Fast Image Encryption based on Random Image Key

Abdulrahman Dira Khalaf
College of Administration & Economics
University of Fallujah

ABSTRACT

Internet plays an important role in circulating a huge amount of multimedia. An example of this multimedia is the image. To send an image over the network secretly, the sender tries to find encryption algorithm to hide image information. This paper 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.

General Terms

Image Processing, Security.

Keywords

Encryption, Decryption, Random Key, XOR operation.

1. INTRODUCTION

There is no doubt that information technology plays a significant role to support the computer applications to many users and establishments in the world like information security, information hiding and information retrieval. As a matter of fact, all users, who use multimedia such as image, audio, video and text, may need to protect information from attacks during sending or receiving them through channel. There are two challenges for multimedia encryption; the first one is the size of data and the second is the cost of encryptions [1]. In this paper, an image encryption method based on a new random key generated from the same image is going to be adopted. The previous related work takes into account to review the points of power in these studies and to see how researchers think in this field. Image Cryptosystem can be classified into two main sections; one for encryption and the other for decryption. The block cipher and stream cipher are two types of cryptosystem, so private key and public key are two strategies to be used in an encryption. In this paper a new algorithm is proposed to encrypt color image using symmetric key which is generated from the same image or any image can be selected. Some tests are applied here to determine performance algorithm. These are histogram, mean square error, peak signal to noise ratio, entropy, correlation coefficients, number of changing pixel rate and unified averaged changed intensity [2]. The proposed algorithm was satisfied with good results where speed of running was good for encryption and decryption algorithm.

2. LITERATURE REVIEW

In this section many studies are summarized here to survey some ideas about the image encryption during the last years. Pratibha S. Ghode et al. [3] 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. [4] proposed an image encryption algorithm using bit sequence random generator based on Chaotic Logistic and Tent maps. Mirzaei et al. [5] 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. [6] 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 [7] 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 [8] 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. [9] 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. [10] 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 [11] 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. [12] 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 [13] 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. [14] suggested an efficient approach using Hill Cipher and random key for every block for encryption of image depending on the properties of the matrix. Al-Khassaweneh et al. [15] proposed an approach based on random vectors to encrypt the image by stratifying the least square approximation techniques.

3. THEORY BACKGROUND

This section introduces the main theoretical background of image encryption and image transformation. There are many types of encryption algorithms developed through the previous time. Most of these methods dealt with text such as Rivest, Shamir and Adelman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES) to generate stream cipher from original text called plain text. Usually, there are three categories of image encryption approaches. First category depend on transposition, second category depend on substitution, the third category is hybrid between first and second [16].

3.1 Image Encryption

In multimedia encryption field, a big data can be obtained from an image. Therefore one of two strategies can applied, the first one is stream cipher, while the second is block cipher. Encryption algorithms require secret key. Secret key can be either symmetric cipher or asymmetric cipher. Secret key in symmetric encryption means that both the sender and the receiver agree on a single key for their communication; it is used to encrypt and to decrypt the data. While public key in asymmetric encryption through which everyone can encrypt data, but cannot decrypt it; only the person holding the secret key can decrypt this, such as RSA and ElGamal [17]. In block image cipher encrypt one block of input to process a block of output have the same size based on the same key then proceed to the next block. Stream ciphers are different to block ciphers; they do not transform blocks of data to another block of data instead based on a key [18].

3.2 Image Transformation

One of important spatial domain is wavelet transform. Haar wavelet transform gives us approximation coefficients in four components for color image. Assume we have an image, wavelet decomposition will filter this image into two component depend on rows these are Low pass filter (L) and High pass filter (H) each one will decompose with the same way to extract four components: LL,HL,LH and HH based on columns; the last three components represent the horizontal, vertical and diagonal respectively. Two-dimension inverse wavelet transform reconstructs the four components to recover the original image; figure 1 illustrates the wavelet and inverse wavelet transforms [19].

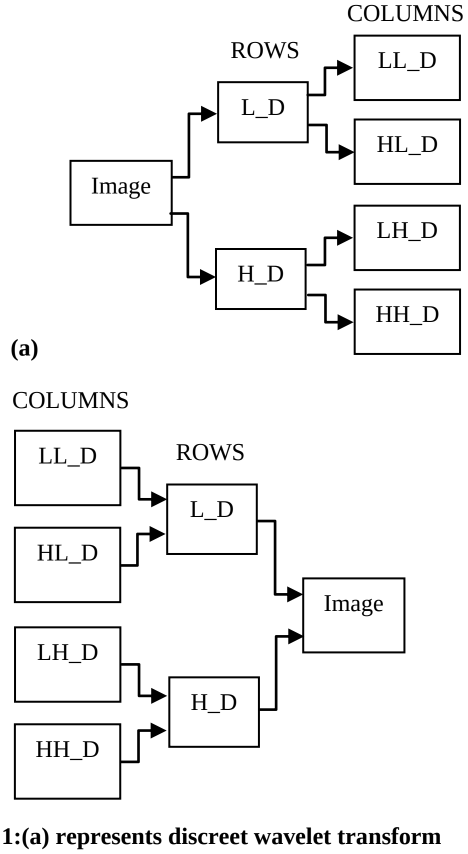


Figure 1:(a) represents discreet wavelet transform decomposition for 1 level , (b) represents discreet inverse wavelet transform decomposition for 1 level, D:Decomposition, R:Reconstract, L: Low pass filter and H:High pass filter.

