter a ,the parameter b , initial value *x0* and initial value *x1* may represent the key.

Step2: After image shuffle, we adopt Henon chaotic map to change the pixel values of the shuffled-image. First, Henon chaotic map is obtained by formula(3). Then transform matrix of pixel values is created.

Step3: The exclusive OR operation will be completed bit-by-bit between the transform matrix of pixel values and the values of the shuffled-image. We can obtain the cipher-image.

Since the chaotic systems are deterministic, the receiver can reconstruct the same shuffled-image exactly using the same secret keys. Then the anti-process of image shuffle is described as:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}^{-1} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod(M) \qquad (4)$$

B. Advantages of Proposed Algorithm

The algorithm reduces the encryption time and transmission cost.
The Algorithm increases the transmission speed

C. Benefits of Using Henon Chaotic System

The algorithm has a large enough key space to resist all kinds of brute force attacks.
The new encrypted arithmetic not only shuffle the pixel positions of the original-image, but also change the grey values of the original-image.
The encryption algorithm is very sensitive to the secret keys.
The operation time of the encryption algorithm is shorter than the 3D Arnold cat map.

III. EXPERIMENTAL RESULTS

Fig: Warning box if any non-numeric key value is entered

Fig: Warning message if non integer values of c, d or no of iterations is entered

Fig: Image encryption when the user enters second image

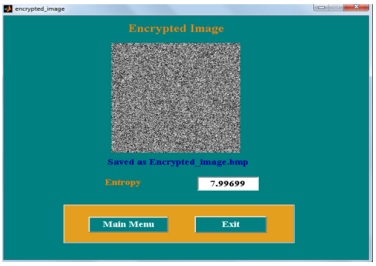


Fig: Encrypted Image

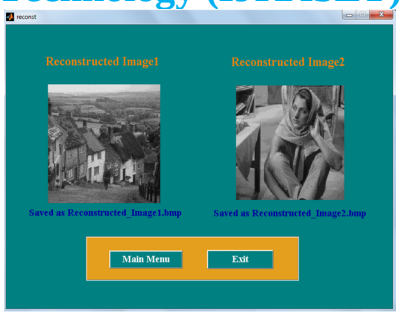


Fig: Decrypted Images at receiver's side when the receiver enters correct key values

IV. CONCLUSIONS

High redundancy and bulk capacity generally make encrypted image data vulnerable to attacks via cryptanalysis as the opponent can gain enough ciphertext samples (even from one picture) for statistical analysis.

