Encryption and Decryption of Digital Image Using Color Signal

Gamil R.S. Qaid [1], Sanjay N. Talbar [2]

[1] **Research Student, Electronics & Telecommunications Dept., S.G.G.S. institute of Engineering and Technology, Nanded, India.**

[2] **Professor Dept., Electronics & Telecommunications, S.G.G.S. institute of Engineering and Technology, Nanded, India.**

ABSTRACT

This paper aims at improving the level of security and secrecy provided by the digital color signal-based image encryption. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage. This new proposed encryption algorithm can ensure the lossless of transmissions of images. The proposed encryption algorithm in this study has been tested on some images and showed good results.

KEY WORDS:

Encryption, Decryption, Image, Color Signal, Digital Image,

1. INTRODUCTION

The rapid spread of the digital world nowadays which is powered by ever-faster system demands greater speed and security. Real time to secure an image is challenging due to the processing time and computational requirement for encryption and decryption. In order to cope with these concerns, innovative image compression and encryption techniques are required.

Encryption is a common technique to uphold image security. Image and video encryption have application in various fields including Internet Communication, Multimedia Systems, Medical Imaging, Tele-medicine and Military Communication.

Many techniques for image encryption were employed in the past. They included selective bit plane encryption, fuzzy PN codes based on color image encryption, polarization encryption, data encryption, standard DES etc. with varying degrees of success to attack resistance and other features. [1]

Recently, with the greater demand for digital world, the security of digital images has become more and more important since the communications of digital products over open network occur more and more frequently [2, 3, 6]. Surveys of the existing work on image encryption were also gave general guideline about cryptography and concluded that all techniques were useful for real-time image encryption. Techniques described in those studies can provide security functions and an overall visual check, which might be suitable in some applications. So no one can access the image which transferring on open network.

2. OBJECTIVES OF THE STUDY

This paper aims at providing high security for the digital images data and keeping them from spying. It also aims at getting encryption algorithm

accuracy and safety features and maintaining the images data from loss when decryption process.

Image encryption is one of the most important applications in transferring images through the internet and cellular phones.

Steps of encryption algorithm:

1- Sending the image to the function Encrypt which, in turn, sends the image to the function affine, which calls the procedure Keys to generate the randomly prime number between (1– 256), under the condition that the common denominator between this number and 256 should be the integer one and keeping it in the matrix (A)

2- Storing seven random keys in a matrix.

3- Dividing the image into a set of blocks.

4- Encrypting each 7bits with the seven keys which stored in matrix (A), according to the following equation:

$$\text{Cipher Bit} = (A * \text{plain Bit} + K) \bmod 226. \quad (1)$$

5- Repeating the step No. (4) in each 7 bits in the same block.

6- Repeating the steps No.(4) and (5) in all blocks

7- Resegmenting the image into whereas each block is a matrix of (4*4)

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

9- Taking each 2 vertically adjacent bits from the bottom of the image (b1, b2)

10- Doing XOR between (b1 and b2) as:

$$b = b1 \; XOR \; b2. \quad (2)$$

11- Doing XOR between the (b and 256) as:

$$Cipher\ Bit = b \; XOR \; 256. \quad (3)$$

Steps of decryption algorithm:

1- Taking each 2 vertically adjacent bits from the beginning of the image (b1, b2)

2- Doing XOR between (b1 and b2) as:

$$b = b1 \; XOR \; b2. \quad (4)$$

3- Doing XOR between the (b and 256) as:

$$Cipher\ Bit = b \; XOR \; 256. \quad (5)$$

4- Resegmenting the image into blocks each block is a matrix (4*4)

5- Doing the tract substitutes for each block in the image by converting the row to the column.

6- Taking the keys stored in the header of the image

7- Finding the inverse of each key from the keys stored in the inverse's matrix

8- Dividing the image into a set of blocks.

9- Decrypting each 7bits of the block accompanied with the inverse of the keys that stored in the matrix (A) according to the following equation:

$$Plain\ Bit = (A * (Plain\ Bit - K) \bmod 256. \quad (6)$$

10- Repeating the same step No. (9) for every 7 bits in the same block.

11- Repeating the steps No. (9) and (10) for all blocks.

