Improved Image Encryption Algorithm using Chaotic Map

Joshi Rohit A
B.TECH Information
Technology, VJTI
Mumbai, INDIA

Joshi Sumit S
B.E Electronics, V.E.S
Institute of Technology
Mumbai, INDIA

G. P. Bhole
Head of the Department
Information Technology, VJTI
Mumbai, INDIA

ABSTRACT

This paper proposes an improved image encryption scheme over existing scheme. The distinct feature of improved encryption scheme is that it encrypts the image using chaotic maps only without further confusing this encrypted image as illustrated in existing scheme. Further, the advantages over existing scheme are 1) the proposed algorithm is completely retrievable in contrast to the existing algorithm 2) the experimental results of proposed algorithm are better than existing algorithm which governs added security level and 3) lesser computational complexity which governs improved speed performance.

General Terms

Chaos Theory, Evolutionary Algorithms

Keywords

Chaos, Security

1. INTRODUCTION

With the evolution of faster computing technologies the need for highly secured encryption algorithms has become the pick of the time. The increase in multimedia transmission in the past decade has brought the focus from text based encryption systems to image based encryption systems. This transition is because the conventional textual encryption methods did not consider the large amount of correlation between adjacent pixels of an image and thus were proved unsecured. We have proposed an improved version of image encryption algorithm over the existing one [1]. The proposed algorithm encrypts the image using Henon Map which is a discrete time dynamic system which possesses all the properties of chaos. Some of the notable advantages of the proposed algorithm over the existing are 1) the proposed algorithm is completely retrievable in contrast to the existing algorithm 2) the experimental results of proposed algorithm are better than existing algorithm which governs added security level and 3) lesser computational complexity which governs improved speed performance.

Organization of rest of the paper is as follows: Section 2 explains existing algorithm with its drawbacks. Section 3 illustrates the proposed algorithm. Section 4 shows the experimental results and security analysis. Section 5 concludes the paper.

2. LITERATURE REVIEW

Large amount of work has been concentrated on chaotic based encryption in the past decade due to high sensitivity of chaotic maps to initial conditions and intrinsic properties such as pseudo randomness [2-4]. Some were proved to be unsecured [5-7]. To improve the same some scrambling techniques were introduced which were robust to statistical and differential attacks governing high security than those of before. Furthermore, algorithms on chaotic coupling were introduced to add to existing security level but were computationally complex and showed low key space [8].

3. EXISTING ALGORITHM AND ITS LIMITATIONS

Existing algorithm encrypts the image in two stages. The first stage comprises of encrypting the image using Henon map and the second stage confuses this encrypted image using logistic map. The first stage comprises of three steps [9] which are explained in brief. The first step represents the plain image matrix into a row matrix and generates an image dependent array. The second step generates a chaotic sequence using Henon map with initial values dependent on above array. The third step encrypts the image as a function of this chaotic sequence. This algorithm encrypts the image successfully but during decryption of the image the entire image is not recovered. This is because the plain image dependent array generated in the first step is a computed as a XOR of two distinct elements. It is necessary and sufficient condition that one of the two elements should be known for decryption process, since both the elements are unknown, it is not a surprise to conclude that the image cannot be decrypted completely using [1].

4. PROPOSED ALGORITHM

We propose an improved algorithm which overcomes the limitations of the existing. The image encryption algorithm is completed in two steps. The first step generates a chaotic sequence using Henon map defined by [7]

$$\begin{cases} x(n+1) = 1 - ax(n)^2 + y(n) \\ y(n+1) = bx(n) \end{cases} \quad (1).$$

Where a=1.4 and b=0.3 to exhibit chaotic behavior.
With initial values obtained from (3). The second step encrypts each pixel of the plain image as a function of chaotic sequence generated in the first step.

