Indian Streams Research Journal
Volume 3, Issue. 5, June. 2013
ISSN:-2230-7850

Available online at www.isrj.net

ORIGINAL ARTICLE

SECURE IMAGE DATA BY THREE STAGES OF ENCRYPTION USING BLOCK BASED TRANSFORMATION

GAYATHRI D. AND SUMETRA MENARIA

CSE Department, PIT, Waghodia, Dist.-Vadodara, Gujarat, India.
CSE Department, PIET, Waghodia, Dist.-Vadodara, Gujarat, India

Abstract:

Information security is an increasingly important problem in the present era of advanced technology, because of which encryption is becoming very important to ensure security. Popular application of multimedia technology and increasing transmission ability of network gradually leads us to acquire information directly and clearly through Images. The digital images, which are transmitted over the internet, must be protected from unauthorized access during storage and transmission for communication, copyright protection and authentication purposes. This can be accomplished using image encryption which is an intelligent hiding of information. Encryption is the process of converting an image from readable form to unreadable form. In this paper, I have encrypted an image at three stages for increasing the entropy and to decrease the correlation between the pixels using block based transformation.Experimental results demonstrate that the algorithm is sensitive to initial conditions to resist the brute-force attack.

KEYWORDS:

Image encryption, Decryption, Permutation,Chaotic system, Position Vector, Symmetric key cryptography.

INTRODUCTION:

The rapid growth of computer networks allows large

files, such as digital images to be easily transmitted over the internet. Security has been the major issue to protect the data from the unauthorized access. Image encryption being a challenging task to protect the image from the unauthorized user. There are various image encryption systems used to encrypt and decrypt the data, and there is no single encryption algorithm satisfies the different image types. Most of the algorithms specifically designed to encrypt digital images are proposed in the mid-1990s. There are two major groups of image encryption algorithms: (a) nonchaos selective methods and (b) Chaos-based selective or non-selective methods. In the chaos based approach image encryption is carried out by the permutation of the pixel position. In this paper we have consider chaos method for image encryption, an index based chaotic approach is used to permute the pixel value of the gray scale image.

Discrete chaotic dynamical systems are nonlinear dynamic behavior, they are pseudorandom, sensitivity to the initial conditions and generate highly complicated signals by a simple recursive procedure. Because chaotic systems have good properties, chaotic systems are widely used in communications, optimization, control and image processing. [1-7]. In 1989, Matthews used discrete chaotic dynamical systems in cryptography firstly [6]. He derived a one dimension chaotic map, which is used to generate a sequence of pseudo-random numbers. In 1991, Habutsu et al. developed a cryptosystem based on a piecewise linear chaotic tent map. In Habutsu's cryptosystem, it is made of the parameter of the tent map as a secret key and the encryption and forward iteration of the chaotic tent map. But the cryptosystem can be easily broken using a 'chosen cipher text attack' and 'known plaintext attack'. Zhang et al.[8] presented a new image encryption algorithm based on chaotic systems. The algorithm validly solves problem of failure of encryption owing to the self-similarity. But the algorithm is not robustness for noise disturbing and also the length of the chaotic sequence is much longer than the length of the integer sequence needed.

In this paper we proposed a new encryption/decryption algorithm based on index based chaotic system. With the help of logistic map a real valued sequence is generated and then picks up the index of the smallest number from the series and put it in another one dimensional matrix. Next we rearrange the pixel of the original image by mapping it with the generated sequence. Section2 briefs about the chaotic system. Section3 discuss the encryption and decryption algorithm and its description. Section4 demonstrate the experimental results of the encryption and decryption process by considering the suitable initial condition. Section5 presents the conclusion.

2. CHAOTIC SYSTEM

A chaotic dynamical system is an unpredictable, deterministic and uncorrelated system that exhibits noise-like behaviour through its sensitive dependence on its initial conditions, which generates sequences similar to PN sequence. The chaotic dynamics have been successfully employed to various engineering applications such as automatic control, signals processing and watermarking. Since the signals generated from chaotic dynamic systems are noise-like, super sensitive to initial conditions and have spread and flat spectrum in the frequency domain, it is advantageous to carry messages with this kind of signal that is wide band and has high communication security. For this reason numerous engineering applications of secure communication with chaos have been developed.[9]

Chaotic Sequences

A chaotic sequence [7] is non-converging and nonperiodic sequence that exhibits noise-like behavior through its sensitive dependence on its initial condition. Chaotic systems have sensitive dependence on their initial conditions. A large number of uncorrelated, random-like, yet deterministic and reproducible signals can be generated by changing initial value. These sequences so generated by chaotic systems are called chaotic sequences. Chaotic sequences are real valued sequences. This real valued sequence can be converted into integer valued sequence. This generated sequence makes it much effective for pixel permutation that can be used for image encryption.

