A Hybrid Image Encryption Algorithm for secure communication

K.Sivaranjani
M.E Communication Systems
Parisutham Institute of Technology and Science, Affiliated to Anna University, Chennai.
Tamilnadu, India.
ranjaniikannan@gmail.com

Mr.P.Bright prabahar
Assistant Professor Dept of ECE
Parisutham Institute of Technology and Science, Affiliated to Anna University, Chennai
Tamilnadu, India.
bright.prabahar@gmail.com

Abstract*— Image encryption design is one of important research field in multimedia security. This paper is proposed with a hybrid encryption technique for the color image based on the random permutation, rotation operation, cipher block chaining (CBC) technique. Then scrambling operation is based on the RGB planes in specified directions such as horizontal vertical, diagonal This method completely eradicates the outlines of the encrypted images, blurs the distribution characteristics of RGB-level matrices, and effectively protects against the decryption of exhaustive attack method. In the proposed system improved security is deployed without the use of transform domain. Testing and analysis part of the image can done using various parameters to ensure the security and effectiveness of this proposed approach. Eventually, pragmatic images are adopted as examples to prove the great encryption performance of the proposed method and also the good potential for practical applications in image encryption.

***Keywords*—random permutation; rotation; CBC; scrambling**.

I. INTRODUCTION

We are living in a society subjugated by information technology and in an era of information where huge amount of Information can be speedily processed and saved on easily accessible media. The explosion of Internet applications leads people into the digital world, and communication via digital data becomes frequent. However, new issues also arose and have been explored, such as data security in digital communications, copyright protection of digitized properties, invisible communication via digital media, etc. Generally speaking the standard of information security has not kept pace with this development. For example, information that before was saved on a large amount of paper and physically difficult to steal can today be saved on a disk that can easily remove. Information security deals with several different 'trust' aspects of information. Another common term is information assurance. Information security is not confined to computer systems, or to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form. Information security chain is needed when information is threatened, lost or misused. Contrarily, in this electronic era of revolutionary changes to the nature of information, it has become difficult to confirm the safety or truth of data, due to the spread of tools used for distortion and manipulation and the capacity of some people to harness technology to serve malevolent ends. This is what led us to think about developing a system to verify the safety of all the contents of the images and keep it safe from any alterations or counterfeiting, intentionally or unintentionally.

II. PROPOSED APPROACH

A. Concept

The main objective of this projected system is that to endow with a two level of corroboration along with the scrambling method. This can be achieved without using any transformation process.

The proposed technique uses a color image and gives an encrypted image which can be decrypted later for various purposes. Firstly the secret image is divided into three planes such as R, G; B .Encryption process is done with the help of random permutation followed by some rotation operation. Two level of corroboration is used for this encryption operation for each plane. Finally scrambling is done for RGB in horizontal, vertical, diagonal directions for each plane in order to make the image more secure.

B. Cipher block chaining

Cipher block chaining (CBC) is a mode of operation for a block cipher one in which a sequence of bits is encrypted as a single unit or block with a cipher key applied to the entire block). One of its key distinctiveness is that it uses a chaining method that causes the decryption of a block of cipher text to depend on all the foregoing cipher text blocks. As a result, the entire validity of all foregoing blocks is contained in the immediately previous cipher text block. A solitary bit slip-up in a cipher text block affects the decryption of all ensuing blocks. Transcription of the order of the cipher text blocks

causes decryption to become corrupted. Basically, in cipher block chaining, each plain text block is XORed with the immediately previous cipher text block, and then encrypted.

C. Scrambling

In this proposed method scrambling is done for the RGB planes in specified directions such as horizontal, vertical, diagonal. It prevents unauthorized people without the gibing decryption key from being able to view the information. The intended user with the correct key can only can unscramble the message and see the contents

D. Encryption Process

Step1: Read the secret color image.

Step2: First the secret image is divided into RGB planes.

Step 3: After the image is subdivided into Red plane. Random permutation is done to the image using the pixel values. It is initiated here to create the random sequence

Step4: The first key is for rotating the image key number of times.

