International Journal of Image Processing and Vision Science

Volume 2 | Issue 1 Article 1

January 2013

ENCRYPTING IMAGE BY USING FUZZY LOGIC ALGORITHM

GAMIL R.S. QAID
Dept. Electronics & Telecommunications, S.G.G.S. Institute of Engineering and Technology, Nanded, India., jrsk80@yahoo.com

SANJAY N. TALBAR
Dept. Electronics & Telecommunications, S.G.G.S. Institute of Engineering and Technology, Nanded, India., sntalbar@yahoo.com

ENCRYPTING IMAGE BY USING FUZZY LOGIC ALGORITHM.

GAMIL R.S. QAID[1], SANJAY N. TALBAR[2]

[1]Research Student, [2]Professor, Dept. Electronics & Telecommunications, S.G.G.S. Institute of Engineering and Technology, Nanded, India.
E-mail: jrsk80@yahoo.com, sntalbar@yahoo.com

Abstract- Data communication is transmission data from a point to another. Nowadays main issue in data communication is the security. It can provide a fine solution by encryption. The encryption algorithm is the mathematical process for performing encryption on data. The proposed algorithm supports for user desired security level and processing level. The algorithm provides security levels and their corresponding processing levels by generating random keys for the encryption/decryption process. This facility is achieved by using fuzzy logic. The results of the proposed encryption algorithm will be analyzed by comparing with other existing encryption algorithms. The aim of the research is to build a new algorithm using fuzzy sets requirement which will be more advanced than the existing encryption algorithms.

Keywords *- Encryption, Decryption, Image, Fuzzy Logic.*

I. INTRODUCTION

The world has recently witnessed major development in the information and communications technology and the digital world. The computer science is used in all areas of life, including sending and receiving digital images as the importance of which are tremendously increasing. The images are sent and treated automatically, and this requires careful secret storage of data to be sent as there are many reasons to protect the image of the breach. Cryptography is the science which deals with ways that help us to protect and store information and transfer in a wide range and these methods depend on a secret key that is used to encrypt data. (1)

Security is the main problem in the modern digital world. There are a lot of cyber-crimes have arisen with the development of technology. [3] As solutions for these security risks users can shut down unused services, keep patches updated, reduce permissions and access rights of applications and users.

Another solution for this problem can be provided by using cryptography. [4]Cryptography consists of cryptology and crypto analysis. Encryption comes under cryptology. It is the process of converting a readable message into an unreadable format. [5] A set of rules is using for that process. It is called an encryption algorithm. Most of the nowadays existing encryption algorithms only concern on security. [6] However, users who have connections with low bandwidths need an encryption algorithm, which uses a low processing power. High security algorithms tend to take little more processing power than the low security algorithms. Nevertheless, newly implemented encryption algorithm, which has the facility to control both desired security level and the processing level, will be a great improvement for current real world applications. Various algorithms have been proposed to implement encryption in digital images. They can be categorized into three major clusters (i) value transformation [2], (ii) pixel position permutation [7, 8] (iii) chaotic systems [15-17].

Fuzzy logic is a problem-solving control system methodology that presents itself to implementation in systems ranging from simple, small, embedded micro-controllers to large, networked, multi-channel PC or workstation-based data acquisition and control systems. [18][19] Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy, or missing input information. [20] In fuzzy logic rules and membership sets are used to make a decision. [21] To achieve security and low processing, the algorithm uses variable keys. 0^{th} position gives a fully low processing algorithm, and 1^{st} position gives fully secured algorithm. The fuzzification changes depending on the key size and the number of mapping tables of the encryption algorithm. Users can input the desired key. One character will be 8-bit long. The main algorithm structure defines different key sizes up to 128bit. User can enter desired key-(application defines as the password) and also depending on the number of mapping tables' algorithm will allocate weight dynamically. Allocation of the weights will differ from 0.0 to 1.0 range; and the number of security levels will be vary from 1-16.The number of rounds will be determined by pre-defined mapping tables and the users initial input. Mapping tables are predefined in the algorithm and consists of mathematically defined values, and then those values will dynamically choose the relevant algorithm procedure once the user input the key to encryption.

Fuzzification

Fuzzification is the operation of making a crisp quantity Fuzzy. It is simply done by recognizing that many of the quantities that are regarded as crisp and

deterministic are actually not deterministic at all; they carry considerable doubt. If the form of doubt happens to arise, because of imprecision, opacity, or ambiguity, then the variable is probably Fuzzy and can be represented by a membership function.