4.1 Initialization of plain image and generation of chaotic sequence using Henon map

Convert the color image of size L X B X D into one dimensional array P.

$$P = (P_1, P_2, P_3 \dots P_H) \qquad (3)$$

Where H=L*B*D

Generate chaotic sequence X and Y by applying H iterations on Henon map with initial values

$$\begin{cases} X_1 = Sum\ of\ intensity\ levels\ of \\ \quad all\ pixels\ of\ P * 10^{-16} \\ Y_1 = Sum\ of\ intensity\ levels\ of \\ all\ diagonal\ pixels\ of\ P * 10^{-16} \end{cases} \qquad (3)$$

Thus we get
$$\begin{cases} X = (X_1, X_2, X_3 \dots X_H) \\ Y = (Y_1, Y_2, Y_3 \dots Y_H) \end{cases} \qquad (4)$$

Generate *chaotic* sequence XO and YO by applying H iterations on Henon map with initial values

$$\begin{cases} XO_1 = X_H \\ YO_1 = Y_H \end{cases} \qquad (5)$$

Thus we get
$$\begin{cases} XO = (XO_1, XO_2, XO_3 \dots XO_H) \\ YO = (YO_1, YO_2, YO_3 \dots YO_H) \end{cases} \qquad (6)$$

4.2 Computation of encryption of the plain image

Compute encrypted matrix Z by applying H-1 iterations on

$$Z_{i+1} = \begin{pmatrix} mod(P_{i+1} + i + 1, 256) \oplus Zi \\ \oplus\ mod(XO_{i+1} * 10^{16}, 256) \end{pmatrix} \qquad (7)$$

Where $Z_1 = (mod(P_1 + 1, 256) \oplus mod(XO_1 * 10^{16}, 256))$ (8)
and $1 \leq i < H$

Thus we get
$$Z = (Z_1, Z_2 Z_3 \dots Z_H) \qquad (9)$$

Here, Z matrix is computed as a function of three distinct matrices 1) plain image matrix P, 2) chaotic sequence XO and 3) Z matrix itself. During decryption process, we know Z matrix and the chaotic sequence XO and thus we can determine the plain image P which is not the case in existing algorithm [1]. Also, since the proposed algorithm doesn't employ any confusion scheme as contrast to existing algorithm the computational complexity is less governing better speed performance.

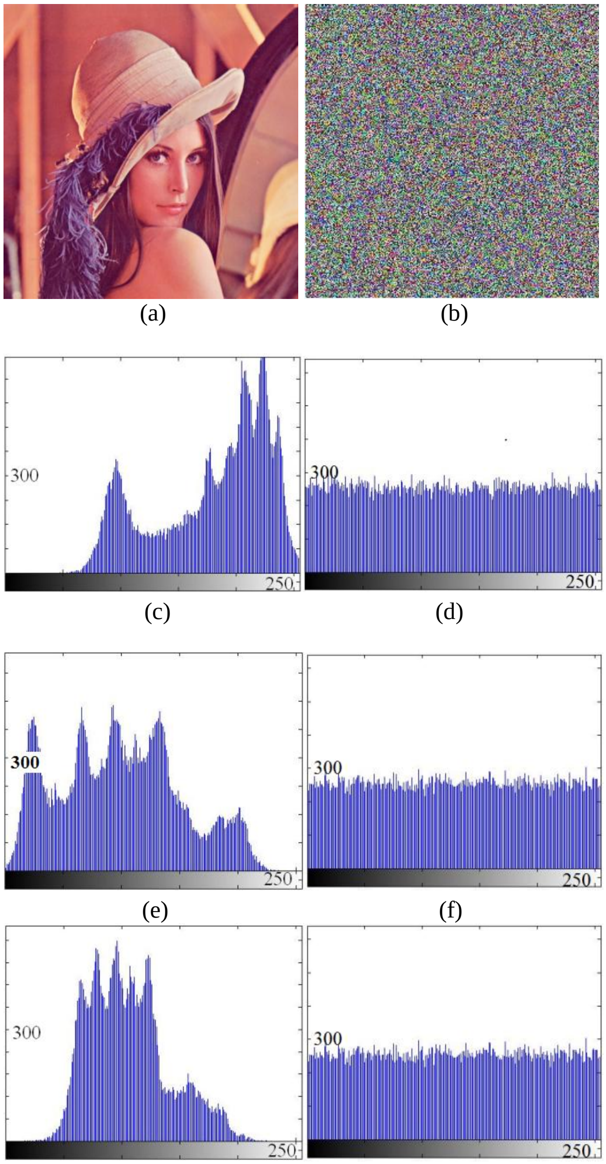
5. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