Generation of Chaotic Sequences

One of the simplest and most widely studied nonlinear

dynamic systems capable of exhibiting chaos is the logistic map $ak+1=\mu *ak*(1-ak)$ .... (1)

Here, here $0< \mu<4$ and ak Є [0, 1].This recursive function of eq(1) can be used to generate a sequence up to length n.

Pseudorandom sequences generated from chaos:

Chaotic dynamical systems are nonlinear dynamic behavior, they are pseudorandom, sensitivity to the initialize conditions. Chaotic map being used widely to generate the sequence of real number. By using those real sequences and their sorted value a pseudorandom sequence can be generated. This generated sequence can be used for image pixel permutation. Random number sequence can be generated from this sequence. [9]

I. Generate the real chaotic sequence of length n by using the formula (1) and store it in an one dimensional matrix a as.
{a1,a2,a3,a4,………..an}

II. Find the index of the smallest number from the sequence of n number and then store it in b(1).Next find the index of the 2nd smallest number and store it in b(2). Repeat This process until getting the nth smallest number and store it in b(n).

III. Now the b contains sequence of n integer random number generated from the chaos sequence.

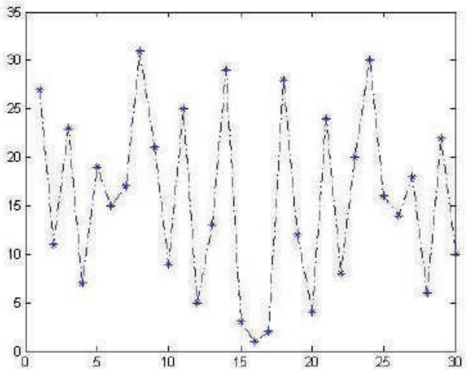


Figure 1 : Pseudorandom Sequence **bn** of length n=30
By taking initial condition a0 =.7 and μ=3.6

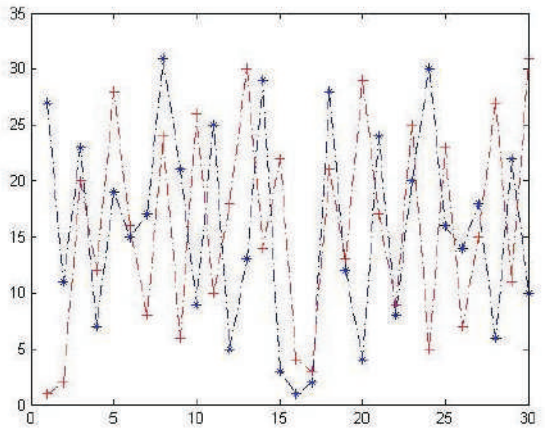


Figure 2 : Pseudorandom Sequence **bn** of length n= 30
for a0 =.7 and μ=3.6 and a0 =.7 and μ=3.6001

The generation of this sequence is the strong part of this proposed model. Figure 2 shows the random number for 30 index value. The integer sequence is varied a lot in its value by slightly changing the parameter. The major advance of this sequence is that random number is the integer sequence and defined in a specific range. Also if the value of the initial seed value is changed then it drastically change the sequence. TheFigure 3 shows the random number generated by varying the initial parameter μ from 3.6 to 3.6001.

DISCRETE COSINE TRANSFORM AND INVERSE

COSINE TRANSFORM

The DCT transforms a signal from a spatial representation into a frequency representation.[10] The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. Lower frequencies are more obvious in an image than higher frequencies so if we transform an image into its frequency components and throw away a lot of higher frequency coefficients, we can reduce the amount of data needed to describe the image without sacrificing too much image quality. For this reason, the DCT is often used in Image compression applications. Here the in build function DCT (image) is used in MATLAB. To rebuild an image in the spatial domain from the frequencies obtained above, we use the IDCT (image).

CORRELATION

Correlation is the average relationship between two or more variables. When the change in one variable makes or causes a change in other variable then there is a correlation between these two variables.

These correlated variables can move in the same direction or they can move in opposite direction. Not always there is a cause and effect relationship between the variables when there is a change; that might be due to uncertain change. [11]

The range of correlation varies from +1 to –1. A zero correlation indicates that there is no relationship between the variables. A correlation of –1 indicates a perfect negative correlation, means that as one variable goes up, the other goes down. A correlation of +1 indicates a perfect positive correlation, means that both variables move in the same direction together. In mathematical terms, correlation is defined as,

$$r_{xy} = \frac{\sum x_i y_i - n\bar{x}\bar{y}}{(n-1)s_x s_y} = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\ \sqrt{n\sum y_i^2 - (\sum y_i)^2}}.$$

Where,
r: correlation value
n: the number of pairs of data
Σxy: sum of the products of paired data
Σx: sum of x data
Σy: sum of y data
Σx^2: sum of squared x data
Σy^2: sum of squared y data

IMAGE ENTROPY

Entropy in simple terms is a measure of the uncertainty associated with a random variable. It can be defined as the expected value of the information contained in data. It is a measure of the average information content. [12]

More precisely it is a measure of disorder, unpredictability.

If an encrypted image is lossless, without any noise being added in the channel, and if we can recover the entire original image after decrypting then the total entropy of lossless image is less compared to the lossy image. A lossless image is more predictable compared to lossy image. The entropy of a message is in a certain sense a measure of how much information it really contains.

Entropy defined as follows,

$$H_e = -\sum_{k=0}^{G-1} P(k) \log_2 (P(k))$$

Where:
He: entropy.
G: gray value of input image (0... 255).
P(k): is the probability of the occurrence of symbol k.

3. PROPOSED ALGORITHM

Image encryption techniques try to convert an image to another one. On the other hand, image decryption retrieves the original image from the encrypted one. Mainly the algorithm begins with the generation of the chaotic sequence using the logistic map. The algorithm begins with the generation of an integer pseudorandom sequence with the help of the chaotic sequence. On the base of this sequence next the pixel position of the image can be permuted to get the encrypted image.

Suppose the image that is being encrypted Image and the encrypted image is Eimage .Both the Image and Eimage having the size (m, n). The proposed algorithm permutes the pixel of image based on the generation of the integer chaotic sequence. DCT is applied on the first block transformed image, then that image is again block transformed using the same chaotic sequence. The algorithm is described as follows.

Step 1: The image is divided into calculated no of blocks.
Step 2: Using the key the chaotic sequence is generated and a reference is taken randomly.
Step 3: The position of reference number is loaded to the vector x as the first value.
Step 4: The positions of the values higher than the reference are noted sequentially in the vector x.
Step 5: The rest of the vector is the position of the values below the reference number in decreasing order.
Step 6: The divided blocks are scrambled according to vector x taking each number as the index.
Step 7: Perform the DCT operation on each block and save the coefficients.
Step 8: The second chaotic sequence is generated in the similar way discussed above.
Step 9: The image on which DCT is applied is transposed using the second chaotic sequence.
Step 10: The encrypted image is obtained.

DESCRIPTION OF THE ALGORITHM

The algorithm begins with the generating a chaotic sequence. The initial condition a0and µ treated as the key for the encryption algorithm. Using the logistic map we can generate the sequence up to length mxn. Step5 and step6 used to shuffle the index position into a permuted vector P according to the sorted value of the sequence. i.e put the index position of the sequence into a position vector P on the basis of their sorted value. Next in Step8 place the pixel of plain image into Eimage with respect to the position defined in the position vector P.

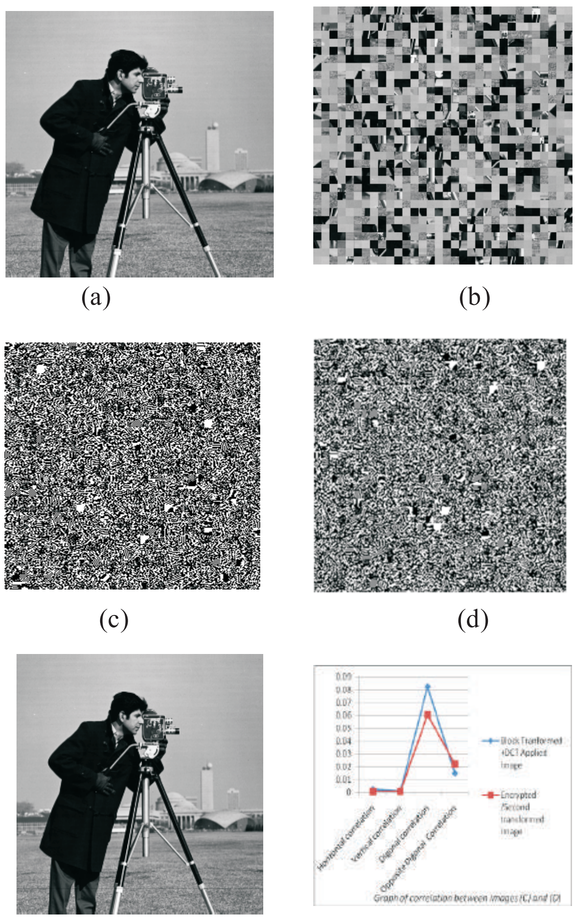
DECRYPTION ALGORITHM

Step 1: The initial value, value of 'µ' and position of reference are taken as the key.
Step 2: Using the two keys, two chaotic sequences are generated.
Step 3: The Encrypted image is then rearranged based on the chaotic sequence.
Step 4: The inverse DCT operation is applied block wise on the rearranged Encrypted image.
Step 5: The obtained image is again rearranged using the second chaotic sequence.
Step 6: Decrypted image is obtained.

Decryption process is also very easy. It's just the replication of the encryption process. On the receiver side for decrypting the cipher image first all the initial condition for the chaotic sequence is required and this initial condition can be treated as the key. With the key, generate the chaotic sequence and then sort the sequence in ascending order. Next find the permuted position vector P that contains all the permuted pixel position. Final rearrange the block of the cipher image into I to get back the original image. This permutation is carried out in accordance to the value of the position vector P, then IDCT in applied on the first retransformed image. The resulting image is again retransformed according to the generated chaotic sequence with the same initial parameters.

4. EXPERIMENTAL RESULT

Upon carrying out the encrypting process of the Image by taking the initial condition, the encrypted image hides the totality of the information contained therein, as seen in figure 3(b), figure 3(c), and figure 3(d), here the chaos initial condition is treated as the key for the encryption of the image. The distribution of intensities of the encrypted image varies when changing the value of the initial condition. When the decryption process is done with the same initial condition, we recover the original image, as shown in figure 3(i).If the keys used in the decryption process are not equal to the keys used in the encryption process, the image will not be recovered, statistical calculation is calculated for measuring the correlation, entropy. The third stage of encryption increases the security of an image.



(a) (b)

(c) (d)

(e) (f)

Fig:3 The effect of encryption and decryption using three stages of encryption using block based transformation (a)Original image. (b) First block transformed Image with initial parameter μ=3.8and ak=0.8. (c) Block transformed + DCT applied image (d) Second block transformed image with parameter μ=3.8 and ak=0.8. (e) Decrypted Image with parameter μ=3.8 and ak=0.8 (f) Graph of correlation between Images (c) and (d).

The correlation of block transformed + DCT applied image and second transformed image is calculated. The graph in figure (f) clearly indicates that the correlation is decreased after the second transformation which indicates secure encryption of image.

5. CONCLUSION

In this paper, we present image encryption using index based chaotic method for encrypting the gray scale image by three stages. The third stage decreases the correlation between the pixels when compare to the second stage of encrypted image. Use of Chaotic system in the digital image encryption greatly increases safety parameters in the encryption of images. Due to the sensitivity of chaotic system to the initial condition it is almost impossible for any cryptanalysts trying to decrypt the image without authorization as the chaotic sequence is sensitive to the initial condition.

REFERENCES:

[1]. D. Xiao, X. Liao, and P. Wei. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons and Fractals, 40(5):2191 – 2199, 2009.
[2]. L. Wang and K. Smith. On chaotic simulated annealing[J]. IEEE Trans on Neural Networks. 1998, 9(4): 716-718
[3]. Han Hen and Neri Merhav. On the Threshold Effect in the Estimation of Chaotic Sequences[J]. IEEE

Trans on Information Theory. 2004, 50(11): 2894-2904
[4]. Liang Zhao et.al. A Network of Globally Coupled Chaotic Maps for Adaptive Multi-Resolution Image Segmentation[C]. Proceedings of the VII Brazilian Symposium on Neural Networks (SBRN'02)
[5].Claudio R. Mirasso et.al. Chaos Shift-Keying Encryption in Chaotic External-Cavity Semiconductor Lasers Using a Single-Receiver Scheme[J]. IEEE Photonics Technology Letters. 2002, 14(4): 456-458
[6].R. A. J. Matthews. On the derivation of a chaotic encryption algorithm[J]. Cryptologia. 1989, 13(1): 29-42
[7]. T. Habutsu, Y. Nishio, I. Sasase, et al. A secret cryptosystem by iterating a chaotic map[A]. Advances in Cryptology EURCRYPT'91[C]. Berlin: Springer- Verlag. 1991: 127-140.
[8] Zhang Han, Wang Xiu Feng et al. A new image encryption algorithm based on chaos system[C]. Proc. IEEE Int. Conf. Robotics, Intelligent Systems and Signal Processing. Changsha, China, October 2003: 778-782.
[9] Chinmaya Kumar Nayak1, Anuja Kumar Acharya2 and Satyabrata Das3 "Image Encryption Using an Enhanced Block Based Transformation Algorithm" International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 2, April 2011.
[10] Andrew B. Watson NASA Ames Research Center," Image Compression Using the Discrete Cosine Transform", Mathematica Journal, 4(1), 1994, p. 81-88.
[11]http://en.wikipedia.org/wiki/Correlation_anddependence_Toc294084375_Toc294114424_Toc294114042_Toc294113719.
[12] http://en.wikipedia.org/wiki/ Entropy