4. PROPOSD ALGORITHM

In this section, 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. The algorithm can be illustrated through the following algorithm.

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.

After introducing color image, the system will generate the symmetric random image key to use in image encryption. As shown in figure 2 each channel of origin image will extract features by applying Haar wavelet transform to give us four components Low Low, High Low, Low High and High Low. In scrambling stage, the complements of last three components take to multiply by (-1) to reverse sign of elements then use shifting to satisfy more confusion and diffusion. To get the scrambled image, Inverse Wavelet Transform is used here. Image encryption will be completed by using XOR logic between the image key generate and scrambling image. Finally, reconstruct image from three channels to get the cipher image.

The steps of proposed encryption algorithm can be illustrated as below:

1. Input plain color image
2. Generate secret key from the plain color image.
3. Get R, G, and B components for color image.
4. Extract features for R, G, and B using Wavelet Transform.

5. Scramble each R, G, and B.
6. Use Inverse Wavelet Transform to obtain new image.
7. Encrypt every channel by secret key using XOR.
8. Combine R, G, and B channels to create the cipher color image.
9. Save cipher image.
10. End.

Decryption image can be obtained by reverse algorithm where the symmetric key is the same as illustrated in figure 3.

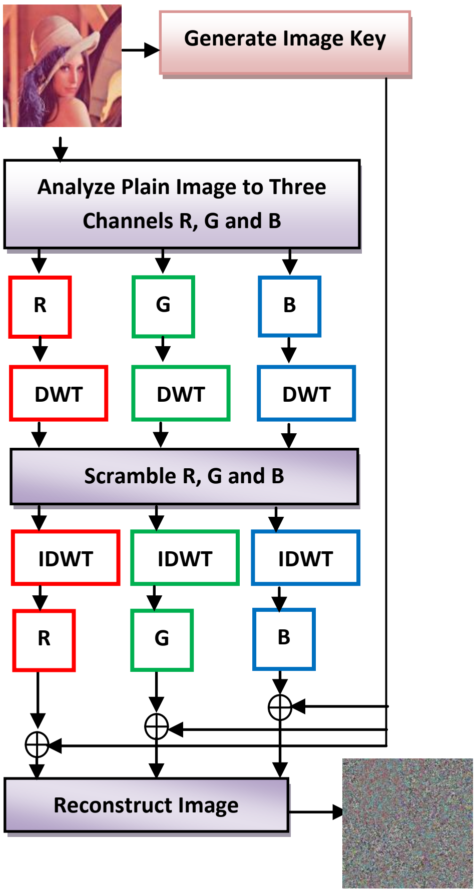


Figure 2: Proposed encryption algorithm

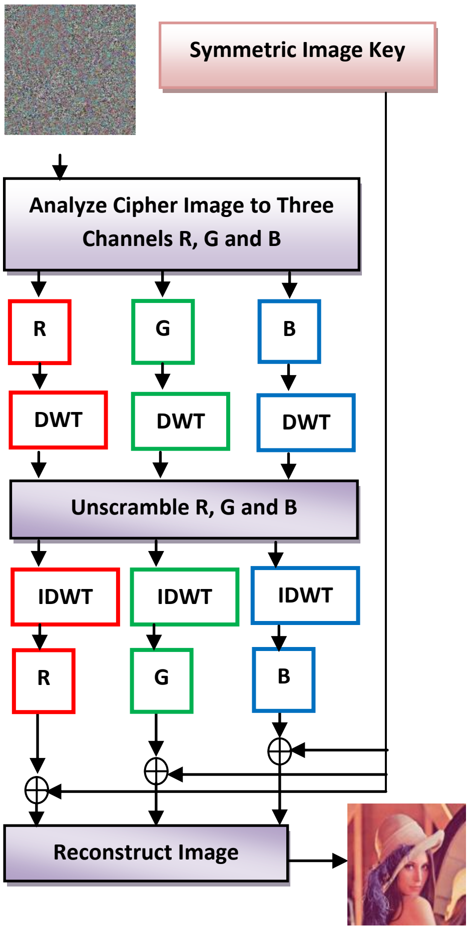


Figure 3: Proposed decryption algorithm

The steps of proposed decryption algorithm can be illustrated as below:

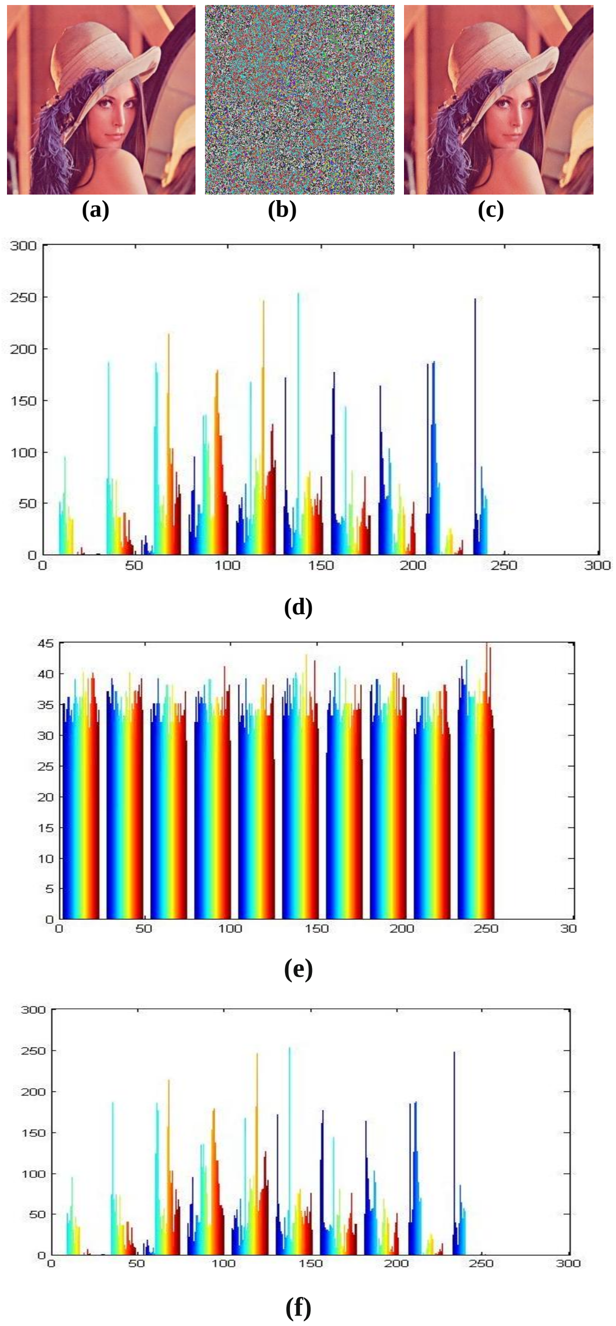
1. Input plain color image.
2. Get R, G, and B components for color image.
3. Extract features for R, G, and B using Wavelet Transform.
4. Unscramble each R, G, and B.
5. Use Inverse Wavelet Transform to obtain new image.
6. Decrypt every channel by secret key using XOR.
7. Combine R, G, and B channels to recover the plain color image.
8. Display origin image.
9. End.

5. RESULTS AND ANALYSIS

Proposed encryption algorithm is implemented using MATLAB R2013a on a personal computer running Windows. The color images with size 256 by 256 are used as input image through the application of the proposed algorithm. In this section, several tests are taken into account; histogram, correlation coefficient, Number of Changing Pixel Rate (NPCR) and Unified Averaged Changed Intensity (UACI), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and entropy of information.

5.1 Histogram

Histogram is statistics measure which is can be used to supply image statistics. It is a representation of color image by distributing the number of pixels to each value. Figure 4 gives us a good idea about histogram for Lena color image, for instance, where distributed pixels values for image encryption are equal to prevent attacker from access origin image. Red, blue and green channels of origin image are decomposed here for the same image, so the histogram for each component is shown in figure 5. The cipher and histogram of each channel through figure 6. Figure 7 can be display the image histogram of plain sample images (Pepper, Baboon and Plan) while figure 8 can be shown the image histogram for cipher these images based on proposed algorithms.