The current section aims at explaining the security and performance analysis of the proposed color image encryption algorithm. The experimental analysis is done on Lena Image of size 256 X 256 X 3. Note that Fig 1(a) is the plain image and Fig 1(b) is the image encrypted using keys XO_1= 0.4769552954269822, YO_1=0.6673664962345311 which are obtained using (5).

5.1 Statistical Analysis

Statistical Analysis determines robustness against statistical attacks. Statistical attacks analyze at least one of the three following aspects which are 1) the relationship between data elements of plain image and cipher image 2) the relationship between adjacent data elements of cipher image 3) the predictability of a particular data element. Experimental results of these attacks are used to identify following aspects 1) the plain text without prior knowledge of private keys 2) ability to reduce the amount of search needed using brute force attacks.

Thus, to determine the amount of vulnerability to these attacks we employ histogram analysis and correlation analysis.



(a) (b)

(c) (d)

(e) (f)

(g) (h)

Fig 1 : (a) Plain Image (b) Encrypted Image (c) R component of plain image (d) R component of cipher image (e) G component of plain image (f) G component of cipher image (g) B component of plain image (h) B component of cipher image

5.1.1 Histogram Analysis

Fig 1 depicts histogram analysis. Fig 1 shows histogram of red, green and blue component of plain image and the histogram of red, green and blue component of cipher image. It is clearly visible that histogram of cipher image is fairly uniform and it does not leak any amount of information about the plain image.

5.1.2 Correlation analysis between color channels of image

Two dimensional correlation coefficients between the three color channels of plain as well as cipher image are determined in this analysis. These correlation coefficients are calculated using [8]

$$C(AB)=\frac{\frac{1}{H\,X\,W}\sum_i^H\sum_j^W\left(A(i,j)-\overline{A}\right)\left(B(i,j)-\overline{B}\right)}{\sqrt{\left(\frac{1}{H\,X\,W}\sum_i^H\sum_j^W\left(A(i,j)-\overline{A}\right)^2\right)\left(\frac{1}{H\,X\,W}\sum_i^H\sum_j^W\left(A(i,j)-\overline{B}\right)^2\right)}} \tag{10}$$

Where, $$\begin{cases}\overline{A}=\frac{1}{H\,X\,W}\sum_{i=1}^{H}\sum_{j=1}^{W}A(i,j)\\ \overline{B}=\frac{1}{H\,X\,W}\sum_{i=1}^{H}\sum_{j=1}^{W}B(i,j)\end{cases} \tag{11}$$

In the above formula, A depicts one of the three color channels i.e. Red, Blue or Green, Similarly, B represents one of the three color channels i.e. Red, Blue or Green. $\overline{A}$ & $\overline{B}$ represent mean of A and B respectively. H stands for height and W stands for width of the image. Hence, we can compute nine different combinations of correlation coefficients i.e. $C_{RR,}$ $C_{RB,}$ $C_{RG,}$ $C_{BR,}$ $C_{BB,}$ $C_{BG,}$ C_{GR} $C_{GB,}$ C_{GG} for pair of plain and cipher image. Table 1 mentions the experimental results of correlation coefficients and these values signify that the plain and cipher image share a very low correlation amongst themselves [1].

