JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Henon Map based Chaotic Cryptosystem

[1]Vishwas C.G.M, [2]R Sanjeev Kunte

[1]Assistant Professor, [2] Professor

[1]Department of Information Science & Engineering,

[1]J.N.N College of Engineering, Shivamogga, Karnataka, India

Abstract : The security of digital data has become a prime priority and thereby encryption is a mechanism to ensure the safety of digital data. In this paper, a chaotic Henon based cryptosystem is proposed that encrypts digital images by choosing the keys from both the key sequences generated by the Henon map. A random number is generated which is indexed as a location/position of the key to be picked that is to be bitxored with the pixel of the image. The choice of the key in the chaotic sequence selected is mainly determined by the division operator. Results show that this system is sensitive to security keys.

IndexTerms **- Chaotic Cryptosystem, Henon Map.**

I. INTRODUCTION

In the past decades, securing digital data has received prime importance in the area of information security. There exists three prime ways in which digital data can be secured from unauthorized access, such as steganography, watermarking, and cryptography [1]. Moreover, images vary from texts and are distinguished by the huge volume of data. And major concern lies in providing security to information employing encryption, which is used in several areas such as telemedicine, the military, the Internet, etc. Various encryption methods have been proposed such as DES, IDEA, and RSA [2-4]. But such implementations are not effective as huge multimedia data persists. Also, because of the slow processing speed, such algorithms possess a vast amount of latency [5]. For these reasons, conventional schemes can not be used. Hence, there is a requirement to develop encryption algorithms to provide security to multimedia data. And presently, chaotic-based encryption algorithms have gained much popularity to provide a solution. Moreover, due to inherent features of chaos, like pseudo randomness, sensitivity to initial conditions and system parameters, and ergodicity, chaotic maps have gained wide usage to encrypt images in present days and many chaos-based image encryption schemes are proposed.

II. LITERATURE SURVEY

Mahmoud Ahmad Al-khasawneh et.al [6] proposed an improved chaotic scheme. Here, an external key is considered along with the henon, logistic and gauss-based iterated maps that have already been generated. A key matrix is generated by merging all of the above maps. The process involves an XOR and multiple key generation. The security of this algorithm is evaluated through experimental analysis and assessment of this scheme is done on the satellite images dataset. The main advantage of this algorithm is that it is a multi-chaotic system that can solve general issues which are associated with encryption algorithms on low-dimensional chaotic map. The implementation is secure and gives much importance to privacy. This scheme is efficient but has the disadvantage in that it needs high computational time and power.

Tong Zhang et.al [7] proposed a new chaos-based system called LS chaotic system which uses Logistic and Sine map (LS), which is based on substitution and permutation network(SPN). This new LS system shows a random behavior and is sensitive to initial values and parameters. This SPN work is a new image based chaotic encryption algorithm. The results prove that implemented scheme is efficient in encrypting images and the algorithm can be successfully applied to provide security for digital data.

Jianming Liu and Huijing Lv [8] propose a new chaotic Duffing-Lorenz algorithm (DL) which is six-dimensional in nature and which is realized as a complex structure. This 6 D-L algorithm and the proposed dynamic mapping features are required for the encryption of images in cryptography. In the proposed algorithm, most required chaotic features are used in chaotic encryption much after designing a dynamic mapping.

Sukalyan Som and Atanu Kotal [9] use more than one chaos-based map for confusion and diffusion grayscale images. They use the concept of changing the location of pixels and changing the intensity of the plain image. Arnold Cat Map scrambles the plain image. One-dimensional Logistic Map generates chaotic sequences. Then, in each iteration, the scrambled image is encrypted by the generated Logistic map from which the logistic chaotic sequences have been generated.

Sanjay Kr et.al., [10] proposed a chaos-based scheme in which the logistic map iterates and simultaneously the look-up table is dynamically updated. This algorithm has a feedback mechanism. The advantage of this scheme is that both the encryption and decryption processes tend to be fast as the count of iterations is minimized.

Hikmat N. Abdullah, Hamsa A. Abdullah [11] developed a chaotic encryption scheme which is an efficient technique using a bunch of chaotic maps consisting of 3 stages namely confusion, shuffling, and diffusion. This robust technique consists of three stages based on generating chaotic sequences and shuffling pixels and can overcome the weakness that exists in other

encryption algorithms. The obtained results prove that this scheme significantly increases the security and also the efficiency of the algorithm because it increases the count of mutual secret keys. The algorithm is tested for grayscale images that can be also applied for color images also.