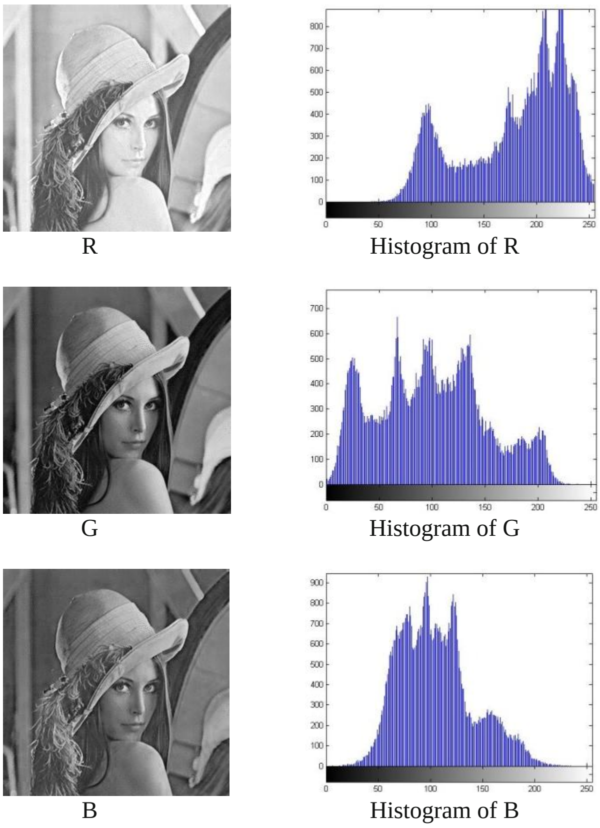
(a) **(b)** **(c)**

(d)

(e)

(f)

Figure 4: a, b and c are origin, encryption and decryption respectively of Lena color image, (d, e, f) histogram of (a, b, c)