Defuzzification
For a given input, several IF/THEN rules could be begun at the same time. Each rule will have a different strength because a given input may belong to more than one Fuzzy set, but with different membership values.

II. THE AIMS OF RESEARCH

The main aim of the research is to build encryption system based on fuzzy logic to secure confidential trading images. Here, the principles of information technology are applied to encrypt images and decrypt them. Besides, it allows the sender to make sure that the images will reach just the people to whom the images are sent to, and the right way that no one can decode it except the receiver person.

III.THE PROPOSED ALGORITHM

1) Steps of encryption algorithm:
1. Loading Image to be encrypted from data store

2. Processing of image using fuzzy Set

3. Generating the randomly prime number between (1– 256),

4. Storing seven random keys in a matrix (A).

5. Getting Image Width and Image Height

6. Dividing the image into a set of blocks.

7. Encrypting each 7bits with the seven keys which stored in matrix (A)

8. Repeating the step No. (7) in each 7 bits in the same block.
9. Repeating the steps No. (7) and (8) in all blocks.

10. Substituting each block in the image by converting the row to the column.

11. Taking each 2 vertically adjacent bits from the bottom of the image (b1, b2) and doing XOR between (b1 and b2).

12. Doing XOR between the (b and 256)

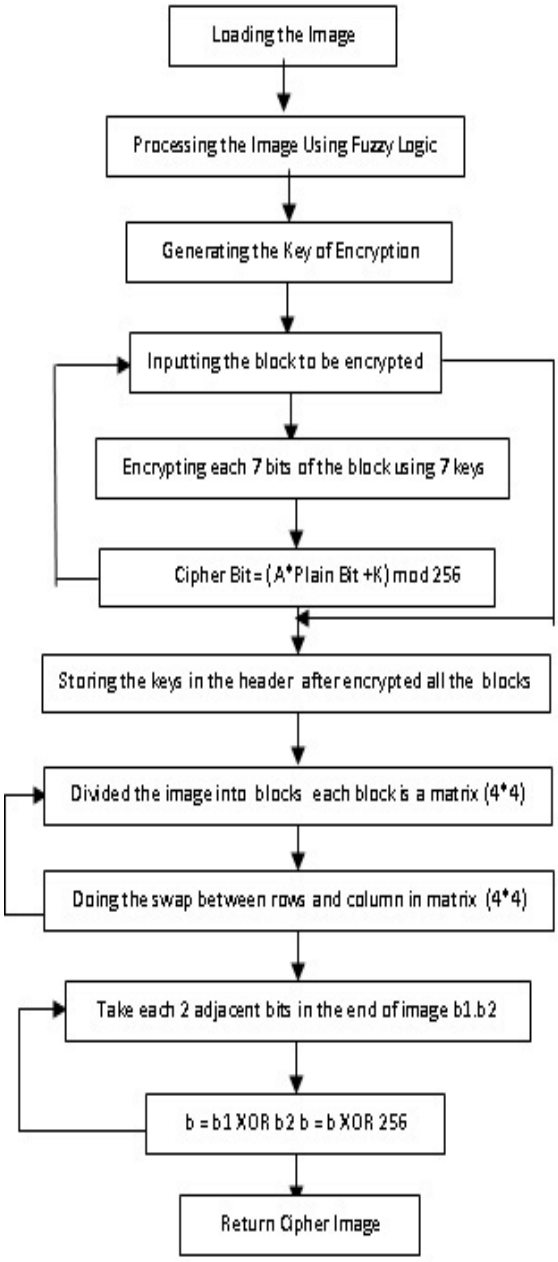
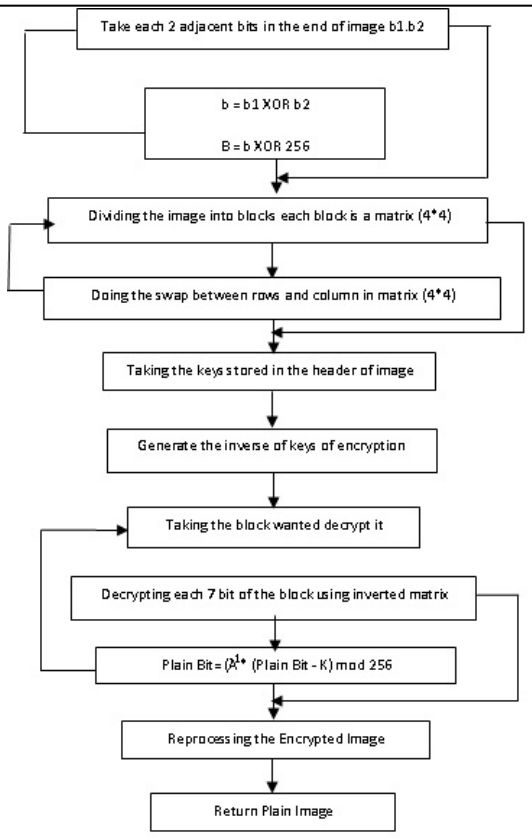


