Image Encryption For Color Images Using Bit Plane And Edge Map Cryptography Algorithm

R.Gopinath[1], M.Sowjanya[2]

[1]M.tech.Student, Sri Indu College of Engineering & Technology, Hyderabad

[2]Associate Professor, Sri Indu College of Engineering & Technology, Hyderabad

Abstract

Image encryption is used to protect the images and transform into different format. In this paper, lossless encryption for color images using binary key images has been proposed. In proposed method, the key image size is same as the original image. The key image is either a bit plane or an edge map generated from another image. The method is discussed against common attacks such as the plaintext attacks, brute force attack and cipher text attacks. The experimental results shows that the lossless encryption of all type of images.

Keywords-lossless image encryption, key-image, plaintext attack, brute force attack, ciphertext attack, bit plane, edge map.

I.INTRODUCTION

Image encryption is an effective approach to protect images or videos by transforming them into completely different formats. Several data encryption algorithms like Data Encryption Standard (DES) [1] and Advanced Encryption standard (AES) [2] are being employed for protecting digital information, chaos based [3] and combinatorial permutations [4] are proposed for encrypting images. Applications in the automobile, medical, Construction and the Fashion industry require designs, scanned data, building plans and blue-prints to be safe guarded against espionage. Considering the long life time of images in the mentioned domains, it is imperative to develop and employ techniques which protect the content throughout their lifetime [5].

Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain [6-8]. One example is the recursive sequence based image scrambling approach. It scrambles images using different recursive sequences such as the Fibonacci sequence [9], Cellular automata [10] and chaotic maps [11-12]. Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain [13, 14]. These approaches have extremely low security levels due to the lack of security keys. Another approach for image encryption is to change image pixel values based on the combination of image bit plane decomposition and logic operations [15, 16]. This security method is also much lower because the results of its decomposition process and logic operations are predictable. It's not immune to plaintext attacks. To achieve higher levels of security, solution is to change image pixel values or blocks while scrambling the positions using different techniques.

In this paper is organized as follows. Proposed algorithm in section II. Section III describes the comparative performance. The simulation results are presented in Section IV. Concluding remarks are made in Section V.

II.PROPOSED ALGORITHM

The color image encryption, i.e. color images and 3D animal and medical images, the color images are contain the several 2D components, each component can be considered as a 2D image. In this paper, the original and existing images are color

images. The image encryption in binary-key image follows two procedures

i) BitplaneCrypt algorithm for color image

ii) The EdgemapCrypt algorithm for color image

These two algorithms explained detail shown below

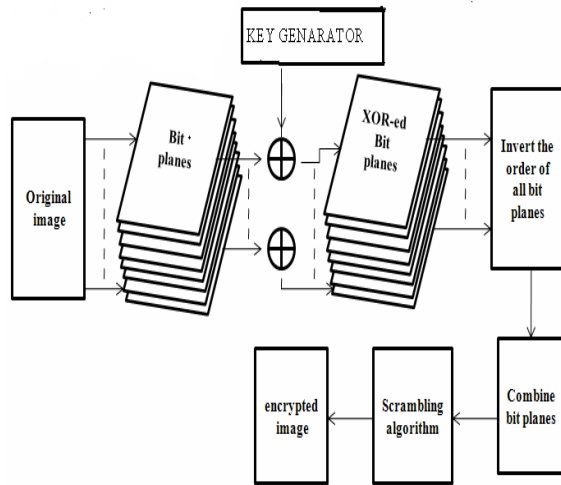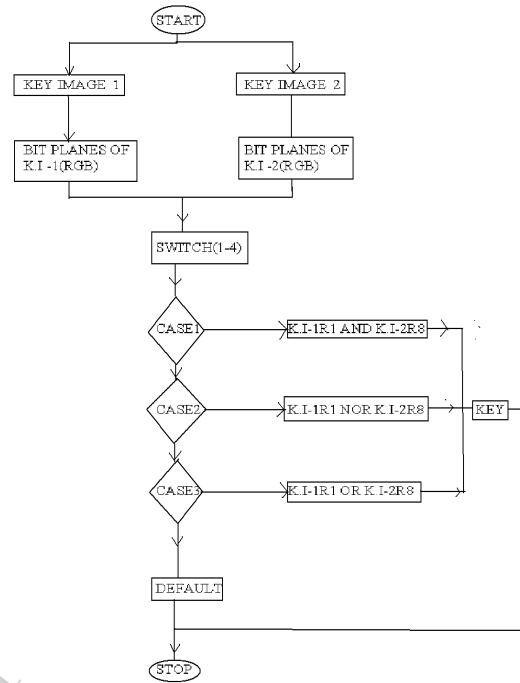### i) BitplaneCrypt algorithm for color image