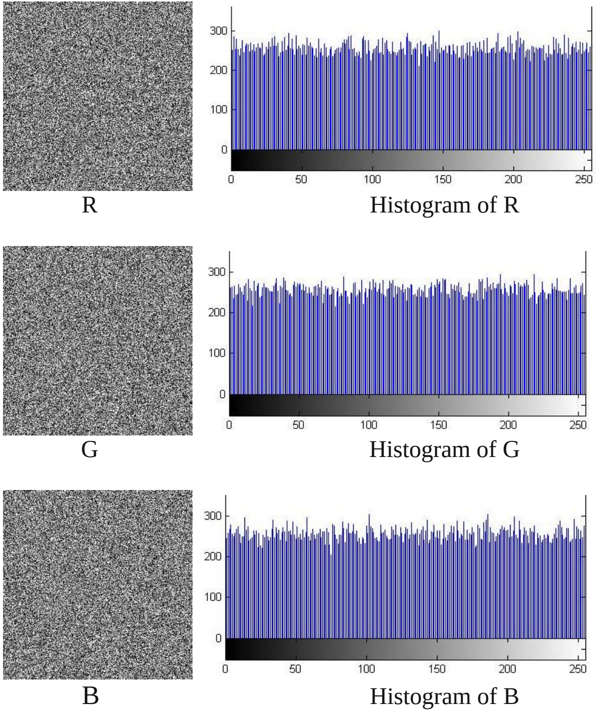


R Histogram of R

G Histogram of G

B Histogram of B

Figure 5: Origin image histograms for R, G and B of Lena

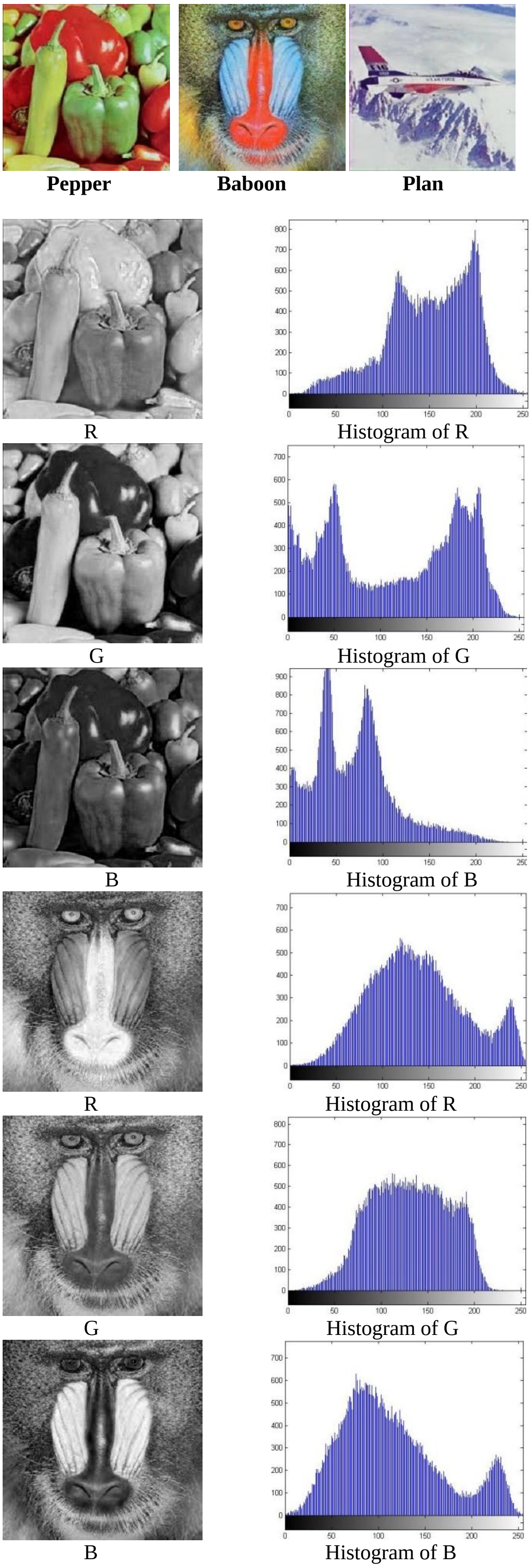


R Histogram of R

G Histogram of G

B Histogram of B

Figure 6: Cipher image histogram of R, G and B based on a proposed algorithm.



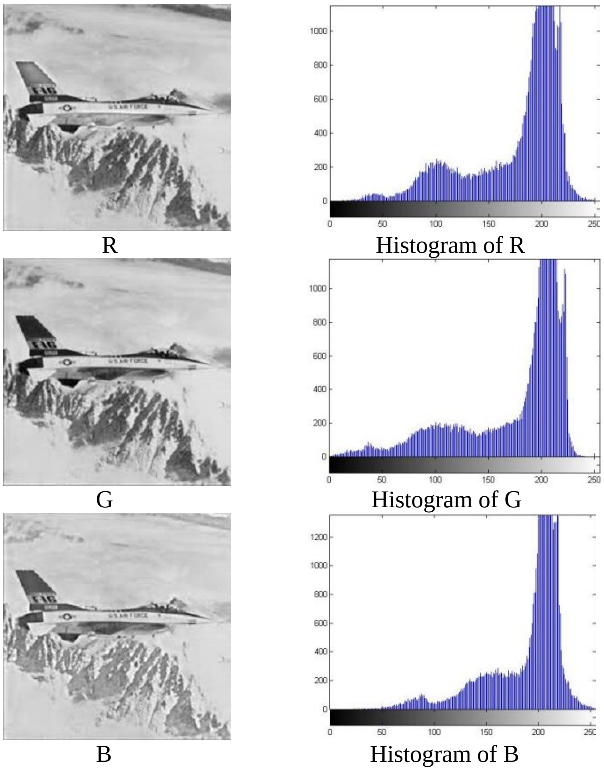
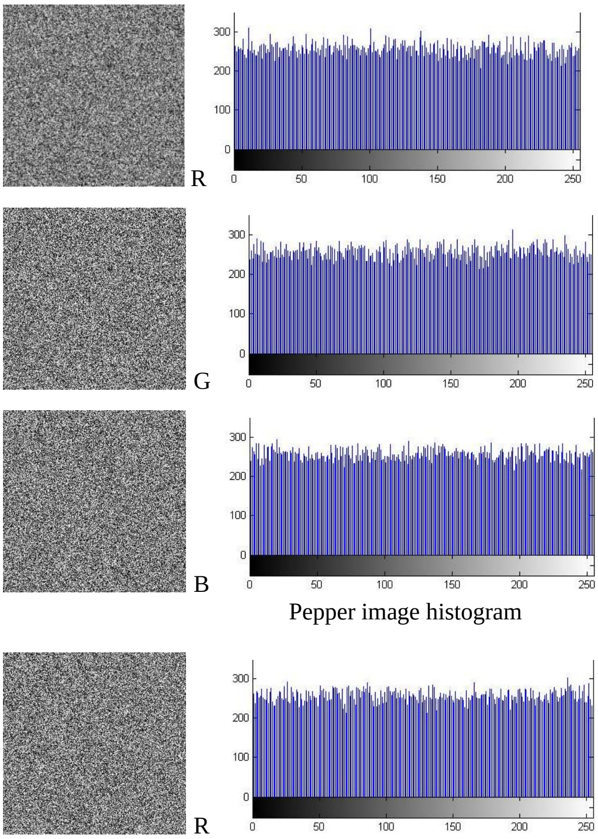
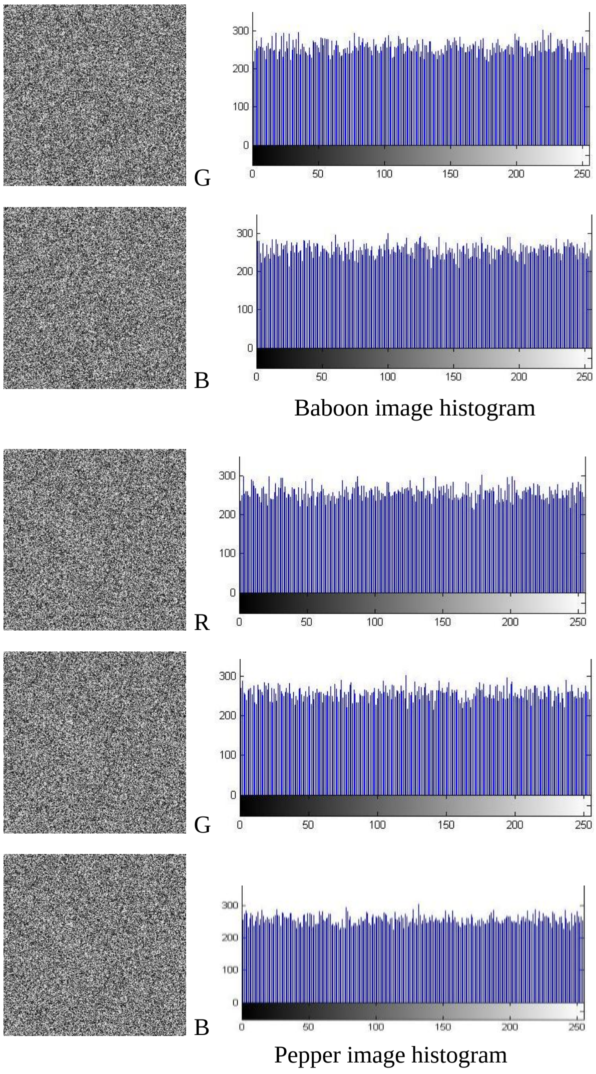