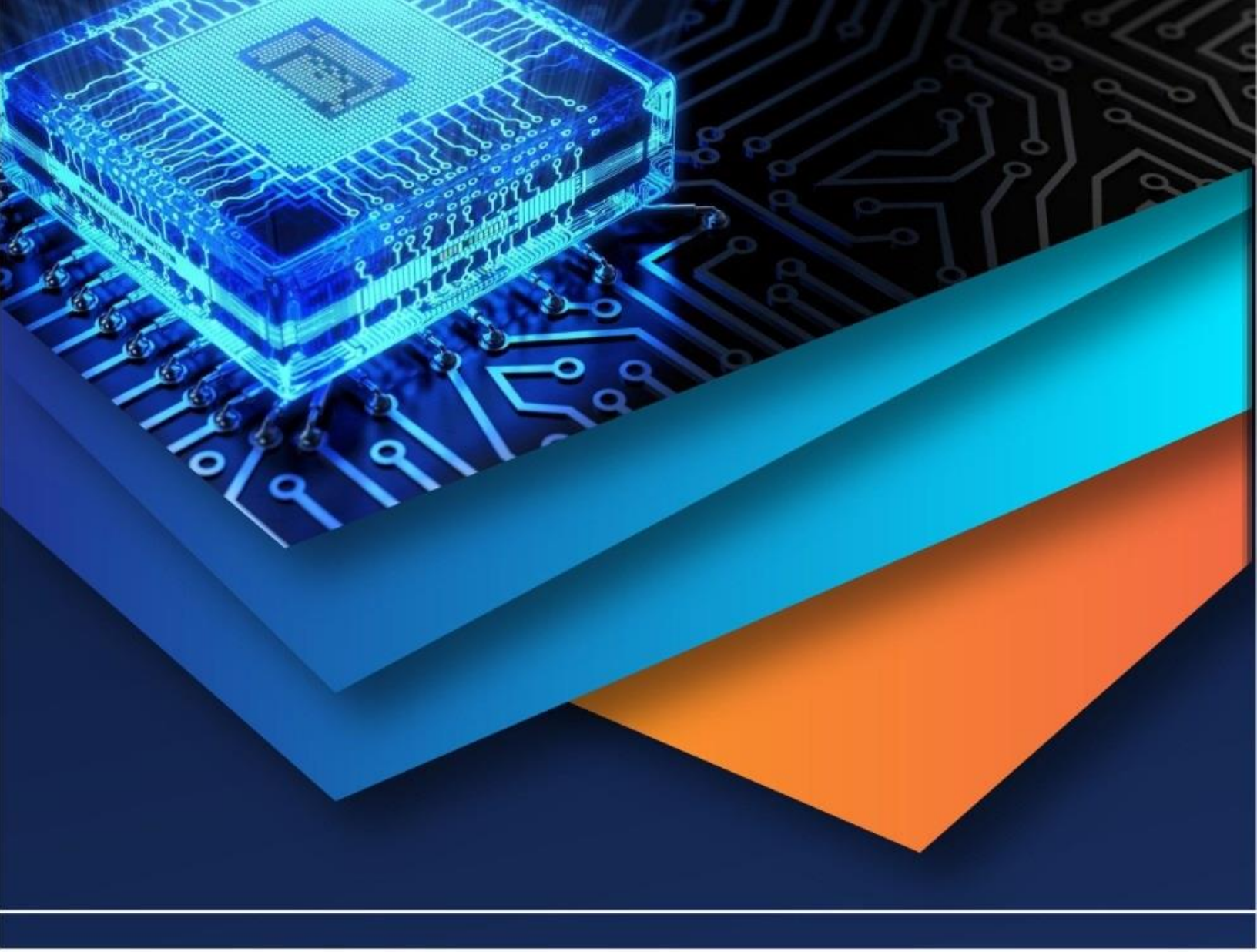
Image data have strong correlations among adjacent pixels, which makes fast data-shuffling quite difficult. Statistical analysis on large numbers of images shows that averagely adjacent 8 to 16 pixels are correlative in the horizontal, vertical, and also diagonal directions for both natural and computer-graphical images. This goal is not easy to achieve under only a few rounds of permutation and diffusion.

Image encryption is to be carried out in combination with data compression. The main challenge is how to ensure reasonable security while reducing the computational cost without downgrading the compression performance.

Human vision has high robustness to image degradation and noise. Only encrypting those data bits tied with intelligibility can efficiently accomplish image protection .

REFERENCES

[1] Jiri Fridrich, "Image encryption based on chaotic maps",1997.
[2] Nikolaos G. Bourbakis, "Image Data Compression-Encryption Using G-Scan Patterns",1997
[3] Jui-Cheng Yen and Jiun-In Guo, "A New Image Encryption Algorithm And Its Vlsi Architecture",1999.
[4] , S. S. Maniccam, N. G. Bourbakis, "Scan Based Lossless Image Compression And Encryption" ,1999.
[5] Jui-Cheng Yen and Jim-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption",2000.
[6]Droogenbroeck and Benedett "Selective Encryption Methods for Raster and JPEG Images", 2002
[7] Aloka Sinha and Kehar Singh, "A Technique for Image Encryption using Digital Signatures", 2003.
[8] Zhi-Hong Guan , Fangjun Huang and Wenjie Guan,"Chaos-based image encryption algorithm", 2005
[9] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "Modified AES Based Algorithm for Image encryption", 2007
[10] Mohammad Ali Bani Younes, Aman, "Image Encryption Using Block-Based Transformation Algorithm", 2008
[11]Chen Wei-bin, Zhang Xin, "Image Encryption Algorithm Based on Henon Chaotic System", 2009.
[12] Ling Li, Weinan Wang and Jinjie , "A novel image encryption algorithm based on high-dimensional compound chaotic systems", 2011.
[13] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry, "Efficiency and Security of Some Image Encryption Algorithms", 2008.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY