International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-4 Number-2 Issue-15 June-2014

Design and Implementation of Image Encryption Algorithm Using Chaos

Sandhya Rani M.H.[1], K.L. Sudha[2]

Abstract

Images are widely used in diverse areas such as medical, military, science, engineering, art, advertising, entertainment, education as well as training, increasing the use of digital techniques for transmitting and storing images. So maintaining the confidentiality and integrity of images has become a major concern. This makes encryption necessary.

The pixel values of neighbouring pixels in a plain image are strongly correlated. The proposed algorithm breaks this correlation increasing the entropy. Correlation is reduced by changing the pixel position this which is called confusion. Histogram is equalized by changing the pixel value this which is called diffusion. The proposed method of encryption algorithm is based on chaos theory. The plain-image is divided into blocks and then performs three levels of shuffling using different chaotic maps. In the first level the pixels within the block are shuffled. In the second level the blocks are shuffled and in the third level all the pixels in an image are shuffled. Finally the shuffled image is diffused using a chaotic sequence generated using symmetric keys, to produce the ciphered image for transmission. The experimental result demonstrates that the proposed algorithm can be used successfully to encrypt/decrypt the images with the secret keys. The analysis of the algorithm also shows that the algorithm gives larger key space and a high key sensitivity. The encrypted image has good encryption effect, information entropy and low correlation coefficient.

Keywords

Cryptography, Chaos, Confusion, Diffusion, Entropy

1. Introduction

Multimedia image security in storage and transmission is a major issue in today's world. Encryption is a common technique to uphold multimedia image security. Internet banking, e-commerce, business in general, defence are the major fields where security and privacy is utmost important. This has led to the development of various techniques and adoption of encryption. There are various methods in encryption; one of the most widely used methods is cryptography. Cryptography develops a cryptosystem, which converts an original intelligible image, referred to as plain image, into apparently random cipher image and it also recovers the image back in its original form [6].

Manuscript received June 05, 2014.

Sandhya Rani M.H., Electronics and Communication Engineering, Sapthagiri College of Engineering, Bangalore, India.

K.L.Sudha, Electronics and Communication Engineering, Dayanand Sagar College of Engineering, Bangalore, India.

2. Chaos

Chaos is a promising candidate for cryptography. The highly sensitive behaviour of chaotic maps to the initial conditions is directly connected to the two basic properties of good cipher: confusion and diffusion [4].

Chaos is a ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit extreme sensitivity to initial conditions and have random like behaviour [7].

Chaos theory is based on the observation that simple rules when iterated can give rise to apparently complex behaviour.

3. Chaotic System

Chaotic systems have a number of interesting properties such as sensitivity to initial condition and system parameter, ergodicity and mixing (stretching and folding) properties, etc. These properties make the chaotic systems a worthy choice for constructing the cryptosystems as sensitivity to the initial condition/system parameter and mixing properties [2] are analogous to the confusion and diffusion properties of a good cryptosystem. In an ideal cryptosystem confusion reduces the correlation between the plain image and cipher image while diffusion transposes the pixel value of the coordinate. In other words, the confusion stage changes the position of data while the data itself is modified during the diffusion process [1].

4. Chaotic Mappings Used

Gingerbreadman Map

The Gingerbreadman system is a discrete-time dynamical system. The values of the map are chaotic for a certain initial conditions and initial parameters. The set of chaotic solutions of this map when plotted resemble Gingerbread.

Gingerbreadman Equations:

$$x_{n+1} = 1 - y_n + |x_n|$$

$$y_{n+1} = x_n \quad \textbf{(1)}$$

Here x, y system parameters. For example system acts chaotic for these values x=0.5, y=3.7.

Cubic Map

The Cubic map is a discrete-time dynamical system. It is an example of a dynamical system that exhibit chaotic behavior .Here the one-dimensional map is mapped into a ternary string via symbolic dynamics in order to evaluate the complexity.

Cubic Equation

$$f_r(x) = rx^3 + (1 - r)x \quad \textbf{(2)}$$

The map depends on the value r which is called as bifurcation parameter. This will be usually 3 to produce chaotic behaviour.

Henon Map

The Henon map is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behaviour. The Henon map takes a point (x_n, y_n) in the plane and maps it to a new point given by the equation below.