, **Table 1. Correlation between color channels of plain and cipher image**

Plain image Cipher Image	Correlation between plain and cipher image		
	Red channel	**Green Channel**	**Blue Channel**
Red channel	-0.0064	-0.0071	-0.0070
Green Channel	-0.0067	-0.0054	-0.0059
Blue channel	-0.0033	-0.0041	-0.0067

5.1.3 Correlation analysis adjacent pixels of cipher image

The amount correlation between adjacent pixels of cipher image should be as low as possible to sustain statistical attack. Correlation between adjacent pixels is determined using [8]

$$C=\frac{\frac{1}{N}\sum_{i=1}^{N}\left(x(i)-\overline{x}\right)\left(y(i)-\overline{y}\right)}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}\left(x(i)-\overline{x}\right)^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}\left(y(i)-\overline{y}\right)^2\right)}} \tag{12}$$

Where $$\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i\ and\ \bar{y}=\frac{1}{N}\sum_{i=1}^{N}y_i \tag{13}$$

Here x (i) and y (i) amount to ith pair of horizontally and vertically adjacent pixels. Also, N is the total number of pairs of horizontally or vertically adjacent pixels. Table 2 mentions the experimental results of correlation between adjacent pixels. Furthermore these values signify that the encryption scheme significantly reduces the correlation between adjacent pixels [1].

Table 2. Correlation between adjacent Pixels of plain and cipher image

Alignment + image type		Correlation adjacent pixels		
		Red channel	**Green Channel**	**Blue Channel**
Horizontal	Plain	0.9236	0.9632	0.9680
	Cipher	0.0072	-0.0054	0.0069
Vertical	Plain	0.9753	0.9721	0.9857
	Cipher	0.0027	-0.0069	0.0044

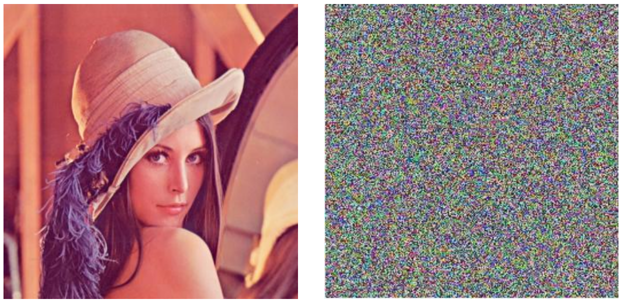
5.2 Key Sensitivity Analysis

An encryption scheme is said to be ideal if it possess high degree of key sensitivity, which in return guarantees security. The key sensitivity is generally observed in two ways (i) the amount of correlation observed between two cipher images when encrypted using keys whose values differ slightly and (ii) correlation observed when the cipher image is decrypted with the correct key and when it is decrypted using key whose value differ from correct one slightly. In the proposed algorithm, the encryption key consists of two parts. Here, we have calculated the correlation between images that are decrypted when one of the two parts of a key are modified slightly.

Table 3 lists the correlation observed when the cipher image is decrypted using Key 1 (correct key) and two different key sets (incorrect key set). Note that Key 2 and Key 3 which are obtained from Key 1 by changing one of the four distinct parts forming the key by unit precision only. These values signify that the proposed encryption scheme offers very high key sensitivity.

The Keys are as follows: Key 1 = (XO_1= 0.4769552954269822, YO_1=0.6673664962345311), Key 2 = (XO_1= 0.4769552954269823, YO_1=0.6673664962345311), Key 3 = (XO_1= 0.4769552954269822, YO_1=0.6673664962345312)

We have also determined the correlation between differently encrypted images as explained above and have realized that correlation values calculated are significantly low governing very high key sensitivity [8]. Fig 2 shows one image retrieved using correct key (Key1) and the other retrieved using slightly different key (Key 2).



(a) (b)

Fig 2 : (a) Decrypted using key1 (correct key) (b) Decrypted using key2 (wrong key)

Table 3. Key Sensitivity Analysis

	Correlation coefficient between the encrypted image using Key 1 and	
	Key 2	**Key 3**
C_{RR}	-0.0067	-0.0039
C_{RB}	0.0048	0.0034
C_{RG}	0.0039	0.0049
C_{GR}	-0.0044	0.0064
C_{GG}	0.0070	0.0058
C_{GB}	0.0053	0.0046
C_{BR}	0.0074	-0.0071
C_{BG}	-0.0047	0.0053
C_{BB}	0.0073	-0.0061

5.3 Entropy Analysis

The entropy of a message can be calculated using [1]

$$H(s) = \sum_s P(s_i) \log_2 \frac{1}{P(s_i)} \qquad (14)$$

Here P (s_i) represents probability of symbol s_i. A true random source must generate ideally 2^8 symbols with each symbol having equal probability. Ideal entropy of H(s) = 8. We have determined the entropy of color cipher image as 7.9976 which is nearly equals 8 and this indicates the cryptosystem is robust against entropy attack. Also, the entropy of plain image was calculated as 7.7599 which enhanced remarkably to 7.9976 in cipher image which indicates increased disorder in cipher image.

