FAST IMAGE ENCRYPTION BASED ON RANDOM IMAGE KEY

D Naga Sudha[1]
[1]Research Scholar JNTUH College of Engineering, Hyderabad, Telangana, India.

Abstract: Image encryption can be defined in such a way that it is the process of encoding secret image with the help of some encryption algorithm in such a way that unauthorized users can't access it. To send an image over the network secretly, the sender tries to find encryption algorithm to hide image information. In this paper t aims at designing an efficient encryption algorithm for color image using random image key generated with minimum time execution for encryption and decryption operations. XOR operation is used here to make more diffusion of the encrypted image to maintain a higher level of security upon transference than it is with the original image. In this paper introduces a new concept for image encryption using a binary "key-image". The key-image is either a bit plane or an edge map generated from another image, which has the same size as the original image to be encrypted. In addition, we introduce two new lossless image encryption algorithms using this key image technique. The performance of these algorithms is discussed against common attacks such as the brute force attack, ciphertext attacks and plaintext attacks. The analysis and experimental results show that the proposed algorithms can fully encrypt all types of images. This makes them suitable for securing multimedia applications and shows they have the potential to be used to secure communications in a variety of wired/wireless scenarios and real-time application such as mobile phone services.

Introduction: Network technologies and media services provide ubiquitous conveniences for individuals and organizations to collect, share, or distribute images/videos in multimedia networks and wireless or mobile public channels. Image security is a major challenge in storage and transmission applications. For example, video surveillance systems for homeland security purposes are used to monitor many strategic places such as public transportation, commercial and financial centers. Large amounts of videos and images with private information are generated, transmitted, or restored every day.

Image encryption is an effective approach to protect images or videos by transforming them into completely different formats Several interesting approaches for image encryption have been developed. One method based on the cryptography concept considers images as data blocks or streams. It encrypts images block by block or stream by stream using different techniques. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two examples of this approach. However, such encryption methods incur large computational costs and show poor error resilience.

Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain .One example is the recursive sequence based image scrambling approach. It scrambles images using different recursive sequences such as the Fibonacci sequence, Cellular automata and chaotic maps .Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain. Nevertheless, these approaches have extremely low security levels due to the lack of security keys or the small key space.

II Related work: Pratibha S. Ghode et al improved a keyless method for image cipher in lossless color images to encrypt and decrypt image without any loss of data quality. Khanzadi H. et al proposed an image encryption algorithm using bit sequence random generator based on Chaotic Logistic and Tent maps. Mirzaei et al introduced a new parallel algorithm for image encryption.

First of all, the plain image is divided into 4 equal blocks and then the position of each block is shuffled. Then a total shuffling algorithm is applied to the whole image. After this, we use different values for encrypting each pixel in each of the 4 blocks of the whole image. Wei et al. introduced image encryption algorithm depending on Deoxyribonucleic acid (DNA) and chaotic system. As well as using Hamming distance to generate the secret keys.

However, Panduranga and Naveen proposed a hybrid approach for partial image encryption to rearrange the mapping image and select a pixel value of re-arranged mapping image based on the mapping function through converting the pixel value of original image into a row and column values of mapping image. Ibrahim and Maaly present a new effective approach for image encryption which employs the main Discrete Fourier

Transform (DFT) followed by Differential Evolution (DE) approach. On the other hand, Wang et al. suggested a new image encryption algorithm based on chaotic maps. It changes the values of the image pixels jointly with the pseudorandom which is generated by chaotic maps. It does not require the width to be equal to the height of the image.

Seyedzade et al implemented a new algorithm which makes it parallel depending on SHA-512 by taking half data of image for encryption of the other half to increase the speed of processing. Min and Lu proposed an algorithm to generate a relation between the plain image and the generated pseudo numbers which are used to shuffle process and pixel value. Pall et al suggested three encryption algorithms in order to develop the security image. Codebook, Index table and Codebook Index Table were applied by using Vector Quantization to compress data of image and XOR operation followed by random methods. Pang introduced an encryption algorithm depending on Daubechies wavelet transform to encrypt image data using binary sequences which were generated by chaos theory. Acharya et al. suggested an efficient approach using Hill Cipher and random key for every block for encryption of image depending on the properties of the matrix. AlKhassaweneh et al. proposed an approach based on random vectors to encrypt the image by stratifying the least square approximation techniques.