P. Ping et.al., [12] propose a scheme that is based on permutation on digit level and diffusion applied on the block. This method can alter the histogram plot of the image, which makes it complicated for attackers to perform statistical analysis after the permutation process. The pixel matrix is generated from an image which is divided into three specific digital matrices, is then shuffled with the help of the Henon map. The usage of both the pixel-level and the bit-level permutation and their combination has a greater advantage in this scheme. The design incorporates a fast diffusion scheme which provides a solution to Cipher Block Changing based diffusion problems which run on lesser efficiency. This scheme also employs an image feature that results in the generation of the keystream that dependents directly on the plain image. This resists well known chosen-plaintext attack. The obtained results show that this algorithm encrypts digital input to random cipher and also efficiently resists the usual attacks. The advantage of using this algorithm is that it provides a high level of security and also high efficiency for an image encryption cryptosystem.

III. CHAOTIC HENON MAP BASICS

Michel Hénon introduced the Henon map. Henon map happens to be one of the widely studied topics of the discrete time-based dynamical system which shows chaotic behavior. It takes a point (x_n,y_n) in the plane and maps it to a new point. The Henon map is as follows:

$$x_n + 1 = y_n + 1 - a * x_n * x_n \quad (1)$$

$$y_n + 1 = b * x_n \quad (2)$$

a & *b* are the two parameters that are considered in the map and the map mainly depends on these two parameters. The values of *a* & *b* are 1.4 & 0.3 respectively for the classical Henon map as shown in Fig. 1. The map may be chaotic, intermittent, or converge to a periodic orbit for other values of *a* & *b*.

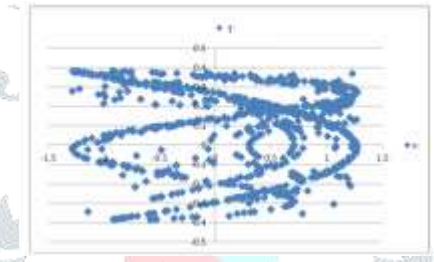

Fig. 1 Henon Map

IV. HENON BASED CHAOTIC CRYPTOSYSTEM

The Henon chaotic encryption process considers an input image. The generation of Henon sequences is designed and implemented in a different module from which the Henon chaotic x and y sequences are generated which is used in the encryption process. This description of Henon sequence generation is given in section 4.2. Fig. 2 shows the Henon based chaotic encryption process.

Initially, *a* and *b* require an initial value. Then, after both the henon chaotic x and y sequences are generated, they are retrieved for encryption. The determination of **key** to be selected for encryption is based on the division operation which determines from which sequence, that is, whether from Henon x sequence or y sequence, a key must be selected for encryption. This key is then bitxored with the RGB converted gray image value of the pixel of the considered input image, and thus the **Cipher** is obtained in the encryption process.

The step-wise flow of the encryption algorithm is as follows.

4.1 The Henon based chaotic encryption process

The process of encryption in steps is as follows

Step 1: Input a Color image ‘ip’ of dimension 3 * M * N where ‘M’ is the height and ‘N’ is the width of the image
Step 2: Convert the RGB image to a gray image, and read it into matrix ‘ip’
Step 3: Initialize parameters *a* and *b* and generate the chaotic Henon x and y sequences
Step 4: Perform read operation of pixels on ‘ip’.
Step 5: Consider each pixel x_a be in the range 0 to 255 from ‘ip’
Step 6: Generate a random number, *RN*
Step 7: Apply bitxor operation between x_a and the key selected by indexing *RN* as a location to either x or y Henon sequence based on the division operator
Step 8: Write the obtained value as a cipher into matrix ‘Cipher’
Step 9: Run Steps 6 to 8 for each of the pixels.
Step 10: Display ‘Cipher’ as Cipher image