5.4 Differential Analysis

An ideal encryption system should be resistant to known plain text attack and chosen plain text attack which employ differential analysis. Thus in order to sustain differential analysis, small difference in the plain image should reflect by a large difference in the cipher image. For this two factor are mainly computed i.e. NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity). NPCR signifies the percentage change in number of pixels between two cipher images whose plain images differ by only one pixel. UACI denotes the average change in intensity between two cipher images. NPCR and UACI are calculated using [1]

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} X\ 100\% \qquad (15)$$

$$UACI = \frac{1}{M\ X\ N} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} X\ 100\ \% \qquad (16)$$

Where M and N are height and width of cipher images, C1 (i, j) and C2 (i, j) represent ith row and jth column of cipher images C1 and C2 respectively.
D (i, j) is defined as [1]

$$D(i,j) = \begin{cases} 0\ if\ C1(i,j) = C2\ (i,j) \\ 1\ if\ C1(i,j) \neq C2\ (i,j) \end{cases} \qquad (17)$$

NPCR and UACI between two images taken at random were observed as 99.6091% & 32.1257%. NPCR and UACI calculated from the proposed encryption scheme yielded values 99.6448% & 33.6182%. These values indicate that the proposed algorithm has greater ability to sustain differential attack than the existing [1].

6. CONCLUSION

This paper introduces an improved image encryption scheme based on chaotic map. The advantage of this encryption scheme is reduced computational complexity and retrievable nature as contrasted with existing scheme. Here, both the parts of the keys are generated using plain image, thus enhancing the ability to resist plain text attacks. Security analysis which includes Statistical analysis, Correlation analysis, Key sensitivity analysis and Differential analysis govern that the proposed algorithm yields a very good performance.

7. REFERENCES

[1] Long Min; Huang Lu,"Design and Analysis of a novel Chaotic Image Encryption,"International Conference on Computer Modelling and Simulation(ICCMS'10), vol 1,2010.pp. 517-520.

[2] N. K. Pareek, Vinod Patidar and K. K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, 2006, pp. 926-934.

[3] H.S. Kwok, W. K. S.Tang, "A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons and Fractals, vol. 32, 2007, pp. 1518–1529.

[4] S. Behnia, A. Akhshani, H. Mahmodi and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos, Solitons and Fractals, vol. 35, 2008, pp. 408–419.

[5] Di Xiao, Xiaofeng Liao, Pengcheng Wei. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons, and Fractals, vol.40,pp. 2191-2199, 2009.

[6] Cahit Cokal, Ercan Solak. Cryptanalysis of a chaos-based image encryption algorithm. Physics Letters A, vol. 373,pp. 1357-1360,2009.

[7] Chengqing Li, Shujun Li, Muhammad Asim, Juana Nunez, Gonzalo Alvarez, Guanrong Chen. On the security defects of an image encryption scheme. Image and Vision Computing, vol. 27, no.9, pp. 1371-1381, 2009.

[8] Patidar, V.; Purohit, G.; Sud, K.K.; Pareek, N.K., "Image encryption through a novel permutation-substitution scheme based on chaotic standard map,"International Workshop on Chaos Fractals Theories and Applications(IWCTA) 2010,pp. 164 – 169.

[9] Ali Kanso, Nejib Smaoui. Logistic chaotic maps for binary numbers generations. Chaos, Solitons and Fractals,vol.40, pp.2557-2568,2009.

[10] Vinod Patidar, N. K. Pareek and K. K. Sud, "A new substitution- diffusion based image cipher using chaotic standard and logistic maps," CNSNS, vol. 14, 2009, pp. 3056-3075.