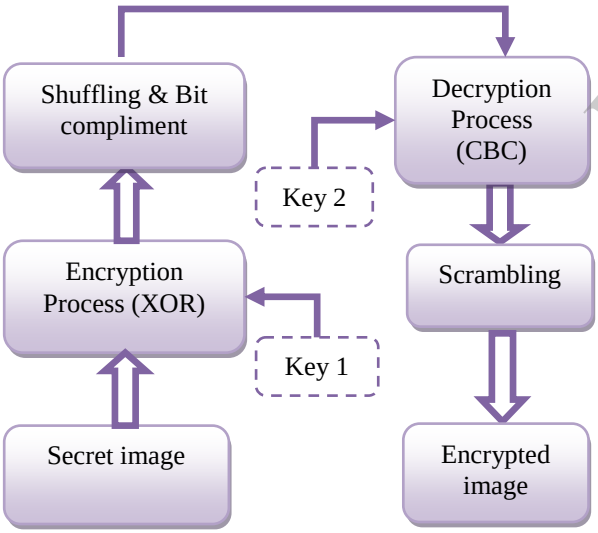


Fig 1: Block Diagram for image encryption

Step5: Shuffled image is obtained. Convert this rotated image into binary

Step6: Then XOR process is done in the first level of substantiation.

Step7: Then make a shuffle of each bit in every pixel of binary image and complement it.

Step8: Apply the most popular techniques in cryptography i.e., Cipher Block Chaining mode to the resultant shuffled image with their keys.

Step9: Then convert each pixel into decimal again.

Step 10: Finally scrambling is done for RGB planes in horizontal, vertical, diagonal directions for each plane in order to make the image more secure.

Step11: Similarly these processes are performed to Green and blue planes also.

Step12: Store the resultant image as encrypted image**.**

E. Decryption Process

Step 1: Read the encrypted image.

Step2: Encrypted image is divided into RGB planes.

Step3: decryption process is performed to the Red plane first.

Step4:Descrambling operation is performed to the red plane.

Step5: Apply CBC process with the key 2 and convert it into binary.

Step6: Take complement to binary.

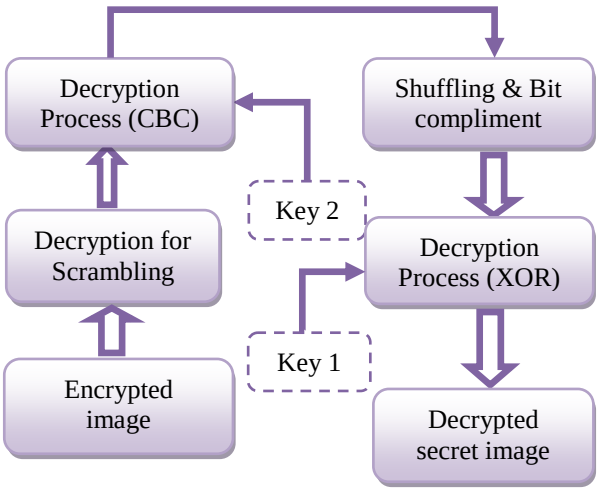


Fig 2: Block Diagram for image decryption

Step7: XOR process is done to the red plane.

Step 8: Shuffle the binary values as in encryption and convert it to decimal. again.

Step9: The Key 1 is used for rotating the image with key number of times.

Step10: Similarly these processes (step 4 to step 9) are performed to Green and blue planes also.

Step11: Finally combine all the planes to obtain the original image.

Step12: Store the resultant image as decrypted (original) image.

III. STOCHASTICITY TEST

Ergodic properties top the priorities of a consummate encryption model. Original and enciphered images are shown in figures which look absolutely absurd. Random literally mentions the processes bring forth identically detached and free-lance samples. The process is random if pragmatic value is determined through its position in sequence else through subsequent observations. Tentative outcomes suggest that this output produced in this paper is absolutely random giving no hint about the clandestine information.

A. MSE:Mean Square Error

MSE is the difference between secret image and encrypted image. This difference must be very high for a better performance.

MSE = (1/MN)*(secret image-encrypted image) (1)

For a 256 * 256 image the values of M = N = 256

B. PSNR: Peak Signal to Noise Ratio

It is the ratio of peak signal power to noise power. It is measured for image quality. For a good encrypted image the value of PSNR must be low.

$$\text{PSNR} = \mathbf{10log_{10}}\left(\frac{I_{max}^2}{MSE}\right) \text{ dB} \quad (2)$$

I_{max} is the maximum intensity of image

Maximum intensity of 256 * 256 images is 255 (0 to 255)

Therefore equation (2) becomes,

$$\mathbf{PSNR} = \mathbf{10log_{10}}\left(\frac{255^2}{MSE}\right) \mathbf{dB} \quad (3)$$

C. Bit Error Rate (Ber)

BER is also a performance criterion which tells about the error witnessed in the procedure. This proposal gives it approximately as 0.5 for all the images. It confirms there is almost 50% error rate which is very much needed in image encryption routines. Since, here witnessed huge error, it qualifies this project as a magnificent modus operandi.