3. APPLICATIONS AND USABILITY:

The algorithm encryption and decryption of an image transform an image into cipher code using the random keys, which allow users to have confidentiality and security in transmission of the image based data as well as in storage in the data warehouse

4. FEATURES:

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

5. EXPERIMENTAL VERIFICATION

The proposed work contents are as follows:

- Encryption and decryption images.
- Dividing the image into (n * n) of random block, where n is a value determined by user.
- Division switch: In this division, the swapping is between the image squares which is divided into (n*n) of blocks of image, the swapping blocks are defined by user.
- Defining the part of image by the user and doing some processes on it, such as save, redraw, encryption and decryption.
- Filters: In this work, doing some filters like grayscale, invert colors, lighten and darken, mirror vertically and horizontally, and histogram for R G B colors.

The proposed algorithm is implemented and tested on a range of different formats images. The results of the six images are given below:

Figure 1. Original images

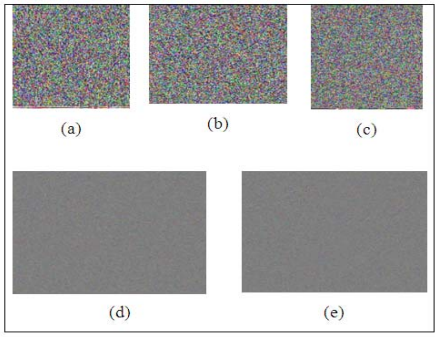

Figure 2. Encrypted images

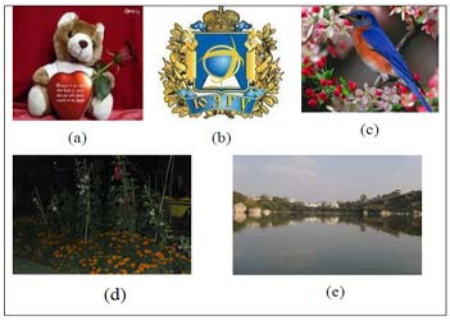

Figure 3. Decrypted images

Table 1 Results of selected Images

Original Image	Type	Dimension	Size	Decrypted Image	Lossless
a	jpg	186 * 139	5.59 KB	a	0
b	png	180 * 180	89.4 KB	b	0.0056
c	tif	259 *194	141 KB	c	0.2230
d	bmp	3968 * 2976	2.87 MB	d	0.0012
e	gif	3968 * 2976	3.52 MB	e	0.0032

$$error = \left(\frac{1}{m \cdot n} \sum_{i=1}^{n} \sum_{j=1}^{m} (Orig.Image(i,j) - Dec.Image(i,j))^2\right)^{\frac{1}{2}} \quad (7)$$

As shown in Table1, the proposed algorithms can be considered as lossless algorithms (original and decryption images are identical); whereas, other cryptography systems in general produce images that are susceptible to distortion and degradation of quality. Therefore, substantial encryption is achieved through the expense of quality. It is also necessary to judge the visual quality of the decrypted images in order to evaluate and compare the performance of different encryption methods.

From the above experiments figures, we can note that the goal lossless is satisfied by this algorithm because the decrypted images are similar to the original images. In other words, the errors in the decrypted images are almost equal to zero. It is clear that the errors between the encrypted images and original images is very low, and the distortion between the original images and the encrypted image is very high.

6. CONCLUSION:

The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage. The scheme presented in this paper has a simple implementation module. The proposed encryption algorithm can ensure multiple criteria such as lossless, maximum distortion, maximum performance and maximum speed. The proposed encryption method in this study has been tested on different format images and showed good results.

Future work will be focused on the development of this algorithm to get exactly errors equal to zero.

7. REFERENCES

[1] Borko Furht, Edin Muharemagic,Daniel SocekMultimedia Encryption and Watermarking,Springer,USA.2005.

[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] 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.

[4] 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.

[5] Ismet Ozturk, Ibrahim Sogukpınar, “Analysis and Comparison of Image Encryption Algorithms” World Academy of Science, Engineering and Technology 3,PP.26-30, 2005.

[6] Al-Ataby A. and Al-Naima F., “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform,” The International ArabJournal of Information Technology, vol. 7, no. 4,pp. 358-364, 2010.

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

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

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