Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 75 (2014) 27319-27323

ISSN: 2229-712X

Performance and analysis of information securty in multimedia communication using chaos based scrambling method

Priyanka Tiwari, Mukesh Kumar, Rohini Saxena and A.K.Jaisawal

Department of Electronics and Communication Engineering, SHIATS- Allahabad, UP, India.

ARTICLE INFO

Article history:

Received: 22 April 2014;

Received in revised form:

20 September 2014;

Accepted: 29 September 2014;

Keywords

Information Security,

Image Encryption,

Image Decryption Chaotic algorithm,

Scrambling, Authentication key,

MATLAB10.

ABSTRACT

In Wireless networks, the security of data and information has important role in digital communication and multimedia communication. Different types of encryption algorithms have an important role to provide the security to the wireless networks. Cryptography basically used for the data confidentiality and privacy by making indiscernible. Hence the original data cannot be interrupted by the unauthenticated user. The encryption techniques and different types of useful algorithms are used to provide the more security to the applications. In this paper the well- known method chaotic algorithm is used. Chaotic algorithm is used in real time secure image transmission systems. This algorithm is very popular method used in Research for encryption and decryption process. The combination of chaotic theory and cryptography has very important role in Information Security. In this communication, a new image encryption algorithm based on chaotic map is proposed for gray scale 2D image. In this proposed algorithm, the plain or original image is taken which has MXN dimension. Then Redistribute the pixel pair wise by deciding.

Introduction

The great demand for the universal personal communications is driving the development of new networking techniques. In wired/wireless communication the security of data has essential role for improvement of the security of data being transmitted different techniques are used. The improved method is important which is used to provide the confidentiality by the data encryption and decryption techniques. Cryptography is the technique of transferring the information on applications using scrambling method. It is associated with the study of mathematical techniques with respect to the information security such as the confidentiality, authentication and integrity of the data. Image encryption and decryption process has important role and to meet the huge demand for real time secure image transmission over the Internet. Comparing with past algorithms like RSA, DES, and AES traditional image encryption and decryption algorithm has the low level of efficiency when the image is large. The Chaos based encryption and decryption algorithm has introduced a new and most useful which deals with the problem of fast and more secure image transmission. Chaotic systems are important techniques which have the sensitive dependence on initial conditions and system parameters, no periodicity, topological transitivity and pseudorandom property. Most properties of chaos based algorithm fulfill the some requirements such as scrambling and diffusion in the respect of cryptography. Therefore, one of the most useful techniques is chaotic cryptosystems as well as practical applications.

An encryption scheme is known as Cryptosystem. The original image is called a plain text and the encrypted image is called cipher image which is denoted by P and C respectively. The encryption method is described as $C=Ek_{key(e)}(P)$,where $K_{key(e)}$ is the encryption function. Similarly, in decryption process the **image** can be describe by $P=DK_{key(d)}(C)$ where $K_{key(d)}$ and D is the decryption function which performs the decryption process.

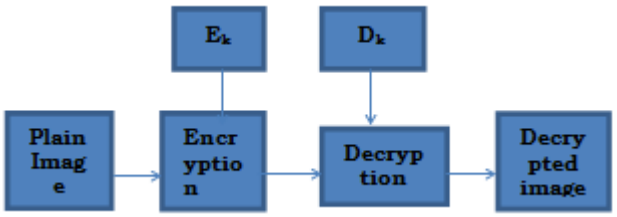

Fig 1. Encryption and Decryption Process

The present research work focuses on the chaos based scrambling method which is more secure image encryption and decryption for Information Security.

Related Works

The Chaos based encryption and decryption algorithm has introduced a new and most useful which solve the problems of fast and high secure image transmission. Chaotic systems are very important techniques which have the sensitive dependence on initial conditions and system parameters, no periodicity, topological transitivity and pseudorandom property. Most properties of chaos based algorithm gain some requirement such as scrambling and diffusion in the sense of cryptography. Therefore, one of the most useful technique is chaotic cryptosystems as well as practical applications .In order to improve the security performance of image encryption and decryption algorithm, the method of rearranging all pixels in entire image using scrambling method.

Chaos based algorithm depends on the energy. It is a measure of information on applications information and content of images. Maximum energy is contents of low frequency coefficients of image. The no. of gray levels is low then energy is high which is widely used in chaotic map.

The Chaos based information Security mainly consists of two stages. The plain image is given at the input side. There are two steps involved in the chaos based image encryption and decryption. First is plain image is scrambled with the help of

Tele:

E-mail addresses: priyankabbs@rediffmail.com

Changing position of the pixels and second is give the authentication key using a random matrix. In this proposed method one can use the scrambling method for chaotic mapping. In chaos based image encryption and decryption change the pixel position with the help of scrambling method over the entire image without disturbing the value of pixels and the image becomes unrecognizable. The second stage provides the authentication key. Repeat the process until entire image is scrambled and no. of iteration of scrambling depends upon the authenticated user which is kept secret for high security.

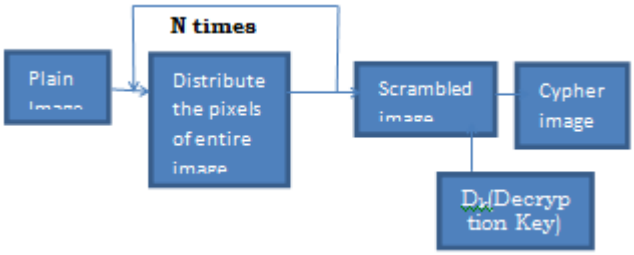

Fig 2. Chaos based Encryption System

To fulfill the demand of reliable and security, protection against unauthorized user, storage of information, transmission of digital images over the wired/wireless networks most of researchers used chaos based algorithm for image encryption /decryption. Chaos based image encryption/ decryption has desirable features such as randomness, high sensitivity to initial conditions, long periodicity and mixing property. These features make chaos based Information Security secure and robust against statistical attacks. Due to iterative processing chaos based algorithm gives randomness, unbalanced image, confusion and diffusion for cryptosystem.

Different types of chaotic mapping

Logistic Map

The logistic map is a polynomial mapping of degree two. Simple mathematical system showing different characteristics of the development of chaotic behavior.

$P_{n+1}= rP_n(1-P_n)$

Where P_n is a number between zero and one, r is a positive no. which represents a combined rate for reproduction and starvation.

2D Cat Map

A 2D cat map is firstly introduced by Arnold. Let coordinates of positions of pixels in an image are A={(p,q),where p,q=1,2,3,4….

X'=(p + aq)mod (n)

Y'=bq+(pq+1)mod(n)

Where p,q are control parameters which are positive integers.

Baker's Map

In dynamical system theory, the baker's map is a chaotic map from the unit square into itself. Folded bakers map acts on the unit square as

$$\mathbf{S_{baker\text{-}folded}(p,q)} = \begin{cases} (2p, \frac{y}{2}) & for\ 0 \le p < \frac{1}{2} \\ \left(2-2p, 1-\frac{q}{2}\right) & for\ \frac{1}{2} \le p, 1 \end{cases}$$

When the upper section is not folded over the map may be written as

$$\mathbf{S_{baker\text{-}unfolded}(p,q)} = \{(2p-|2p|, (q+|2p|)/2)$$

The folded baker's map is a two dimensional analog of tent map.

$$\mathbf{S_{tent}(p)} = \begin{cases} 2p & for\ 0 \le p < 1/2 \\ 2(1-p) & for\ \frac{1}{2} \le p < 1, \end{cases}$$

Proposed Cryptosystem

A. Encryption System: Proposed cryptosystem has two parts- One is scrambling of original image and second is generate a security random matrix which gives the security key to protect the plain image from attackers.

Mathematical Operation for Encryption

Distribute the pixel pair wise

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ m$$

I(decrypt) = EX-OR(I(scramble),I(sec)),

Where I(scramble)=scrambled matrix,

I(sec)=random matrix generate security key.

The main goal of scrambling image is to convert a meaningful image into a meaningless or disordering of original image. Scrambling method gives the computation complexity for plain image attack. Many cryptosystem have been chosen to achieve secure image scrambling these methods are-Baker Map, Arnold Cat map, Standard map etc.