Henon Equations

$$x_{n+1} = 1 - ax_n^2 + y_n$$
$$y_{n+1} = bx_n \quad \textbf{(3)}$$

The map depends on two parameters, *a* and *b*, which for the classical Henon map have values of $a = 1.4$ and $b = 0.3$. For the classical values the Henon map is chaotic.

Logistic Map

Logistic Map is a polynomial equation of degree 2. Chaotic behaviour can arise from very simple non-linear dynamical equations.

Logistic Equation:

$$x_{n+1} = rx_n(1 - x_n) \quad \textbf{(4)}$$

Where x_n is a value between 0 and 1and it will be usually 0.1 and r is a positive value. Usually for the system to behave chaotic r=4.

5. Proposed Image Encryption Algorithm

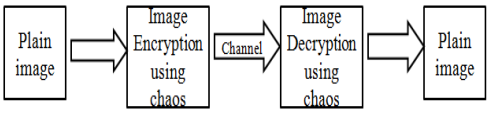

Figure 1: General block diagram of cryptosystem Encryption

The proposed image encryption algorithm has two major steps. Firstly, the correlation among the adjacent pixels is disturbed completely as the image data have strong correlations among adjacent pixels. For image security and secrecy, one has to disturb this correlation. To achieve this, a block and stream based image shuffling scheme is proposed using the three chaotic maps mentioned above. Then the pixel values of the shuffled image are modified by employing Henon map. Encryption is done in two stages confusion and diffusion.

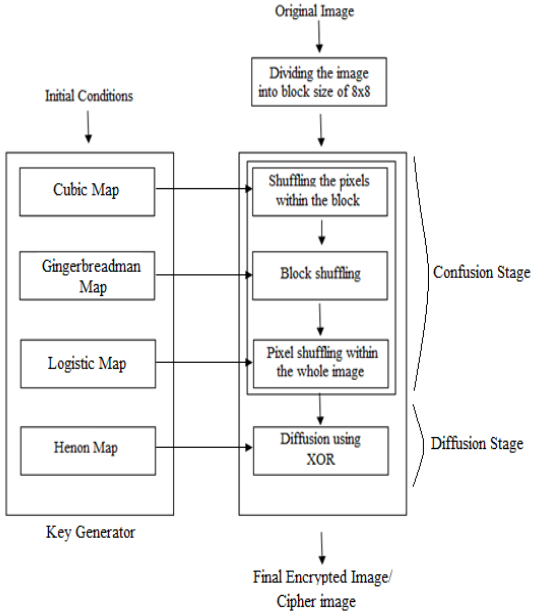

Figure 2: Block Diagram of Encryption Stage.

Confusion stage

The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. Three levels of shuffling are employed in this stage.

The steps followed are:

Step1: An image of size NxN is divided into 8x8 sized blocks.
Step2: The pixels within the block are shuffled using Cubic Map.
Step3: All the 8x8 blocks within an image are shuffled using Gingerbreadman map.
Step4: The pixels in the whole image are shuffled using Logistic Map.

Diffusion stage
In the diffusion stage, the pixel values are modified sequentially by the sequence generated by the chaotic systems. After confusion stage even though the pixels are shuffled the histogram remains unchanged. Here pixel values are modified to get a normalized histogram. Diffusion is performed using XOR operation.

Decryption
Here reverse algorithm of encryption is used to get back the original image using the same chaotic maps with same initial conditions.