Figure1. Encryption algorithm

2) Steps of decryption algorithm:
1. Taking each 2 vertically adjacent bits from the beginning of the image (b1, b2) and doing XOR between (b1 and b2).
2. Doing XOR between the (b and 256).
3. Doing the tract substitutes for each block in the image by converting the row to the column.
4. Taking the keys stored in the header of the image
5. Finding the inverse of each key from the keys stored in the inverse's matrix (A).
6. Dividing the image into a set of blocks.
7. Decrypting each 7bits of the block accompanied with the inverse of the keys that stored in the matrix (A).
8. Repeating the same step No. (7) for every 7 bits in the same block.
11. Repeating the steps No. (7) and (8) for all blocks.



Figre2. Decryption algorithm

3) Processing image.
Method of processing image using fuzzy sets
Fuzzy image processing (FIP) has three main stages:
1. Image fuzzification
2. Modification of membership values
3. Image defuzzification

IV. FEATURES

The proposed algorithm has been proved to provide high protection to the images data from illegal intrusions. It is fast in the process of encryption and decryption. The decryption process does not induce any loss of image data, and it can deal with different format of images as will.

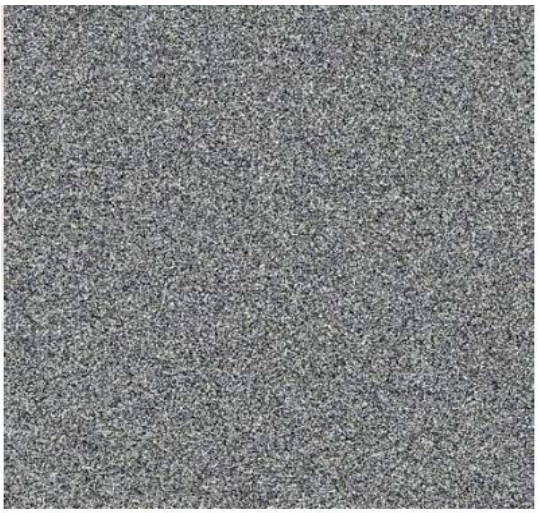
V. EXPERIMENTAL DETAILS AND RESULT

The proposed encryption algorithm can be classified into multiple criteria such as lossless, maximum distortion, maximum performance and maximum speed. In this section, the proposed algorithm is applied on different sizes and types of images.

The test images employed show a positive result. The encryption and decryption algorithm are implemented in VISUAL BASIC.NET and the test of lossless in MATLAB 7.0 , in core2duo of 2.66 GHz machine. The decryption algorithm takes between 76 and 100 Milliseconds to get executed. Calculating the lossless by this formula:

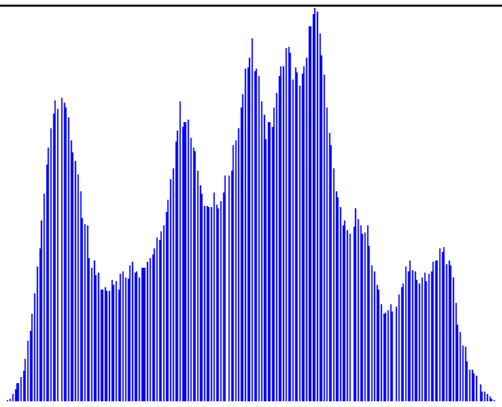
$$\text{error} = \left(\frac{1}{m * n}\sum_{i=1}^{n}\sum_{j=1}^{m}(\text{Orig. Image}(i.j) - \text{Dec. Image}(i,j)\right)^{\frac{1}{2}}.$$

