V.Deepthi, Dr.Sandeep.V.M / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.1308-1311

Simple Tool For Efficient Image Cryptography

V.DEEPTHI[1] Dr.SANDEEP.V.M[2]
ECE Dept., JPNCE, Mahabubnagar, Andhra Pradesh[1]
HOD & Prof., ECE Dept., JPNCE, Mahabubnagar, Andhra Pradesh[2]

Abstract-

Secure transmission and storage of color images is gaining importance in recent years due to the proliferation of multimedia network applications. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, to get the encrypted image. In this paper we propose a new effective and simple method for image encryption which employs magnitude and phase manipulation using cross-over and mutation approaches for encrypting color images. The proposed approach is very sensitive to any slight changes in the secret key values, making it very different to decrypt heuristically.

Keywords- cross-over, cipher, cryptography, decryption, encryption, mutation.

I. INTRODUCTION

The rapid growth of computer networks, information security is an increasingly important problem popular application of multimedia technology and increasingly transmission ability of network gradually lead us to acquired information directly and clearly through images [6]. Hence image security has become a critical and imperative issue [7]. Image encryption techniques try to convert an image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption [1][8]. Many image encryption methods have been proposed but some of them have been known to be insecure [12], so we always in need to develop more and more secure image encryption techniques. Traditional data encryption techniques can be divided into two categories which are used individually or in combination in every cryptographic algorithm [2]. Image encryption approaches fall into two broad categories: spatial domain methods [9] and frequency domain methods [10] [14].

In this paper we present a novel image encryption scheme for magnitude and phase manipulations using crossover and mutation techniques these techniques are composed with a simple diffusion mechanism [13]. The proposed method dealing with private key cryptosystem in frequency domain and it can be retrieved from the encrypted image if and only if the key is known. The resulting encrypted

image is found to be fully distorted, resulting in increasing the robustness of the proposed work.
The remainder of this paper organized as follows. In section 3, we describe our proposed cryptosystem. We validate the proposed method through experiments and finally we conclude in section 4.

II. BACKGROUND

In this section we give an overview of different image encryption and decryption methods. Literature suggests many techniques for encryption and decryption.

2.1. DIGITAL SIGNATURE

A. Sinha and K.Singh [13] have proposed a technique to encrypt an image for secure image transmission. Before transmission digital signature of original image is embedded to the encoded version. Encoding is done by using error control code. At the receiver end after decryption digital signature is used to authenticity of the image without the knowledge of the specific error control code it is very difficult to obtain the original image. The dimensions of the image also changes due to the added redundancy increment in the size of the image due to added redundancy in the disadvantage of this algorithm.

2.2 Linear independence scheme and logistic map method

Hazem Mohammad Al-Najjar [3] proposed encryption method based on logistic map method. In this method by applying XOR operation between two neighbor pixels it will creates a linear independence relationship. Logistic map method is developed encryption keys for images by shuffling the pixel positions.

2.3 Chaotic sequence method:

Yi Kai-Xiang and Sun Xiang [5] give an image encryption algorithm based on chaotic sequence the real number value chaotic sequences. First, the real number value chaotic sequences using the key value is generated. Then it is dispersed in to symbol matrix and transformation matrix. Finally the image is encrypted using them in DCT domain. DCT is a lossy data compression technique, image may occur some distortions

caused by lossy data compression and noise, but this method can still correctly decrypt and restore original image, and can achieve a high security degree.

2.4.Double random phase encoding:

S. Zhang and M. A. Karim [15] have proposed a new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green-Blue) formats. The proposed single-channel color image encryption method is more compact and robust than the multichannel methods. This technique introduces color information to optical encryption. An RGB color image is converted to an indexed image before it is encrypted using a typical optical security systems. At the decryption end, the recovered indexed image is converted back to the RGB image. Since only one channel is needed to encrypt color images, it reduces the complexity and increases the reliability of the corresponding optical color image encryption systems [11].

2.5 Spatial domain:

The approaches in this category are based on direct manipulation of pixels in an image. In this algorithm the general encryption usually destroys the correlation among pixels and thus makes the encrypted image incompressible. By using spatial domain the encryption efficiency is very less.

From above discussions we can say that due to the redundancy, distortions and noise in images may reduces the efficiency of encryption levels. To overcome these problems the proposed method is useful. In this method by using the crossover and mutation operations will results in better encryption efficiency.

III. EFFICIENT AND ROBUST IMAGE ENCRYPTION

In this paper, we propose a method that improves the encryption efficiency and yet maintain its simplicity in implementation. The method uses cross-over and then mutation process in frequency domain to achieve a better encryption.

3.1Transposition method in frequency method:

Frequency domain gives a better encryption of an image than spatial domain. The Fourier transform of an image can be complex and hence both the magnitude and the phase functions are necessary for the complete reconstruction of an image from its Fourier transform. Displacing the component positions in original image the new scrambled image will be created which can be hard to understand. The process of shuffling is done by considering different combinations of components in an image. By reordering the adjacent components the original image can be encrypted but it is near to the original image. To increase the security different combinations of re-order mechanisms are used. Just replacing the pixel positions or reordering the neighboring rows and columns is not sufficient for the better image encryption so we have to implement a new algorithm for image encryption and decryption.

After reordering process the mutation operation is performed. In this mutation **NOT** operation is applied on the reordered components. Disadvantage of this method is the encrypted image is easily recognized because the scrambled image components are having the same components as the original image.

3.2 Image Encryption and Decryption in FFT:

Further improvement of image encryption a new effective algorithm is introduced in frequency domain.FFT is a fast algorithm for discrete Fourier transform. Here in this case FFT is a secret key between the users for encryption and decryption of an image. When the fast Fourier transform is applied to the original image the components are a combination of real and imaginary parts. The complexity of scrambled image will be increased by adding some more new algorithms to encrypted images along with FFT.

3.3 Cross-Over Operation:

In this section two frequency domain components are taken and combined about crossover point their by creating two new components. The cross-over method is used for swapping the real and complex parts of the one component with the real and complex parts of other component, which will result in a change in the amplitude and the phase of the new components. Reversibility of crossover operation the same indices will be generated and consequently the crossover effect will be removed and the original components will be retrieved again [15]. Before applying the crossover operation the image is containing the below real and complex values.

R1=real1, C1=complex1
R2=real2, C2=complex2

After performing the crossover operation on image the resultant components will be formed as follows;

R1=complex2, C1=real2
R2=complex1, C2=real1

3.4 Mutation Operation:

Mutation technique is introduced to further complicate the encryption. In this method NOT operation is performed on the components. By applying mutation the resultant components are

compliment of an original image which will gives the beneficial encryption results. This mutation function is self invertible

3.5 Mixture of cross-over and Mutation:

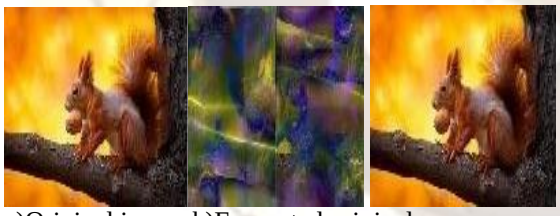
Combination of crossover and mutation methods will give better privacy when compared to the individual methods and also gives the confidential results. In this section the Mutation method is added along with the crossover technique for better image encryption in frequency domain. This simulation will results very nice encryption effects and good robustness.

3.6.RGB model

In order to improve the privacy of scrambled color images the combination of crossover and mutation methods are performed on tri-colors (Red, Green and Blue) of an image. Ciphering of image by slicing the image into sub images whose dimensions are kept confidential and applied proposed methods to each of these sub images this will increases the efficiency of an encryption.

a) Original image b) Encrypted image c) Decrypted image

Fig1: The response of Proposed Cryptosystem on a Color Image



a)Original image b)Encrypted original c)Decrypted image

Fig2: Response of proposed method

IV. Performance evolution:

The proposed method is applicable for gray-scale images and also for color images. From the above shown encrypted image we can say that the regions of the scrambled image are totally invisible.

Experiments conducted wherein the various encrypted images are shown to a group of 50 people to identify them. The fewer the number of people who could identify the object in the image, the better efficient will be encryption algorithm.

TABLE1

Encryption / Decryption efficiency of the proposed method.

S.NO	Object type	Encryption efficiency in %
1.	Animals	96
2.	Human beings	90
3.	Flowers	75
4.	Historical places	98
5.	Natural images	84

The table shows the number of encrypted images that the viewers were able to visualize and recognize the objects that were in the original image. The fewer the objects were recognized, the better will be the encryption process. It can be seen from the table that the images containing object like flowers are very easily recognized. Encryption complexity in such cases should be increase.