Proposed Method: fast algorithm is proposed here to encrypt and decrypt color image. Proposed algorithm applies for any size of image. In symmetric image encryption, the sender and the receiver must share the same key. In this paper, a new algorithm is designed to generate image key from the same image or any image selected by the sender. XOR logic plays the main role in this algorithm. The basic idea is cutting the picture where not everyone can recognize them, especially if it has been cut horizontally and vertically into smaller parts as much as possible. In this paper, image key is generated according to this idea by rotating the origin image to three directions. The four images are cut and scrambled randomly then using XOR logic to generate image key.

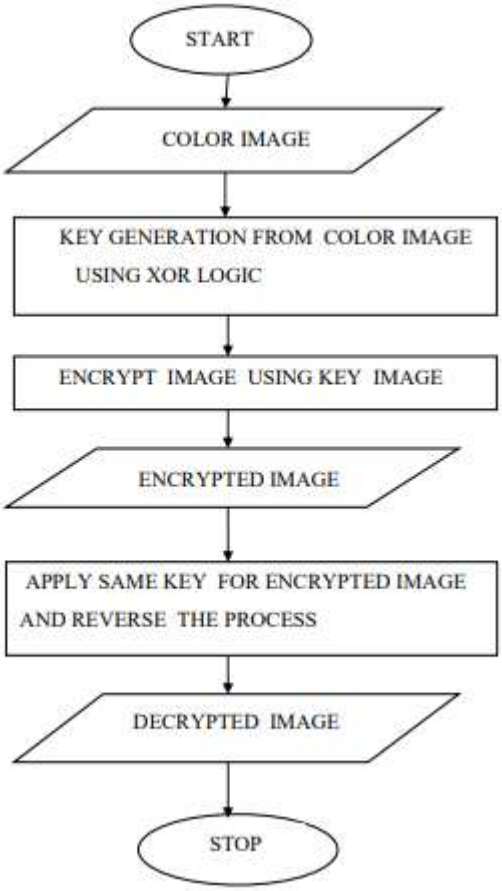

Figure 1 . Process flow

Image Key Generating Algorithm Steps: 1. Input color image. 2. Rotate color image to three directions (left, right and down). 3. Cutting and random permutation each image which get from step 1 and 2. 4. Generate primary key from step 3 using XOR logic. 5. Analysis primary key to three channels (R, G and B). 6. Flip R to three directions (left to right, up to down and right to left) 7. Rotate R and flip it to three directions (left to right, up to down and right to left) 8. For all matrixes generated in steps 6 and 7 use XOR to get new R. 9. Repeat steps from 6-8 to get new G and New B. 10. Reconstruct R, G and B to new image. 11. Use XOR between origin image in step1 and new image in step 9. 12. Analysis image in step 11 to three channels (R, G and B). 13. Apply XOR for R, G and B to generate image key. 14. End