Figre3. Original Image

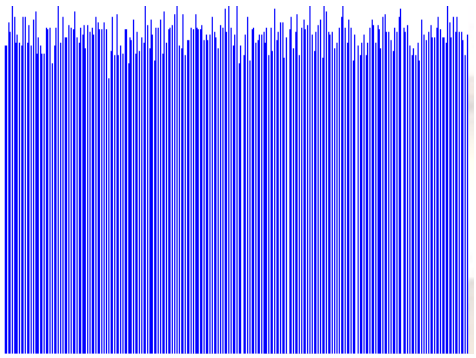


Figre4. Encrypted Image

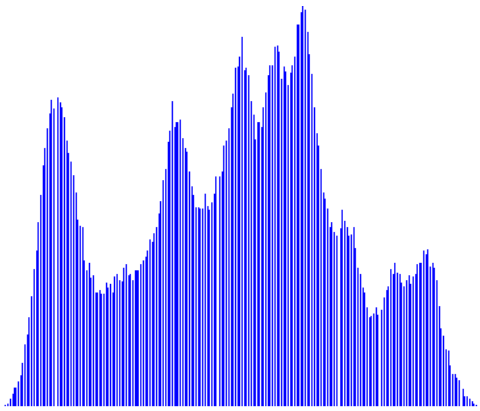
Figre5. Decrypted Image



Figre6. Histogram of Original Image



Figre7. Histogram of Encrypted Image



Figre8. Histogram of Decrypted Image

Security analysis

The strength is the most essential feature that a good quality encryption algorithm should possess. If the encryption algorithm is unable to prevent all types of attack including statistical and brute force attacks, it will not be sufficient for protecting the data. Many experiments are done for defining the competency of the proposed technique. In this part, the proposed technique is applied on images which have different formats and sizes.

1) Statistical Analysis

The encrypted images should hold certain random properties to prevent statistical attacks. A statistical analysis has been done by calculating the histograms, the entropy, the correlations and differential analysis for the plain image and the encrypted image for proving the strength of the proposed algorithm. After various images are tested, it appears that the intensity values are good.

2) Histogram Analysis

An image histogram is a commonly used method of analysis in image processing and data mining applications. One of the various benefits of the histogram is that it shows the shape of the distribution for a large set of data. Therefore, an image histogram provides a clear illustration of how the pixels in an image are distributed by graphing the number of pixels at each color intensity level. It is essential to make sure that the encrypted and original images possess different statistics. The histogram analysis shows the ways that pixels in an image are distributed by plotting the number of pixels at each intensity level. The Fig. 5. shows the results of the experiment on the plain image, its corresponding cipher image and their histograms. The histogram of each plain image explains how the pixels are distributed by graphing the number of pixels at every grey level [26]. The results show that the histogram of the encrypted image is uniformly distributed and significantly different from the respective histograms of the original images.

TABLE I. IMAGE PROPERTIES

No.	Image name	Dimensions	Size before encryption	Size after encryption
1	Lena	256 * 256	22.9 KB	21.5 KB
2	Bird	259 * 194	21.6 KB	19.7 KB
3	Baboon	350 * 350	32 KB	29.4 KB

VI. CONCLUSION

In this paper, a new image encryption algorithm is proposed. This algorithm is based on the Fuzzy sets to confuse the relationship between the plain image and the encrypted image. The proposed encryption algorithm can ensure multiple criteria such as lossless, maximum distortion, maximum performance and maximum speed. The proposed encryption method, in this paper, has been tested on different format images and showed good results.

ACKNOWLEDGMENT

This paper is part of PhD work in the Department of Electronics and telecommunication, S.G.G.S. institute of Engineering and Technology, S.R.T.M University, Nanded, India.

REFERENCES

[1] Gamil R.S. Qaid , Sanjay N. Talbar, "Encryption and Decryption of Digital Image Using Color Signal" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 2, PP. 588 -592,March 2012.

[2] Komal D. Patel, Sonal Belani "Image Encryption Using Different Techniques: A Review", International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 1, PP. 30 -34. 2011.

[3] Borko Furht, Edin Muharemagic, Daniel Socek "Multimedia Encryption and Watermarking",Springer,USA.2005.