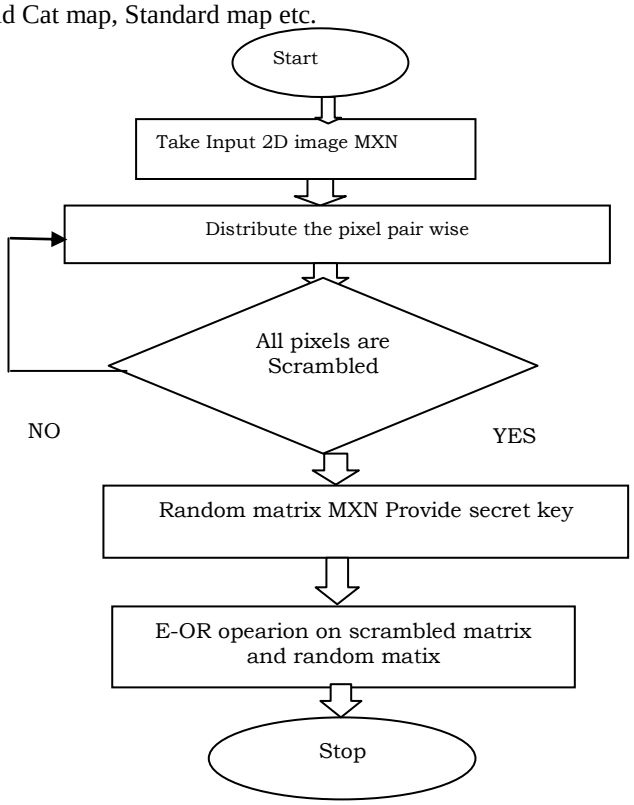

Fig 3. (A) Flow Chart for Proposed Encryption Process

Decryption System

The purpose of this decryption method is to transform the meaningless information to meaningful and reallocate the ordering of image. In proposed Decryption System Encrypted image given to the input stage which is scrambled by the pixel pair wise. Scrambled image (Iscram) is produced and one random matrix I(sec) is generated. After EX-OR operation of scrambling image and random matrix the decrypted image will be found.

Mathematical Operation for decryption

Reallocate the pixel $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} X' \\ Y' \end{bmatrix} mod\ m$

I(decrypt) = EX-OR(I(scramble),I(sec)),

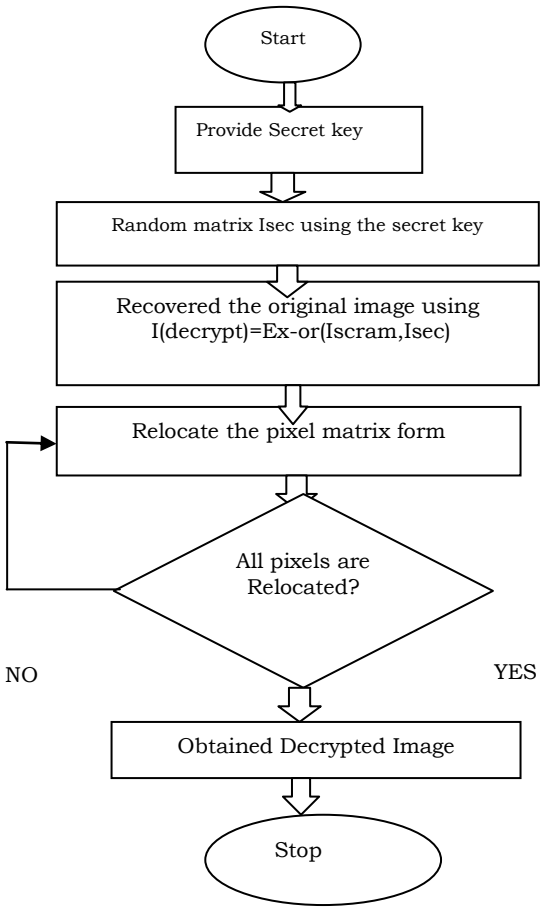

Fig 3. (B) Flow Chart for Proposed Decryption Process

Proposed Algorithm

Proposed Image Encryption Algorithm:

Step1. Take the Input Image I of dimension MxN.

Step2. Redistribute the pixel pair wise.

a) Decide the parameters for relocating.

b)The equation for distribute the pixel pair wise

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ m$$

a,b,c,d should be kept secret and known only to the rightful owner.

c) Form the scrambled image Iscrambled of size MxN.

Step3.Repeat step 2 iteratively to optimize the scattering of energy.

Step4.To enhance the security of algorithm we are using user defined authentication key.

Step5. Generate a random matrix Isec of size MxN using the security.

Step6.Take bitwise X-OR of Iscram image and secret random matrix.

Iencrypt=Ex-OR(Iscrambled,Isec)

4.2Proposed Image Decryption Algorithm

Step1. Now Input will be scrambled image(Iscram).

Step2. Receiver or authentication user will provide the secret key.

Step3.Generate the random matrix Isec using the secret key.

Step4.Bit wise X-OR Isec with Iscram(the image that is being received on the receiver end). Idecrypt=Ex-OR(Iscramble,Isec)

Step5.Relocate the pixel pair wise using the equation and the parameters known only to the rightful owner.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} X' \\ Y' \end{bmatrix} mod\ m$$

Repeat the process iteratively and no. of cycles depend upon the user (used at the time of encryption).

Step 6. Obtained the decrypted image.

Result and Discussion

MATLAB is High-level language for technical computing. It is used to compute 2-D and 3-D graphics functions for visualizing data. It is a compatible tool for digital image processing. All experiments and results are implemented using MATLAB. Original image, encrypted image, decrypted image are shown in figure with Chaos based algorithm encryption and decryption. More secure due to randomness in nature and using authentication key. The decrypted image after applying scrambling method in chaotic systems was obtained original image.

(a)Plain image, Encrypted image, Decrypted image of Baboon

(b)Plain image, Encrypted image, Decrypted image of Lena

(c) Plain image, Encrypted image, Decrypted image of Baf

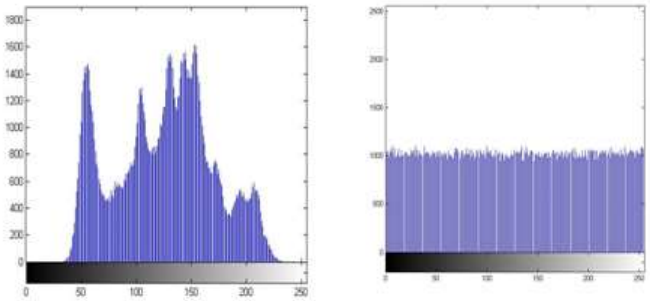

Fig.5(a) plain image and cypher image of baboon and its histogram

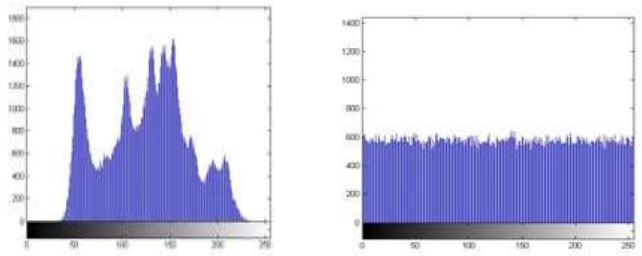

Fig.5(b) plain image and cypher image of lena and its Histogram

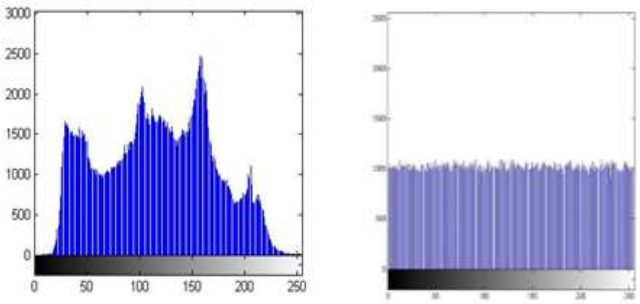

Fig 5(c). Plain image and cypher image of baf and its histogram

On implementing improved Chaos based image encryption on Matlab, using different type of images such as .bmp,.tif,.jpeg etc. format, above results are obtained. It can be concluded from the above experiments that image encryption and decryption is more secure than other methods and Encrypted Image does not provide any information due to randomness property of proposed algorithm and security key. As a result the proposed algorithm can resist any type of histogram based attacks and unauthorized accessing.

Key Space Analysis

Key space is defined by the total number of different keys which is used in cryptography. A good cryptosystem have large key space to protect from attackers. In proposed Algorithm key space variable are declared as uint8 which value has 0-255.Thus the key space of the proposed algorithm is extensively large which gives high protection.

Key Sensitivity

The proposed encryption algorithm should be sensitive to secret key. An unauthenticated user who doesn't know the secret key will be unable to access the original image.

Shannon Entropy

In information theory, entropy is a measure of the uncertainty in a random variable.[1] In this context, the term usually refers to the Shannon entropy, which quantifies the expected value of the information contained in a message.[2] Entropy is typically measured inbits, nats, or bans.[3] Shannon entropy is the average unpredictability in a random variable, which is equivalent to its information content. Shannon entropy provides an absolute limit on the best possible lossless encoding or compression of any communication, assuming that[4] the communication may be represented as a sequence of independent and identically distributed random variables.