Figure 7: Histogram of sample color images (Pepper, Baboon and Plan)



Pepper image histogram



Baboon image histogram

Pepper image histogram

Figure 8: Histogram of sample color images (Pepper, Baboon and Plan) for three channels R, G and B respectively based on proposed algorithm

5.2 Correlation Coefficients

In this section, the correlation coefficients between the plain image and cipher image can be illustrated as shown in table (1). The following equation gives us the correlation value for every channel of plain and cipher image [20]:

$$r = \frac{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(P(i,j)-\bar{P})(C(i,j)-\bar{C})}{\sqrt{\left(\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(P(i,j)-\bar{P})^2\right)\left(\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\bar{C})^2\right)}} \quad (1)$$

M: width of image N: height of image, $\bar{P}$&$\bar{C}$ are the average of Plain and Cipher, P(i, j): pixel value at position (i, j) in plain image, C(i, j): pixel value at position (i, j) in cipher image.

Table 1: Correlation between plain and cipher image

Image	Average	R	G	B
Lena	0.0042	0.0066	0.0034	0.0027
Pepper	-0.0035	0.0001	-0.0109	0.0002
Baboon	0.0062	0.0086	0.0083	0.0018
Plan	-0.0080	-0.0094	-0.0066	-0.0079

The correlation between two adjacent pixels for each plain and cipher image is shown in table 2 and table (3). The range value of correlation coefficient (r) is between (-1, 1), when r value is equal to zero, means no correlation between two adjacent pixels. On the other hand, when r value is equal to 1; this means positive perfect correlation, but when r=-1; this refers to a negative perfect correlation. In this paper, r values are closed to zero, it refers to the efficiency of image encryption algorithm. Correlation coefficients can be computed using equation (2).

$$r = \frac{\frac{1}{N}\sum_{i=1}^{N}(P_i-\bar{P})(C_i-\bar{C})}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}(P_i-\bar{P})^2\frac{1}{N}\sum_{i=1}^{N}(C_i-\bar{C})^2}} \qquad (2)$$

where $\bar{P}$ & $\bar{C}$ are the average of image and it after one pixel change for plain or cipher image which that mean grey level values of two adjacent pixels in the input image, that can be performed on horizontal, vertical, and diagonal.

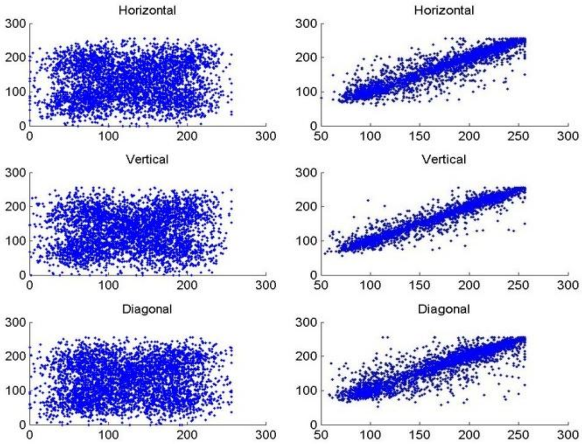
Table 2: Correlation Coefficients of two adjacent pixels for plain image