D. Correlation of Two Adjacent Pixels

A correlation is a statistical measure of security that expresses a degree of relationship between two adjacent pixels in an image or a degree of association between two adjacent pixels in an image. The aim of correlation measures is to keep the amount of redundant information available in the encrypted image as low as possible.

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{var\,(x)}\sqrt{var\,(y)}} \quad (4)$$

$$cov\,(x,y) = E[(x_i - E\,[x_i])(\,y_i - E\,[\,y_i])] \quad (5)$$

$$E\,[x] = \frac{1}{N}\sum_{i=1}^{N} x_i\,,\; E\,[y] = \frac{1}{N}\sum_{i=1}^{N} y_i, \quad (6)$$

$$var\,(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E[x_i])^2 \quad (7)$$

$$var\,(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E[y_i])^2 \quad (8)$$

IV. SIMULATION AND EXPERIMENTAL RESULTS

A.Encryption

To justify the effectiveness of this project, the algorithm is simulated in MATLAB 7.10 with Peacock image&Temple images are taken as the secret image. These images are in the equal dimension with 256*256

1. *Test images:* The secret image here taken are peacock and temple images with the dimensions of 256*256. These secret images are Joint Photographic Expert Group image (Jpeg). These images are divided based on three planes RGB (Red, Green and Blue) and scrambling is done to all the three planes. It is depicted in Figure 3 & figure 4.

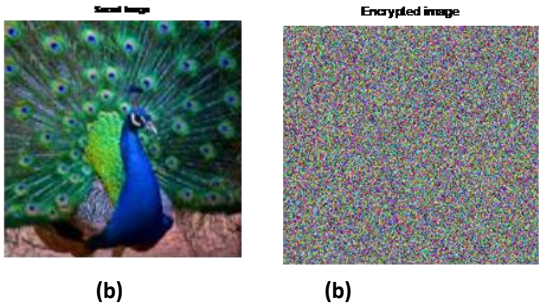


Fig 3a) Secret image b) Encrypted image

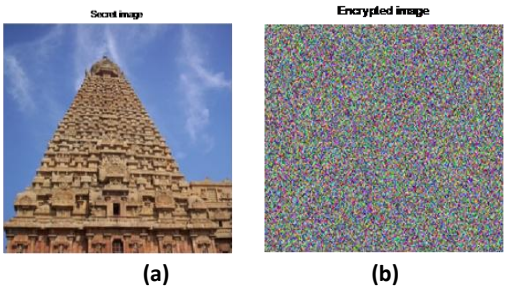


Fig 4a) Secret image b)Encrypted image

2. *Histogram Analysis:* To prevent information leakage to attackers, it is important to ensure that the encrypted and original images do not have statistical similarities. The image histogram clarifies how the pixels in an image are distributed using graphical display of the pixels. The basic idea is to compare the histograms of the original and encrypted media. This is Depicted in the following figures for the test images such as the peacock and temple image in Figure 5 & 6.