[4] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),PP.229-234.

[5] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition, 34 (2001),PP.1229- 1245.

[6] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari, Hamida Almangush," A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1,PP.41-47 July 2012.

[7] Liu, Z., et al.," Image encryption scheme by using iterative random phase encoding in gyrator transform domains", Optics and Lasers in Engineering, 2011. 49(4): PP. 542-546.

[8] Guo, Q., Z. Liu, and S. Liu, "Color image encryption by using Arnold and discrete fractional random transforms in HIS space", Optics and Lasers in Engineering, 2010. 48(12): PP. 1174-1181.

[9] Liu, Z., et al.," Image encryption by using gyrator transform and Arnold transform", Journal of Electronic Imaging, 2011. 20: PP. 013020.

[10] R. Tao, X. Y. Meng, and Y.Wang." Image encryption with multi orders of fractional Fourier transforms In Information Forensics and Security", 2010: IEEE Transactions on Image Processing.

[11] Zunino, R.,"Fractal circuit layout for spatial décor relation of images", Electronics Letters, 1998. 34(20): PP. 1929-1930.

[12] Zhang, G. and Q. Liu, " A novel image encryption method based on total shuffling scheme". Optics Communications, 2011.

[13] Zhao, X. and C. Gang." Ergodic matrix in image encryption", 2002.

[14] Zhu, Z., et al., "A chaos-based symmetric image encryption scheme using a bit-level permutation" Information Sciences, 2011. 181(6): PP. 1171-1186.

[15] Huang, C. and H. Nien," Multi chaotic systems based pixel shuffle for image encryption", Optics Communications, 2009. 282(11): PP. 2123-2127.

[16] Wang, K., et al., On the security of 3D Cat map based symmetric image encryption scheme. Physics Letters A, 2005. 343(6): PP. 432-439.

[17] Wang, X.Y., et al., A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics, 2010. 62(3): PP. 615-621.

[18] Fuzzy Logic: An Introduction [online] http://www.seattlerobotics.org

[19] Europe Gets into Fuzzy Logic" ,Electronics Engineering Times, 1991

[20] "Fuzzy Sets and Applications: Selected Papers by L.A. Zadeh", ed. R.R. Yager et al. (John Wiley, New York,1987).

[21] "U.S. Loses Focus on Fuzzy Logic" (Machine Design, June 21, 1990).

[22] Wang, Y., et al., A new chaos-based fast image encryption algorithm. Applied Soft Computing, 2011. 11(1): p. 514-522.

[23] Monisha Sharma, Shri Shankarcharya, Manoj Kumar Kowar, "Image Encryption Techniques Using Chaotic Schemes: A Review" International Journal of Engineering Science and Technology. Vol. 2(6),PP. 2359-2363.2010.

[24] Nawal El-Fishawy, Osama M. Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms " International Journal of network Security, Vol.5, No.3, PP.241–251, Nov.2007.

[25] Sara Tedmori, Nijad Al-Najdawi " Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform" IAJIT First Online Publication vol.3,2011.

[26] Nassiba Wafa Abderrahim , Fatima Zohra Benmansour , Omar Seddiki "Integration of chaotic sequences uniformly distributed in a new image encryption algorithm" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.

Mr. Gamil R. S. Qaid is a Ph.D. student at S.G.G.S. Institute of Engineering and Technology, Nanded, India. He is doing research in the field of images security. He received the B.E and M.E. degree (Computer Engineering & information Technology) from Kursk State Technical University , Russia, in 2005 and 2007, respectively. He is a lecturer in Computer Engineering Department, Faculty of Computer Science & Engineering, Hodeidah University.Yemen.

S.N. Talbar has received his B.E and M.E degree from the S.G.G.S. institute of Engineering and Technology, Nanded, India, in 1985 and 1990 respectively. He is obtained his Ph.D. from SRTM University, India in 2000. He received the Young Scientist Award by URSI, Italy in 2003. He had a collaborative research program at Cadiff university Wales. UK. Currently, he is working as professor in Electronics and telecommunication Department of S.G.G.S. institute of Engineering and Technology, Nanded, India. He is member4 amember of many prestigious committees in the academic world of India. His research interests are Signal & image processing. Pattern Recognition and Embedded System Design. He has published 40 Papers in Journals and had about 105 papers in conferences

◈◈◈