Image		R	G	B
Lena	Horizontal	0.9401	0.9427	0.8899
	Vertical	0.9681	0.9700	0.9396
	Diagonal	0.9163	0.9208	0.8515
Pepper	Horizontal	0.9663	0.9818	0.9625
	Vertical	0.9718	0.9861	0.9688
	Diagonal	0.9381	0.9672	0.9320
Baboon	Horizontal	0.9462	0.9146	0.9488
	Vertical	0.9383	0.9039	0.9447
	Diagonal	0.9096	0.8574	0.9157
Plan	Horizontal	0.9491	0.9591	0.9256
	Vertical	0.9459	0.9555	0.9195
	Diagonal	0.9011	0.9198	0.8565

Table 3: Correlation Coefficients of two adjacent pixels for cipher image

Image		R	G	B
Lena	Horizontal	0.0636	0.0750	0.0591
	Vertical	0.0548	0.0683	0.0508
	Diagonal	0.0530	0.0564	0.0480
Pepper	Horizontal	0.0553	0.0690	0.0494
	Vertical	0.0522	0.0708	0.0480
	Diagonal	0.0510	0.0554	0.0514
Baboon	Horizontal	0.0181	0.0245	0.0098
	Vertical	0.0236	0.0298	0.0167
	Diagonal	0.0267	0.0283	0.0239
Plan	Horizontal	0.0017	0.0061	0.0030
	Vertical	-0.0071	-0.0030	-0.0063
	Diagonal	0.0046	0.0063	0.0057

Randomly 2000 pixels are selected from plain and cipher image (Lena) to see the correlation coefficient for each one horizontal, vertical and diagonal as figure 9.



(a) (b)

Figure 9: Correlation coefficient between pixel pairs for proposed encrypted image (a) and origin image (b)

5.3 Differential Attack

Usually, the attacker will try to make slight change on cipher image to discover key encryption. A good encryption algorithm can be able to withstand differential attack. Therefore, we need to measure the impact on pixel change by using two wide analyses; they are the number of changing pixel rate (NPCR) and unified averaged changed intensity (UACI) [2]. They are defined as equations (3, 4):

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M\times N} \times 100\% \qquad (3)$$

$$\mathrm{UACI} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|C_1(i,j)-C_2(i,j)|}{255}}{M\times N} \times 100\% \quad (4)$$

$D(i,j)=0$ if $C_1(i,j) = C_2(i,j)$ otherwise $D(i,j)=1$ where $C_1(i,j)$ & $C_2(i,j)$ are the pixel values in position (i,j) of the respective cipher images encrypted from the plain image.

Different images are tested here where each image is encrypted twice; the first one is an original image which is encrypted by the proposed algorithm, the second is the cipher of original image after changing randomly one pixel value for instance; pixel value of Lena image at the position (27, 54, 3) is changed from 87 to 34, pixel value of Pepper image at the position (43,94,2) from 36 to 165, pixel value of Baboon image at the position (182,81,3) from 76 to 200, pixel value of Plan image at the position (226,137,1) from 154 to 0. NPCR and UACI scores for sample images are computed for three components (R-G-B) of color images as table 4 and table 5.

Table 4: NPCR values for encrypted image with encrypted image after one pixel changed

Image	Average	R	G	B
Lena	99.3922	99.321	99.4415	99.4141
Pepper	99.3805	99.3561	99.3896	99.3958
Baboon	99.4344	99.4293	99.4446	99.4293
Plan	99.5041	99.5422	99.5239	99.4461

Table 5: UACI values for encrypted image with encrypted image after one pixel changed

Image	Average	R	G	B
Lena	24.4334	24.1749	24.8729	24.2524
Pepper	24.1609	24.0026	24.6989	23.7811
Baboon	27.3418	27.1718	27.7478	27.1059
Plan	31.6307	31.6262	31.8068	31.4591

The optimum value for NPCR is 100% although this value cannot be reached even if two independent random values used. In this paper all NPCR values are near to optimum vales. On the other hand vales of UACI are different from one image to another depending on the density of colors.

5.4 Mean Square Error (MSE) and Peak to Noise Ratio (PSNR)

The different rate values of plain image and cipher image can be computed by mean square error MSE measure while the PSNR gives us the disarrangement ratio of cipher image from plain image see table 6 and table 7. The two measures MSE and PSNR are defined by equations (5) and (6) respectively [21].

$$\mathrm{MSE} = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[f(i,j) - \hat{f}(i,j)\right]^2 \quad (5)$$

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{{\max_f}^2}{\mathrm{MSE}}\right] \qquad (6)$$

Where: $f(i,j)$ is the source image $\hat{f}(i,j)$is the reconstructed image, and M, N is the two dimensions of image $\max_f$ is maximum possible value of an image f.