Figure 1.

The block diagram of bit plane Crypt algorithm as shown fig.1 Select two key images and split them in to their respective components (R, G, and B). Then switch case is used to select different cases (1-3).Key is generated. The key-image size is same as the original image. Perform the XOR operation between the key image and each bit plane of the original image, the XOR-ed bit planes are invert the order of all bit planes and combined. Finally scramble the resulting image using a selected scrambling method to generate the resulting encrypted image. In color image contain 3 colors. They are i=1 represent as red, i=2 represent as green and i=3 represent as blue.

In the decryption process, the correct security keys should be provided to the authorized user to generate the key-image. The user unscrambling the encrypted image using the corresponding scrambling algorithm, the resulting image into bit planes. Applied an XOR operation between the key-image and each bit plane the order of bit planes is reverted to the original order. The original image can be reconstructed by combining all bit planes.

Key Generation Flow chart.

ii) The EdgemapCrypt algorithm for color image

The edge map is frequently used in image enhancement, compression, segmentation and recognition. The application of edge maps can also be extended to image encryption. An edge map is considered as the key-image in this algorithm. The edge map is generated from new/existing image for color or grayscale image with same size as the original image using the specific edge detector with a selected threshold value. The new image or any existing edge detector or any threshold value to generate the edge map used as a key-image. They also have flexibility to use any existing image scrambling method for the EdgemapCrypt algorithm. The security of this algorithm consist of the image or its location which is used to generate the edge map, type of edge detector, threshold value, and the security keys of the scrambling algorithm. To reconstruct the RGB image, the users should be provided the correct security key-image (i.e. edge map). The decryption process first generates the edge map from the selected image using the security keys. It then unscrambles the encrypted image using the selected scrambling algorithm. Next, it decomposes

the unscrambled image into its binary bit planes and performs XOR operation between the edge map and each bit plane. The order of all bit planes is restored to the original order. And combine all bit planes [17].

The algorithm of EdgemapCrypt algorithm as shown below

Take color image

Calculate edge map from exiting image with same size of original image

Decompose the original color image into binary bit plane

Apply XOR operation between edge map and biplane of original image

Combine all bit planes together to obtain the 3D image.

Scramble the resulting image using a selected scrambling method to generate the resulting Encrypted image.

II.EXPERIMENTAL RESULTS

The experimental results of color image as shown below. The propsed algorithm has successfully implemented for lossless compression.

Fig.(a)   Fig.(b)
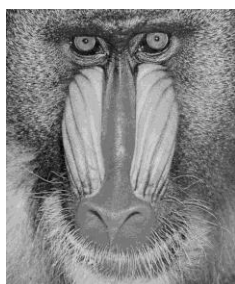
Figure (a) Original image.(b) Key image 1.

Fig. (c)   Fig. (d)

Fig (c) Key image 2. (d) Encrypted image

Fig. (e)

Fig (e) Decrypted image

III.CONCLUSION

In this paper, two algorithms are implemented for lossless encryption. To generate key image an either a bit plane in the BitplaneCrypt or an edge map in the EdgemapCrypt algorithm. These two algorithms produced lossless encryption for all type of formats like jpeg, bmp and so on. Both algorithms are easy to implement in hardware because they operate at the binary levels. They are also suitable for multimedia applications and real time application such as mobile phone services and wireless networks.