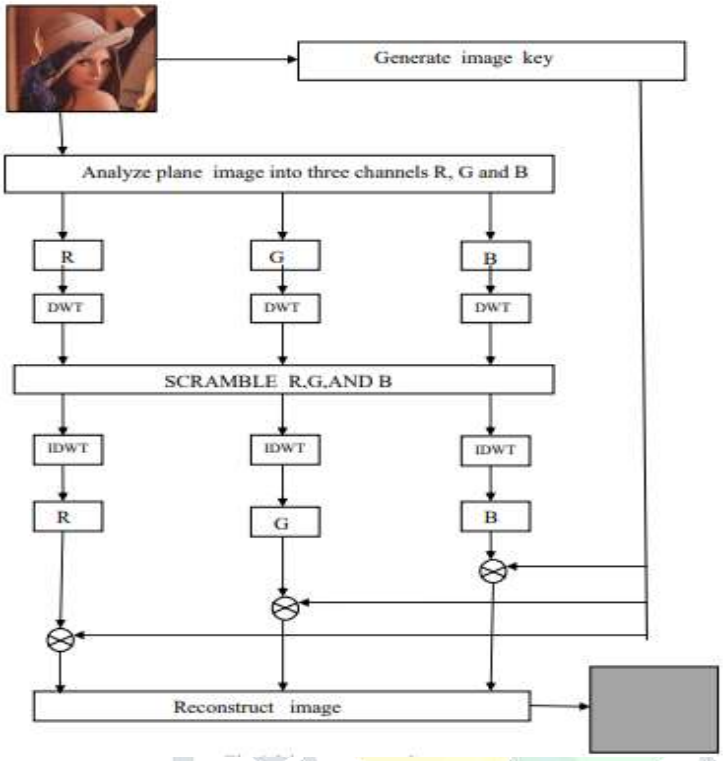

Figure 2 Image Encryption

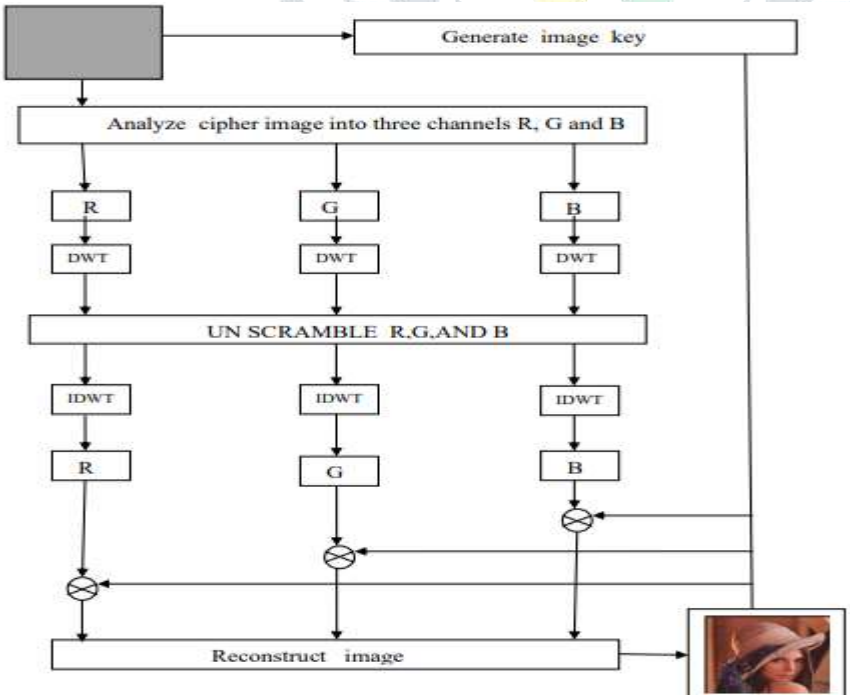

Figure 3. Image decryption

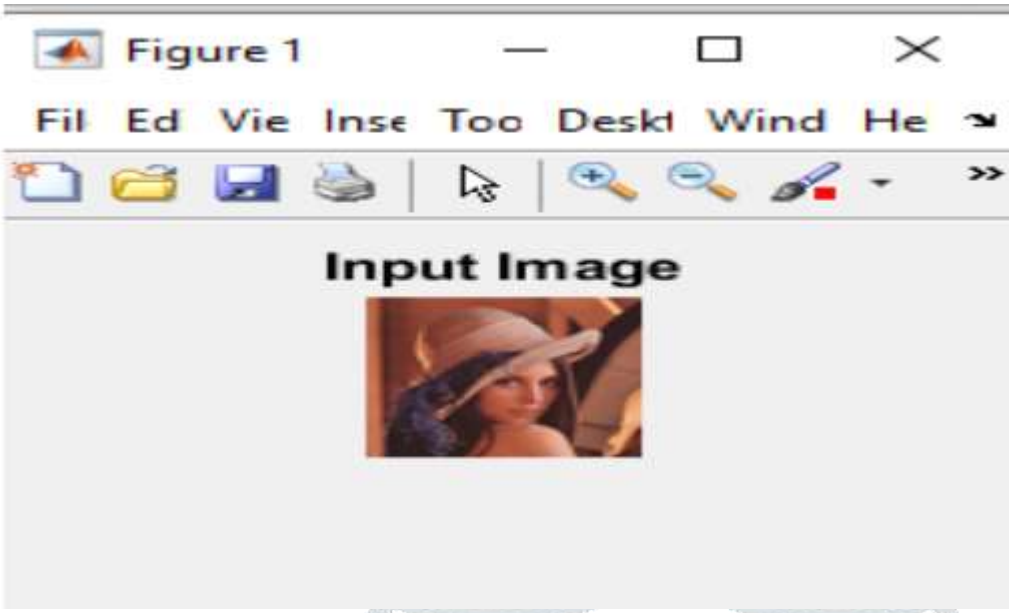

Figure 4. Input Image

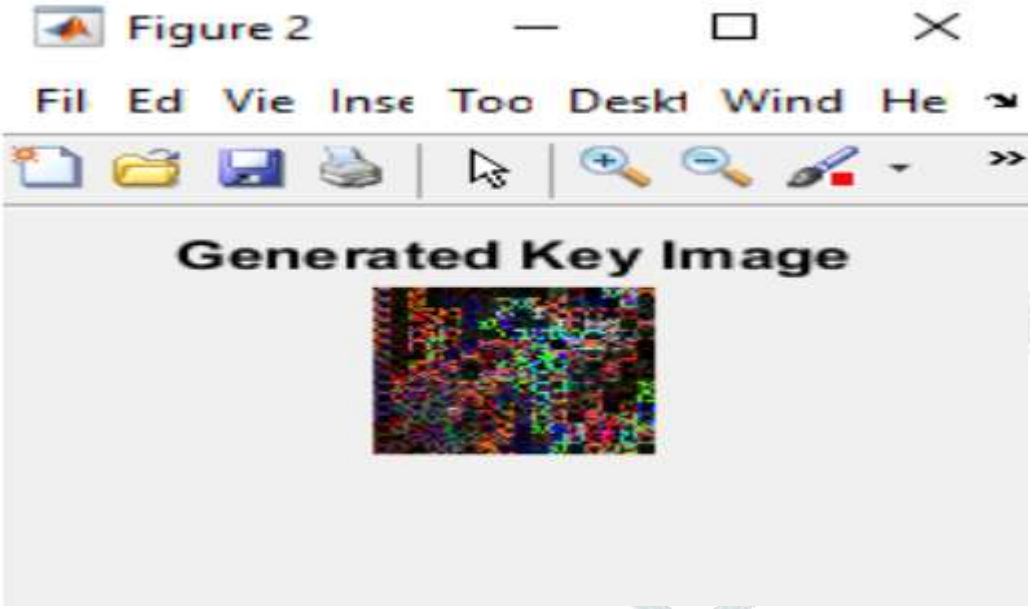

Figure 5 Generated key image

Figure 6. Encrypted Image

Figure 7: Decrypted image

Figure 8. Parameters of image

Conclusions: The color image encryption and decryption algorithm is proposed and implemented depend on fast image key. Image key can generate from the same image or any image must the same size of origin color image. The sender and receiver shared the same image key which has the same properties of hash function therefore, the attacker cannot discover the plain image from the image key notably, if one pixel value is changed, different key will generated. Proposed algorithm give a good results through applied some

statistical tests as well the proposed algorithm achieved encryption rate about 0.134136 and 0.106204 for decryption rate.

Finally, it is possible to encrypt partial image instead of full image encryption. Also it can be applied as a block cipher instead of stream cipher to get good results. As well as it can be developed by compression of the plain image with image key to reduce the cost of data transition.

References:

1. Wang X., Zhao J. and Liu H. 2012 "A new image encryption algorithm based on chaos", Elsevier.Vol.285 No.5, pp562–566.