6. Results

Results of Confusion stage

Figure 3: Original image

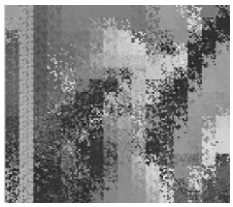

Figure 4: Shuffling within blocks

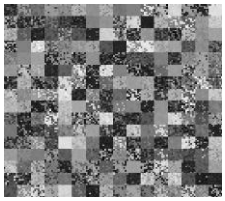

Figure 5: Confused image

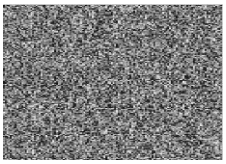

Figure 6: Block shuffling Results of Diffusion Stage

Figure 7: Original image

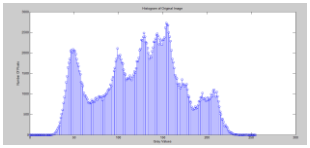

Figure 8: Histogram of original image

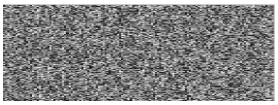

Figure 9: Confused image

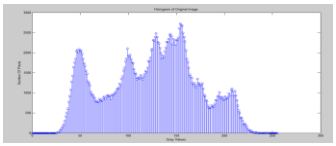

Figure 10: Histogram of confused Image

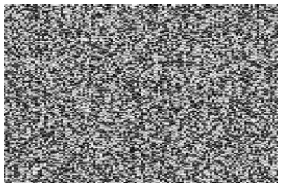

Figure 11: Diffused image

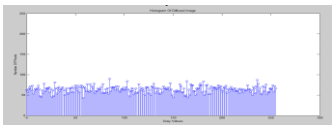

Figure 12: Histogram of diffused Correlation Analysis

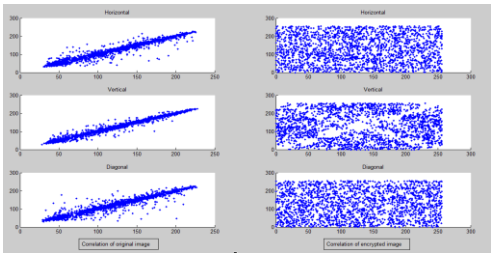

Figure 13: Correlation between two adjacent pixels horizontally, vertically and diagonally.

In this section, the correlation between two vertically, two horizontally and two diagonally adjacent pixels is analysed. In the original image, each pixel is highly correlated with its adjacent pixels either in horizontal or vertical direction and cipher images should have no correlation in the adjacent pixels .Figure 13 shows the distribution of two horizontally, vertically and diagonally adjacent pixels in the plain image and cipher image. To compare the horizontal, vertical and diagonal correlations of adjacent pixels in the plain and cipher images, the following formulae are used to get the correlation co-efficient [7]. The ideal coefficient value of original image will be 1 and for cipher image it will be 0.

$$E(X) = \frac{1}{N}\sum_{i=1}^{N} X_i,$$

$$D(X) = \frac{1}{N}\sum_{i=1}^{N} (X_i - E(X_i))^2,$$

$$cov(X,Y) = \frac{1}{N}\sum_{i=1}^{N} (X_i - E(X_i))(Y_i - E(Y_i)),$$

$$r_{XY} = \frac{cov(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}} \qquad (5)$$

In equation (5) xi and yi are the values of two adjacent position of pixels in the image and N is the total number of pixels present in the image.
Correlation coefficients calculated for the original and encrypted images are given in Table 1. It is clear from Table 1 that the two adjacent pixels are highly uncorrelated.

Table 1: Correlation Coefficient of Two Adjacent Pixels in Two Images.

Direction of adjacent pixel	Plain image	Ciphered image
Horizontal	0.9719	-0.0040
Vertical	0.9850	-0.0333
Diagonal	0.9593	0.0047

Key Space Analysis: Key space gives the total number of different keys that are used in the cryptographic system [8]. There are in total eight initial conditions of chaotic maps used in the algorithm and the initial conditions are x0, y0, r (for Logistic), a, b (for Henon), r (for Cubic), which can be used to generate the secret keys of encryption and decryption. In this case, the precision is 10^{-17}, the key space size is $(10^{17})^{10}$ i.e. $\mathbf{10^{170}}$, which is extensively large enough to make the brute force attack and other related attacks infeasible.
Key Sensitivity: A cryptosystem should be sensitive to a small change in secret keys i.e. slight change in secret key value in decryption process results into a completely different decoded image which will be similar to cipher image [3]. Encryption algorithm proposed in this paper is sensitive to a small change in the secret keys. If we change a single bit in any of the initial conditions then the decrypted image is totally different from the plain-image. For example if one of the initial condition is 1.4 and we replace it by 1.41, then we get a complete random image. To get back the proper decrypted image the initial condition should be **1.40000000000000001**.