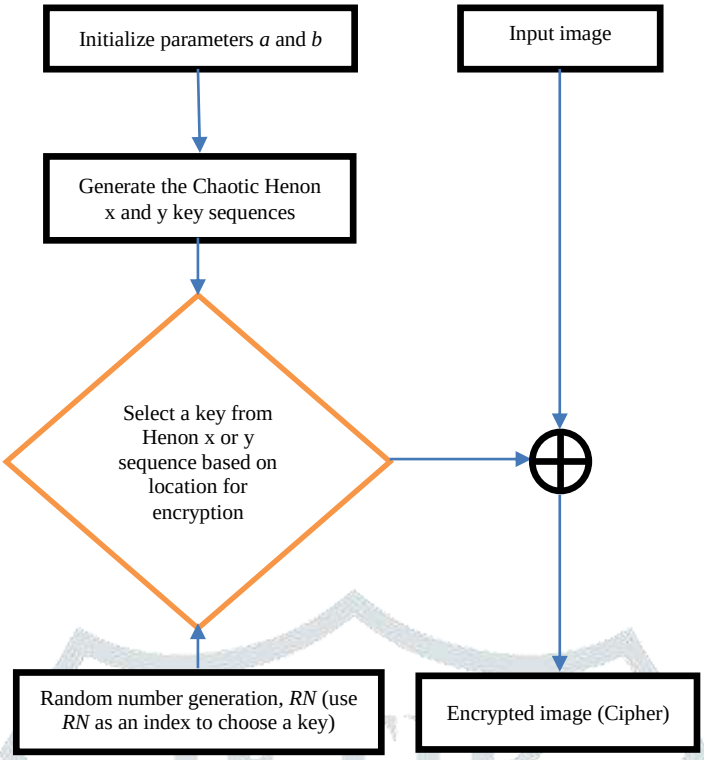

Fig. 2 The Henon based Chaotic Encryption process

The chaotic image decryption process is exactly the reverse of encryption.

4.2 Chaotic Henon x and y sequences generation

Step 1: Initialize values for a and b

Step 2: For n belongs to range 0 - (P*Q)

$$x_n + 1 = y_n + 1 - a * x_n * x_n$$

$$y_n + 1 = b * x_n$$

where P and Q being the size of the RGB to grey converted input image. Both x and y sequences consists of the number of keys generated which are equal to the size of the **P*Q**.

V. EXPERIMENTAL ANALYSIS AND RESULTS

The obtained results for the chaotic Henon based cryptosystem are presented in this section. The implementation is done in MATLAB. Standard images are considered for experimentation purpose such as Lena, Barbara and Flowers. The obtained results are presented as follows:

5.1 Inputs and Outputs of the Cryptosystem

The Lena image is input (Fig. 3(a)) to the cryptosystem. Fig. 3(b) shows the cipher as part of the result of the encryption. It is observed from Fig. 3(b) that no clue about the input image is revealed in the cipher. On execution of decryption, the original image(decrypted image) is obtained successfully (Fig. 3(c)).

Fig. 3(a) Input image

3(b) Cipher

3(c) The decrypted image

5.2 Histogram

Histogram analysis evaluates the security of the implemented chaotic cryptosystem, Fig. 4(a) is the histogram of the input image. Fig. 4(b) depicts the histogram of obtained image cipher.

Fig. 4(a) shows pixels are unequally distributed. Fig. 4(b) illustrates that in the histogram of the cipher, the distribution of pixels is almost uniform. Similar histograms are also obtained for the cipher of Flowers and Barbara images also.

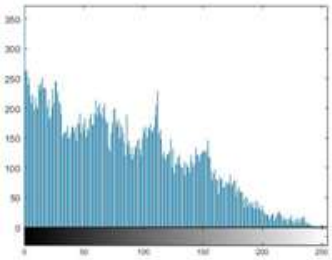

Fig. 4(a) Histogram of the Input (Lena) image

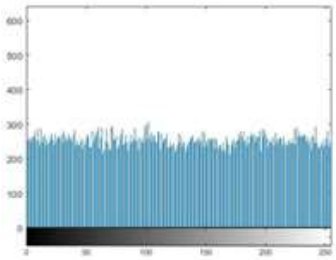

Fig. 4(b) Histogram of Cipher (Lena) image

5.3 Mean Squared Error (MSE) & Peak Signal-To-Noise Ratio (PSNR)

The MSE and PSNR are evaluated and tabulated in Table 1.

Table 1: MSE and PSNR

Images	MSE	PSNR
Barbara	98.9157	28.2121
Flowers	86.9139	28.7739
Lena	70.4580	29.6854

It is shown in Table 1 that all four images have high MSE and low PSNR values.

5.4 Entropy

Table 2: Entropy of input and cipher image

Images	Input Image	Cipher Image
Barbara	7.4328	7.9950
Flowers	7.1818	7.9923
Lena	7.4995	7.9916

It is observed that in Table 2 that the entropy values of the input digital image and the obtained cipher of all the four images are nearer to the ideal value 8.

5.5 Number of Changing Pixels (NPCR) and Unified Average Changing Intensity (UACI)

Table 3 lists the NPCR & UACI values of the proposed algorithm.

Table 3: NPCR & UACI

Image	NPCR Input & Cipher	UACI Input & Cipher
Barbara	0.98842	0.30332
Flowers	0.98846	0.34395
Lena	0.98842	0.33572

The obtained NPCR values are nearer to the ideal value of 0.99 and the values of UACI of all the images are nearer to 0.33.