Mathematical expression for entropy

$$H(S) = -\sum_{i=0}^{255} (\mathrm{P}(s_i) \log_2 P(s_i)$$

where $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits. If the message source S emits 28 symbols as S = {s0, s1, . . . , s255g} with equal probabilities, then the entropy of S is 8, which corresponds to a true random source and represents the ideal value of entropy for S. If the entropy of a cipher-image is significantly less than the ideal value, then there would be a possibility of predictability which threatens the image security.

Table 5.3 entropy of Plain Image and Cypher Image

Entropy of Plain Image and Cypher Image		
Test Image	Plain Image	Cypher image
Baboon	7.3579	7.9994
Lena	7.3470	7.9987
Baf	7.6022	7.9993
Bridge	7.1241	7.9967

Conclusion

In this paper a new algorithm of encryption and decryption is introduced. The algorithm is based on the concept of scrambling the position of pixels without changing the original pixel value. The entropy of the cypher image is also more than the plain image in the proposed method. This method is applied only for 2D gray scale images. For high security, the authentication key provide by the rightful owner which is kept secret and only known to the authenticated user. All the simulation and experimental analysis show that the proposed image encryption system has-

- Very large key space.
- High Sensitivity to secret key.
- Due to randomness property unauthorized user cannot access the image.
- Hence we can say that all the analysis prove the security, effectiveness and robustness of the proposed image encryption algorithm.

References

1. Zhang Han, Wang Xiu Feng(2003), Li Zhao Hui, Liu Da Hai, Lin You Chou, "A New Image Encryption Algorithm Based on Chaos System", Proceedings of the IEEE International Conference on Robotics, Intelligent Systems and Signal Processing, Changsha, China, pp.778-782.
2. S. Lian, J. Sun, Z. Wang(2005), A block cipher based on a suitable use of chaotic standard map, Chaos Solitons 117–129.
3. Peng Fei, Shui-Sheng Qui, Long Min(2005), "An Image Encryption Algorithm based on Mixed Chaotic Dynamic Systems and External Keys", Proceedings of 2005 International Conference on Communications, Circuits and Systems,,Vol. 2, pp.1139.
4. Z. Guan, F. Huang, W. Guan(2005), Chaos-based image encryption algorithm, Phys. Lett. A 346 (2005) 153–157.
5. Kristina Kelber , Wolfgang Schwarz(2005) , "General Design Rules for Chaos-Based Encryption systems", Proceedings of International Symposium on Nonlinear Theory and its Applications(NOLTA2005) Bruges, Belgium, pp.465-468.
6. Yong-Hong Zhang, Bao-Sheng Kang(2006), Xue-Feng Zhang, "Image Encryption Algorithm Based On Chaotic Sequence", Proceedings of the 16th International Conference on Artificial Reality and Telexistence - Workshops(ICAT'06),Hang Zhou, Zheijang, China, pp. 221-223.
7. Z. Liehuang, L. Wenzhou, L. Lejian, L. Hong(2006), A novel image scrambling algorithm for digital watermarking based on chaotic sequences,Int. J. Comput. Sci. Netw. Secur.,125–130.
8. Huang Yuanshi, Xu Rongcong, Lin Weiqiang(2006), "An Algorithm for JPEG Compressing with Chaotic Encrypting",

Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation (CGIV'06).
9. Chong Fu, Zhen-chuan Zhang(2007), Ying-yu Cao, "An Improved Image Encryption Algorithm Based on Chaotic Maps", Computer Society, IEEE.
10. Chengqing Li(2007), "On the security of a class of Image Encryption Scheme", IACR's Crytologye.
11. T. Gao, Z. Chen(2008), Image encryption based on a new total shu_ing algorithm, Choas Solitons Fract. 38 (2008) 213–220.
12. S. Sridhar, Oxford university publication. , Digital Image Processing.
13. R. C. Gonzalez, Digital Image Processing, Prentice Hall of India, Second Edition, 2006.
14. Xin Zhang, Weibin Chen(2008), "A New Chaotic Algorithm For Image Encryption", pp 889-892 IEEE.
15. Dong enxeng, Chen Zengqiang(2008), Yuan zhuzhi, Chen zaiping, "A Chaotic Images Encryption Algorithm with The Key Mixing Proportion Factor",pp 169-174 Computer Society IEEE.
16. Chaotic image encryption algorithm based on frequency domain scrambling.
17. F. Zhang, L. Luo, M. Du(2009), Y.Wang, An image encryption algorithm based on spatiotemporal chaos, Int. Congress on Image and Signal Process,1–5.