Information Entropy Analysis
The entropy H (m) of a source m is calculated by the equation [5]

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log_2 \frac{1}{p(m_i)} \quad bits \qquad (6)$$

Where p (mi) represents the probability of occurrence of symbol mi. Entropy is expressed in terms of bits. Here each pixel in the image is represented by 8 bits so number of different values that it can have is 2^8. It is equivalent to a source emitting 2^8 symbols with equal probability. When this is applied to eq. 5 we get h (m) =8 which corresponds to a completely random source. Entropy is less than 8 for plain images but when images are encrypted their entropy has to ideally be 8. If it is not 8 then degree of predictability is high.

It is observed that for Lena image information entropy of encrypted image using the proposed algorithm is **7.9890** which are very close to the theoretical value of 8. This implies that the algorithm is secure against entropy attack.

Peak Signal to Noise Ratio (PSNR)
The term **peak signal-to-noise ratio (PSNR)** is an expression for the ratio between the maximum possible value (power) of a signal and the power of

distorting noise that affects the quality of its representation. It helps to compare different image enhancement algorithms and identify the best among them. The mathematical representation of the **PSNR** is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (7)$$

Where the **MSE** is the Mean Squared Error.
The PSNR value obtained for the proposed algorithm is **77. 3503.**

7. Conclusion and Future Work

In this paper, a new algorithm of encryption and decryption of images using chaos is presented. The algorithm is based on the concept of shuffling the pixels positions and changing the gray values of the pixels in the image. To perform the shuffling of the plain-image's pixels, a block and stream based shuffling scheme is proposed, in which the plain-image is decomposed into 8x8 size blocks and a different chaotic maps are applied in three different ways to achieve good shuffling effect. The encryption of the shuffled image i.e. diffusion is done using chaotic sequence generated through a Henon map. The experimental results and analysis show that the proposed image encryption system has a very large key space, high sensitivity to secret keys, has low correlation coefficients close to the ideal value 0, good entropy value and high PSNR value. Hence, the proposed algorithm is effective and provides a better security.

References

[1] G.A. Sathishkumar, K.Bhoopathy Bagan and N. Sriraam, "image encryption based on diffusion and multiple chaotic maps" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[2] Guanrong Chen, Yaobin Mao, Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps" Chaos, Solitons and Fractals 21 (2004).

[3] Honge Ren, Linlin Dai and Jian Zhang, "Image Encryption Algorithm based on Chaos Mapping and the Sequence Transformation" Research Journal of Applied Sciences, Engineering and Technology 5(22): 5308-5313, 2013.

[4] Ibrahim S. I. Abuhaiba1, Hanan M. Abuthraya, Huda B. Hubboub, Ruba A. Salamah , "Image encryption using chaotic map and block chaining" I. J. Computer Network and Information Security, 2012, 7, 19-26 Published Online July 2012 in MECS.

[5] K.Sakthidasan, Sankaran and B.V. Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images" International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.

[6] Kamel Faraoun , "chaos-based key stream generator based on multiple maps combinations and its application to images encryption" The International Arab Journal of Information Technology, Vol. 7, No. 3, July 2010.

[7] Musheer Ahmad and M. Shamsher Alam. Musheer Ahmad, "A new algorithm of encryptionand decryption of images using chaotic mapping" International Journal on Computer Science and Engineering, Vol.2 (1), 2009, 46-50.

[8] Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B, " Image encryption using block based uniform scrambling and chaotic logistic mapping " International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.1,March 2012.

Sandhya Rani M.H. received the B.E. degree in electronics and communication engineering from the University of Mysore, and M.E. in Digital Electronics from Karnataka University and pursuing Ph.D. in Jain University, India. She is presently working as Associate Professor in the E&C Dept.in Sapthagiri College of Engineering, Bangalore with 15 years' experience in teaching.

Dr. K. L. Sudha, presently working as professor in ECE department, Dayanandsagar College of Engineering, Bangalore, India has 16 years of teaching experience in Engineering Colleges. She obtained her Bachelor's degree in electronics engineering from Mysore University, Masters from Bangalore University and Ph.D. from Osmania University, Hyderabad. She has published more than 15 research papers in national/ international journals and conferences. Her research interests are in Wireless communication, Coding theory, image processing and chaotic theory.