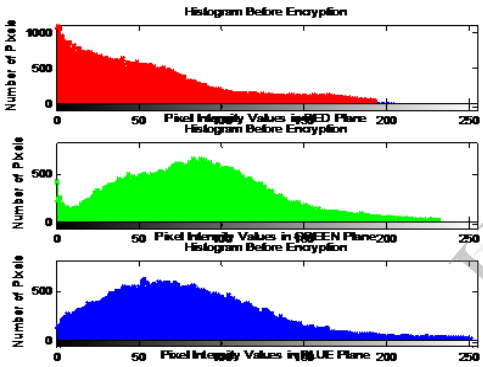


Fig 5(a) Histogram before Encryption

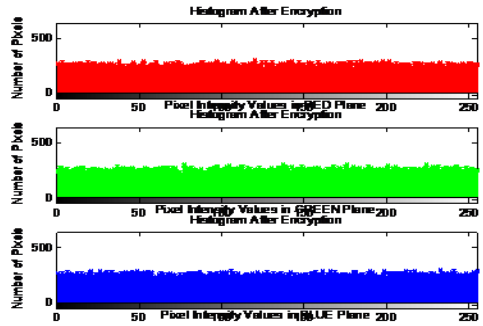


Fig 5(b) Histogram after Encryption

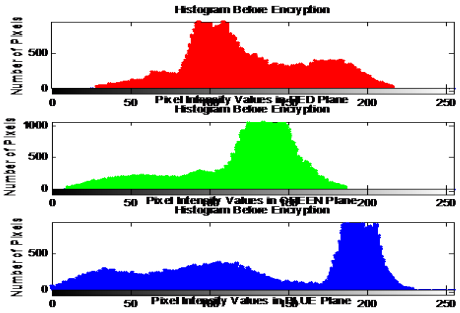


Fig6(a) Histogram before Encryption

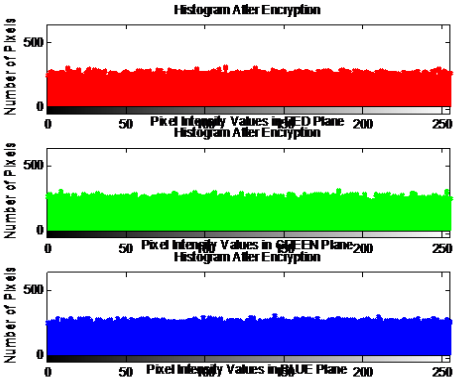


Fig6 (b) Histogram after Encryption

3. *Performance Analysis*: Performance analysis is done to the proposed method. In Table 1 Mean Square Error(MSE) values for the Secret image (original) is depicted. In Table 2 Peak signal to Noise Ratio (PSNR) values for the Secret image (original) is depicted. In Table 3 Bit Error Rate is depicted. In Table 4 Correlation Coefficient of Original And Encrypted images of peacock and temple is depicted.

TABLE 1
PERFORMANCE ANALYSIS-MSE

Secret image	MSE		
	Red	Green	Blue
Peacock	4.4670e+003	3.0692e+003	3.3391e+003
Temple	2.3159e+003	2.2484e+003	3.1635e+003

TABLE 2
PERFORMANCE ANALYSIS- PSNR

Secret image	PSNR		
	Red	Green	Blue
Peacock	11.6306	13.2605	12.8945
Temple	14.4836	14.6121	13.1291

TABLE 3
PERFORMANCE ANALYSIS- BIT ERROR RATE

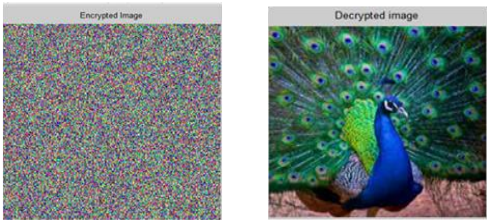
Secret image	BER	Total No of Pixel errors
Peacock	0.5006	262444
Temple	0.4995	261867

TABLE 4
PERFORMANCE ANALYSIS-CORRELATION COEFFICIENT

Correlation coefficient	Secret image		Encrypted image	
	Peacock	Temple	Peacock	Temple
Vertical Correlation	0.9243	0.7518	0.0011	-0.0077
Horizontal Correlation	0.9128	0.8838	-0.0026	-0.0011
Diagonal Correlation	0.8662	0.7000	-0.0057	0.0046

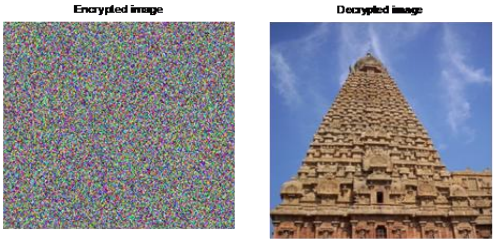
B.Decryption

Even though encryption at the sender is the prime concern of this project, decryption is also given importance to prove that this modus operandi works well in the receiver side as well. This image is retrieved with no deformation in anyway thereby proving the efficiency of the algorithm. The highlight here is unless and until one has the correct keys and knows the encryption mode, he or she cannot recover the original image. This is depicted in figure 7&8.