V. CONCLUSION & FUTURE WORK:

In this paper, a successfully efficient implementation of encryption scheme is introduced for digital image encryption. This encryption scheme proposed crossover and mutation operation on the frequency domain components of the plain image, therefore changing this components amplitude and phase in order to achieve more confusion and diffusion in the cipher image. When compared to many commonly used algorithms the proposed algorithm resulted in the best performance. According to the results of our proposed method, we conclude that the future research will be expanded to increase the efficiency of fewer objects which are recognized by the viewers, by adding some new algorithms along with the proposed method to increase the complexity.

References:

[1] H. El-din H. Ahmed, M. K Hamdy, and O. S. Farag Allah, "Encryption quality analysis of theRC5 block cipher algorithm for digital images," Optical Engineering, Vol. 45, Issue 10107003, 2006.

[2] B. A. Forouzan, “Traditional Symmetric-Key Ciphers,” in Introduction to Cryptography and Network Security, 1st ed., New Yourk, the McGraw-Hill Companies, Inc., 2008, ch. 3, sec. 1,pp. 60-61.

[3] Hazem Mohammad Al-Najjar,”Digital Image Encryption Algorithm Based on a Linear Independence Scheme and the Logistic Map”.

[4] Ibrahim S I Abuhaiba and Maaly A S Hassan ‘’image encryption and decryption using differential evaluation approach in frequency domain”. signal and image

processing: An International Journal (SIPIJ) vol.2, No.1, March 2011.

[5] Yi Kai-Xiang and Sun Xing et al., "An image encryption algorithm based on chaotic sequences," Journal of Computer Aided Design and Computer Graphics, Vol. 12, No. 9, 2000, pp. 672-676

[6] W. Lee, T. Chen and C. Chieh Lee, "Improvement of an encryption scheme for binary images," Pakistan Journal of Information and Technology. Vol. 2, no. 2, 2003, pp. 191-200..

[7]. A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, Vol. 1, no. 1, 2006, p.127.

[8] B. Mohammad Ali and J. Aman," Image Encryption Using Block-Based Transformation Algorithm," IAENG Int. Journal of Computer Science, Vol. 35, Issue 1, 2008, pp. 15-23.

[9] S. K. Panigrahy, B. Acharya, and D. Jena, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm," 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[10] S. R. M. Prasanna, Y. V. Subba Rao and A. Mitra, "An Image Encryption Method with Magnitude and Phase Manipulation using Carrier Images," International Journal of Computer Science, Volume 1, Number 2, February 20, 2006

[11] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," IEEE Trans. Multimedia, 2002.

[12] Li. Shujun, and X. Zheng "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process, Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, pp. 708-711.

[13] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Optics Communications, 2003, pp. 1-6

[14] W. Zeng and S. Lei, "Efficient Frequency Domain Selective Scrambling of Digital Video," IEEE Trans. Multimedia, 2002.

[15] S. Zhang and M. A. Karim, "Color image encryption using double random phase encoding," Microwave and optical technology letters, Vol. 21, No. 5, June 5 1999, pp. 318-322.

Authors Information:

1.V.Deepthi Pursuing M.Tech(DSCE) from JayaPrakash Narayana College of Engineering B.Tech(ECE) from JayaPrakash Narayana College of Engineering Currently she is working as Assistant Professor at Jayaprakash narayan college of engineering And has 2 years of Experience in teaching . Her areas of interest include,Image Processing ,wireless networks, signal processing

2. Dr. Sandeep V.M. completed Ph.D in Faculty of Electrical and Electronics Engineering, Sciences, from Visveswaraiah Technological University, Belgaum, and M.Tech from Gulbarga University and B.Tech from Gulbarga University. His research interests are in the areas of Signal and Image Processing, Pattern Recognition, Communication, Electromagnetics. He is Reviewer for Pattern Recognition Letters (PRL). He acted as Reviewer for many International Conferences.He has 24 years of teaching experience. He is member of LMIST – Life Member Instrument Society of India (IISc, Bangalore). And he guided more than 100 projects at UG level and 35 at PG level.And published more than 10 papers in international journals and 9 Conference Proceedings.