5.6 Corr2

Correlation Coefficient returns the 2-D correlation coefficient between two arrays. It can range in between in an ideal value from –1 to +1. The Corr2 values for Henon chaotic encryption are presented in table 4.

Table 4: Correlation Coefficient **(Corr2)**

Corr2 of Input Image & Cipher Image		
Barbara	**Flowers**	**Lena**
-0.081899	0.027337	-0.039645

The correlation coefficients of the proposed algorithm are obtained which reside in the specified range.

5.7 Key Sensitivity

In the encryption process, the seed is initialized to 5 and the parameters a and b are initialized to 1.4 and 0.3 at both the sender and receiver side and hence resulting in a successful decryption of the cipher. Suppose, at the decryption end, the seed is taken as 5 itself and the parameters are initialized as a = 1.400001 and b = 0.300001, which leads to unsuccessful decryption of the output image as shown in Fig 5.

Fig. 5(a) The original image

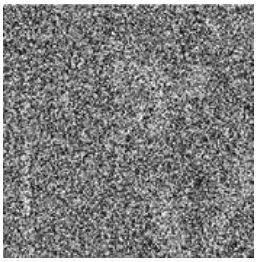

Fig. 5(b) Output (Lena) image, decrypted with wrong keys

with a = 1.400001 and b = 0.300001

The sequence of random numbers, *RN* generated depends on the seed value initialized. Hence the seed value, and the parameters *a* and *b* act as security keys in this cryptosystem and determine the successful decryption of the cipher.

VI. CONCLUSION

In the present scenario, the security of digital data has received vast importance. Also, for its many advantages, chaos is being used for encryption. In the proposed work, a new chaotic Henon based cryptosystem that is sensitive to keys is presented. A simple Henon map is made used in the generation of the keys. But the initialization of seed value and security keys makes this chaotic cryptosystem strong and the generation of the key sequences unpredictable and resists attacks on the cryptosystem. Here, the keys from both Henon x and y sequence are made use in the generation of the cipher, which doubles the keyspace. The experimental results yield high MSE values low PSNR values. The entropy values are closer to 8. Also, the evaluated NPCR and UACI are in the expected range. To conclude, the experimental results obtained show that the proposed method is efficient in securing the digital image. Therefore, the proposed Henon based chaotic cryptosystem can be used to securely transmit the digital image.

REFERENCES

[1] [1] Vinothkanna M. R, A Secure Steganography Creation Algorithm for Multiple File Formats, Journal of Innovative Image Processing(JIIP), 1(01), pp. 20-30, 2019.

[2] Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., January 1977.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice-Hall, New Jersey, 1999.

[4] S. Wang and G. Liu, "File Encryption and Decryption System Based on RSA Algorithm", 2011 International Conference on Computational and Information Sciences, Chengdu, China, pp. 797-800, 2011.

[5] B. Furht and D. Socek, "Multimedia Security: Encryption Techniques", IEC Comprehensive Report on Network Security, International Engineering Consortium, Chicago, IL, 2004, pp. 335-349.

[6] Mahmoud Ahmad Al-Khasawneh, Siti Mariyam Shamsuddin, Shafaatunnur Hasan, Adamu Abu Bakar, An Improved Chaotic Image Encryption Algorithm, International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2018, Malaysia, pp. 1-8.

[7] Tong Zhang, Yicong Zhou, C. L. Philip Chen, A New Combined Chaotic System for Image Encryption, International Conference on Computer Science and Automation Engineering (CSAE), 2012, China, pp 331-335.

[8] Jianming Liu, Huijing Lv, A new Duffing-Lorenz Chaotic Algorithm and Its Application in Image Encryption, International Conference on Control Engineering and Communication Technology (ICCECT), China, 2012, pp 1022-1025.

[9] Sukalyan Som and Atanu Kotal, Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps, National Conference on Computing and Communication Systems (NCCCS), India, 2012, pp. 1-5.

[10] Sanjay Kr. Meena, Nitesh Chouhan, D.N. Vyas, Mamta Rani, A More Secure Chaotic Cryptography Approach Using Hyperchaotic Logistics Map, Fifth International Conference on Communication Systems and Network Technologies, India, 2015, pp. 618-623.

[11] Hikmat N. Abdullah and Hamsa A. Abdullah, Image Encryption Using Hybrid Chaotic Map, International Conference on Current Research in Computer Science and Information Technology (ICCIT), Iraq, 2017, pp. 121-125.

[12] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, A Chaos Based Image Encryption Scheme Using Digit-Level Permutation and Block Diffusion, in IEEE Access, vol. 6, pp. 67581-67593, 2018.