(a) **b)**

Fig 7 (a) Encrypted image (b) Decrypted image



(a) (b)

Fig 8 (a) Encrypted image (b) Decrypted image

V. CONCLUSION

This paper is proposed with a new hybrid encryption technique for the color image based on the random permutation, rotation operation, cipher block chaining (CBC) technique .Then scrambling operation is based on the RGB planes in specified directions such as horizontal vertical, diagonal This method completely eradicates the outlines of the encrypted images, blurs the distribution characteristics of RGB-level matrices, and effectively protects against the decryption of exhaustive attack method. This can be achieved in the spatial domain itself, without making it so complex by incorporating transform domain. The intended scheme is trouble-free, rapid and approachable to the secret key.

REFERENCES

[1] Ahmed Bashir Abugharsa1, Abd Samad Bin Hasan Basari2 and Hamida Almangush , "A Novel Image Encryptionusing an Integration Technique ofBlocks Rotationbased on the Magic cube and the AES Algorithm"

[2] CAO Guang-hui1, Hu Kai, Yang He and E Xu, "Algorithm of Image Encryption based on Permutation Information Entropy**",** 2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010), DOI: 10.7763/IPCSIT.2012.V53.No.2.16

[3] Changci Wen, Qin Wang , Xianghong Liu , Fumin Huang "An Image Encryption Algorithm Based on Scrambling and Chaos" Journal of Information & Computational Science 10:17 (2013) 5725{5733 November 20, 2013

[4] Gaurav Bhatnagar, Q.M. Jonathan Wu," Selective image encryption based on pixels of interest and singular value Decomposition", 2012 Elsevier, 1051-2004.

[5] H B Kekre, Tanuja Sarode, Pallavi Halarnkar "Image Scrambling using R-Prime Shuffle", IJAREEIE, ISSN (Print): 2320 – 3765, Vol. 2, Issue 8, and August 2013.

[6] Huan Zhang, Ruhua Cai "Image Encryption Algorithm Based on Bit-Plane Scrambling and Multiple Chaotic Systems Combination", 2010 IEEE. 978-1-4244-6837-9/10.

[7] ISO 7498-2:1989, Information Processing Systems, Open Systems Interconnection, Basic Reference Model—Part 2: Security Architecture, http://www.iso.org, International Organization For Standardization; 19.

[8] Ji Won Yoon, Hyoungshick Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps" ,2010 Elsevier, 1007-5704

[9] Jun Lang, "Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation," 2012 Elsevier, 0143-8166.

[10] Manjunath Prasad , K.L.Sudha "Chaos Image Encryption using Pixel shuffling" D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 169–179, 2011,DOI: 10.5121/csit.2011.1217

[11] Nanrun Zhou, YixianWang, LihuaGong, XiuboChen, YixianYang,"Novel color image encryption algorithm based on the reality preserving fractional Mellin transform," 2012 Elsevier, 0030-3992.

[12] Narendra K Pareek "Design and analysis of a novel digital Image encryption scheme" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[13] R.Gopinath, M.Sowjanya, " Image Encryption For Color Images Using Bit Plane And Edge Map Cryptography Algorithm", International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October – 2012 ISSN: 2278-0181

[14] Ratinder Kaur, V. K. Banga "Image Security using Encryption based Algorithm", International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP'2012) July 15-16, 2012 Singapore.

[15] Rinki Pakshwar , Asst Prof. Vijay Kumar Trivedi , Prof.& HOD Vineet Richhariya " Image Encryption Using Random Scrambling and XOR Operation", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March – 2013 ISSN: 2278-0181

[16] Sesha Pallavi Indrakanti, P.S.Avadhani "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011.

[17] Yong Feng, Juan Li, Fengling Han, and Tohari Ahmad "A Novel Image Encryption Method based on Invertible 3D Maps and its Security Analysis", 2011 IEEE, 978-1-61284-972-0/11

[18] Yue Wu ,Yicong Zhou, Joseph P. Noonan, Karen Panetta, Sos Agaian "Image Encryption using the Sudoku Matrix" Mobile Multimedia/Image Processing, Security, and Applications 2010,Proc. of SPIE Vol. 7708, 77080P doi: 10.1117/12.853197

[19] Zhang Yong "Image Encryption with Logistic Map and Cheat Image" 2011 IEEE ,978-1-61284-840-2/11

[20] Zhengjun Liu, MengYang , WeiLiu, SheLi, MinGong, WanyuLiu , ShutianLi, "Image encryption algorithm based on the random local phase encoding in gyrator transform domains",2012 Elsevier, 0030-4018.