Table 6: mean square error for sample of images

Image	Average	R	G	B
Lena	0.1013	0.1264	0.1030	0.0744
Pepper	0.1171	0.0869	0.1341	0.1303
Baboon	0.0987	0.1016	0.0869	0.1075
Plan	0.1521	0.1457	0.1536	0.1569

Table 7: Peak signal to noise ratio for sample of images

Image	Average	R	G	B
Lena	10.0454	8.9814	9.8727	11.2821
Pepper	9.3950	10.6083	8.7263	8.8504
Baboon	10.0754	9.9316	10.6086	9.6860
Plan	8.1809	8.3641	8.1358	8.0429

5.5 Entropy of Information

One of an important goal for image encryption is the ambiguity, entropy formula as equation (7) is used to clarify the probability of occurrence to all pixel values for image and encrypted image. The optimum case will exist when the probability of each pixel value is same [2]. Table 8 illuminates the entropy values for sample images before and after encryption.

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i)\log_2[P(m_i)] \qquad (7)$$

Where: $P(m_i)$ is the probability of m_i , H(m)=8 is optimum entropy for image (m_i) consists of 256 values when there are equal probabilities for each value.

Table 8: Entropy for images before and after encryption

Image	Entropy of image	Entropy of cipher image
Lena	7.7697	7.7597
Baboon	7.7842	7.7928
Pepper	7.6433	7.9002
Plan	6.8009	7.9702

6. PERFORMANCE ANALYSIS

Proposed encryption algorithm satisfied good execution time for coding and image key generation, so a good running time for decoding using the same key. Results of testing four samples of images are illustrated in table 9.

Table 9: Elapsed time for encryption and decryption image

Image	Encryption	Decryption
Lena	0.137826	0.110376
Baboon	0.133219	0.106537
Pepper	0.133801	0.102553
Plan	0.131697	0.105351
Average	0.134136	0.106204

7. CONCLUSIONS AND FUTURE WORK

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.

8. REFERENCES

[1]. Changgui Shi, Sheng-Yih Wang, Bharat K. Bhargava 1999: "MPEG Video Encryption in Real-time Using Secret Key Cryptography". PDPTA: pp2822-2828.

[2]. 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.

[3]. 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.

[4]. 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

[5]. 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.

[6]. 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.

[7]. 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.

[8]. 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.

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

[10]. Seyedzade S. M., Atani R. E., and Mirzakuchaki S. 2010 "A Novel Image Encryption Algorithm Based on Hash Function", In 6th Iranian Conference on Machine Vision and Image Processing IEEE.

[11]. Min L. and Lu H. 2010 "Design and analysis of a novel chaotic image encryption", 2nd International Conference on Computer Modelling and Simulation, Publication IEEE, pp517-520.

[12]. Pall A. K., Biswas G. P. and Mukhopadhyay S. 2010 "Designing of High-Speed Image Cryptosystem Using VQ Generated Codebook and Index Table", International Conference on Recent Trends in Information, Telecommunication and Computing IEEE, pp39-43.

[13]. Pang C. 2009 "An Image Encryption Algorithm Based on Discrete Wavelet Transform and Two Dimension Cat Mapping", Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing IEEE, Vol. 2, pp711-714.

[14]. Acharya B., Patra S. K., and Panda G. 2008 "Image Encryption by Novel Cryptosystem Using Matrix Transformation", 1st International Conference on Emerging Trends in Engineering and Technology IEEE, pp77-81.

[15]. Al-Khassaweneh M. and Aviyent S. 2008 "Image Encryption Scheme Based on Using Least Square Approximation Techniques", International Conference Electro Information Technology IEEE, pp108-111.

[16]. Gupta M. et al. 2012 "A New Approach for Information Security using Asymmetric Encryption and Watermarking Technique" International Journal of Computer Applications (IJCA) Vol.57 No.14.

[17]. Francia A., Yang M. and Trifas M. 2009 "Applied image processing to multimedia information security", Int.

Conf. Image Analysis and Signal Processing IEEE, pp286 - 291

[18]. Mursi M. et al. 2014 "Combination of Hybrid Chaotic Encryption and LDPC for Secure Transmission of Images over Wireless Networks", International Journal of Image, Graphics and Signal Processing, pp8-16.

[19]. Toufik, B. and Mokhtar N. 2012 "The Wavelet Transform for Image Processing Applications. In: Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology", Chapter 17, InTech, USA, pp395-422.

[20]. Sivakumar T. and Venkatesan R. 2014 "A Novel Approach for Image Encryption Using Dynamic Scan Pattern" International Journal of Computer Science IAENG, Vol. 41, No. 2, pp91-101.

[21]. Thakur N, Devi S. 2011 "A new method for color image quality assessment" International Journal Computer Application. Vol. 15, No.2, pp10–17.