REFERENCES

[1]   National Institute of Standards and Technology, "Data Encryption Standard (DES)," http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.

[2]   National Institute of Standards and Technology, "Advanced Encryption Standards (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf,   2001.

[3]   J. Cheng; J.I. GUI, "A new chaotic key-based design for image Encryption and Decryption," The 2000 IEEE International Symposium on Circuits and Systems, 2000. Proceedings. ISCAS   Geneva, vol.4, pp. 49-52, May. 2000.

[4]   S. Li, C. Li, G. Chen, N. G. BourBakis, and K.-T. Lo, "A General quantitative cryptanalysis of Permutation-only Multimedia ciphers against plaintext attacks," Signal Processing: Image Communication, vol. 23, no. 3, pp.212-223, 2008.

[5] K. C. Iyer and A. Subramanya, "Image Encryption by Pixel Property Separation,"

http://eprint.iacr.org/2009/043.pdf, Cryptology ePrint Archive, 2009.

[6] M. Ashtiyani, P. M. Birgani, and H. M. Hosseini, "Chaos-Based Medical Image Encryption Using Symmetric Cryptography," in Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on, 2008, pp. 1-5.

[7] M. Yang, N. Bourbakis, , "Data-image-video Encryption," potential, IEEE, vol. 23, no. 3, pp. 28-34, 2004

[8] Y. Zhou, S. Again, V. M. Joyner, and K. Panetta, "Two Fibonacci p-code based image scrambling algorithms," in Image Processing: Algorithms and Systems VI, San Jose, CA, USA, 2008, pp. 681215-12.

[9] J. Zou, R. K. Ward, and D. Qi, "A new digital image Scrambling method based on Fibonacci numbers," in Circuits And Systems, 2004. Iscas'04. Proceeding of the 2004 International Symposium on, 2004, pp.III- 965-8 vol. 3.

[10] R.-J. Chen and J.-L. Lai, "Image security system using Recursive cellular automata substitution," pattern

Recognition, vol. 40, no. 5, pp. 1621-1631, 2007.

[11] J. C. Yen and J. I. Geo, "Efficient hierarchical Chaotic Image Encryption algorithm and its VLSI

realization," Vision, Image and Signal Processing, IEEE Proceeding-,vol.147, no. 2, pp. 167-175, 2000.

[12] Z. H. Guan, F. J. Huang, and W. J. Guan, "Chaos-based Image Encryption algorithm," Physical Letters A,

vol. 346,No. 1-3, pp. 153-157, Oct 2005

[13] G.-S. GU and G.-Q. Han, "The Applications of Chaos and DWT in Image Scrambling," in Machine Learning

and Cybernetics, 2006 International Conference on, 2006, pp. 3729-3733.

[14] T. Li, S. Zhou, Z. Zeng, and Q. Ou, "A new ScramblingMethod based on semi-frequency domain and chaotic

System," in Neural Networks and Brain, 2005. ICNN&'05. International Conference on, 2005, pp.607-610.

[15] J.-W. Han, C.-S. Park, D.-H. Ryu and E.-S. Kim, "Optical Image Encryption based on XOR operations,"

Optical Engineering, Vol. 38, no. 1, pp. 47-54, 1999.

[16] R. Lukac and K. N. plataniotis, "Bit level based secret Sharing for image encryption," Pattern Recognition,

vol. 38, no. 5, pp. 767-772, 2005.

[17] Simhadri kollu, p.soundarya "Lossless Encryption for Color Images using a Binary Key-image" vol. no.9 issue

no.2,314-321

Mr.**R.GOPINATH** graduate from Swami ramananda tritha institute of science & technology in **Electronics& Communications**. Now pursuing Masters in **Digital Electronics and Communication Systems** (DECS) from Sri Indu College of Engineering & Technology.