2. Changgui Shi, Sheng-Yih Wang, Bharat K. Bhargava 1999: "MPEG Video Encryption in Real-time Using Secret Key Cryptography". PDPTA: pp2822-2828. 3. Wu Y., Noonan J., and Agaian S. 2011: "NPCR and UACI randomness tests for image encryption", Journal of Selected Areas in Telecommunications (JSAT), pp. 31–38.

4. Pratibha S. Ghode, SEM IV. and Tech M. 2014 "A Keyless approach to Lossless Image Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 5, pp 1459-1467.

5. Khanzadi H., Eshghi M. and Borujeni S. E. 2013 "Image Encryption Using Random Bit Sequence Based on Chaotic Maps", Arabian Journal for Science and Engineering AJSE, Vol.39, No. 2, pp1039–1047

6. Mirzaei O., Yaghoobi M. and Irani H. (2012) "A New Image Encryption Method: Parallel Sub-Image Encryption with Hyper Chaos", Nonlinear Dynamics, Vol. 67,No. 1, pp557-566.

7. Wei X., Guo L., Zhang Q., Zhang J., and Lian S. 2012 "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system",The Journal of Systems and Software, Vol. 85, No. 2, pp290- 299.

8. Panduranga H. T. and Naveen kumar S. K. 2011 "Hybrid Approach to Transmit a Secrete Image", 2nd National Conference on Emerging Trends and Applications in Computer Science IEEE.

9. Ibrahim S. I. Abuhaiba and Maaly A. S. Hassan 2011 "Image Encryption Using Differential Evolution Approach In Frequency Domain", Signal & Image Processing An International Journal SIPIJ Vol. 2, No. 1.