International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Color Image Encryption and Decryption Based Pixel Shuffling with 3D Blowfish Algorithm

Asia Mahdi Naser Alzubaidi[1], Noor Dhia Kadhm Al-Shakarchy[2]

[1]Computer Science Department, College of Science, Karbala University, Karbala, Iraq

[2]Computer Science Department, College of Science, Karbala University, Karbala, Iraq

Abstract: ***In recent years, With the wide development in communications networks and applied the e-government in most field depending on the internet and its technologies, with the development in the hackers ability to intruder the communication channels. Consequently, cryptographic techniques are required to accomplish a sufficient level of security, integrity, confidentiality as well as, to prevent unauthorized users from accessing of important information during storage, recovery and transmission of data. To meet this challenges, a novel and efficient color image encryption method depending on the diffusion and confusion mechanesim presented in this papper. a permutation manner existing by 2D Arnold cat map transform with row_column wise methods to make more distortion of the relationship among connected pixels of original image by hide the statistical structure of pixels. Moreover, the proposed method applied a blowfish algorithm on image to presented confusion and diffusion on it with 3D logistic mapping in order to diffuse the relation between plain and encrypted images by changing the gray value of original image pixels. The strongest of Encryption algorithm is evaluated dependent on the relation between the plain and cipher image must be contradicting by hiding the natural feature of image. Also, the algorithm in this study has been tested on some images and showed good results. These results evaluated using security and statistical analysis such as Entropy function, NPCR and UACI Factors with the degree of randomness.***

Keywords: 3D Blowfish Algorithm; 2D Arnold cat map; Image encryption Techniques; 3D Logistic Map; Row-Column Wise method**.**

1. Introduction

The widest multimedia used in communication is digital image. Digital images are used in many important fields such as military plan, medical reports, and financial treatment and so on. The protection of these images becomes very pressing using many ways such as cryptography. During the past years, many algorithms used to encrypt the image which is suitable with the properties and features of digital images. These algorithms depend on scrambling the pixels using one algorithm such as Arnold Cat Map to provide the confusion concept then used another algorithm to provide the diffusion by modify the image colored value.The famous encryption algorithms such as RSA, DES, AES etc designed to provide the diffusion and confusion in same algorithm and same step[2]. In the other hand, these algorithms have a good security and strongest. Different techniques are used with its suitable data to deal with own data features. Most encryption algorithms mainly used for text data but may not be suitable for multimedia data such as digital image. To employ these points, the proposed system presented a digital image encryption algorithm depending on a blowfish algorithm. After many pre-processes is working on the digital image to become suitable with blowfish algorithm. Actually,Blowfish is a block cipher symmetric encryption algorithm, that's mean it uses the same secret key to both encrypt and decrypt process and dealing with fixed length blocks. We can summarized the main features of Blowfish algorithm by[3]:

- The block size encrypted and decrypted in Blowfish is 64 bits
- The range of key size used is 32 bits to 488 bits.
- Blowfish is published algorithm and don't want any permit or authorized to use or working on it, its free algorithm.

2. Aim of Research

In this research we present an encryption algorithm which used for text data in digital image encryption after some taming to become suitable with digital image. Blow fish algorithm provides good randomness, confusion and diffusion concepts evolving in encryption and decryption process. as well as the decryption process to reduce the original image in recipient side has a high accuracy and prevent the lossless of image information. In addition to encryption aims. Such as the **privacy** which cannot anyone except the exact receiver reads the image, **data integrity** which guarantee that no change and manipulation in image data during image transmission, **Authentication** which provides the Verification of the person that you want to read the sent image and finally Non repudiation which makes the person whose image message sent to him Unable to denial that he's the right person the image message sent to him.
The main system functionalities are:

- Read color image.
- Represent and display the information of color image as text.
- Encrypt the color image using blowfish algorithm and produced cipher image.
- Save cipher image in file.
- Display the cipher image from file saved.
- Decrypt the image from encrypted file saved
- Save the plain image (output of decryption process) in another file.
- Display plain image. Figure (1) depicts the Encryption and Decryption architecture via network.

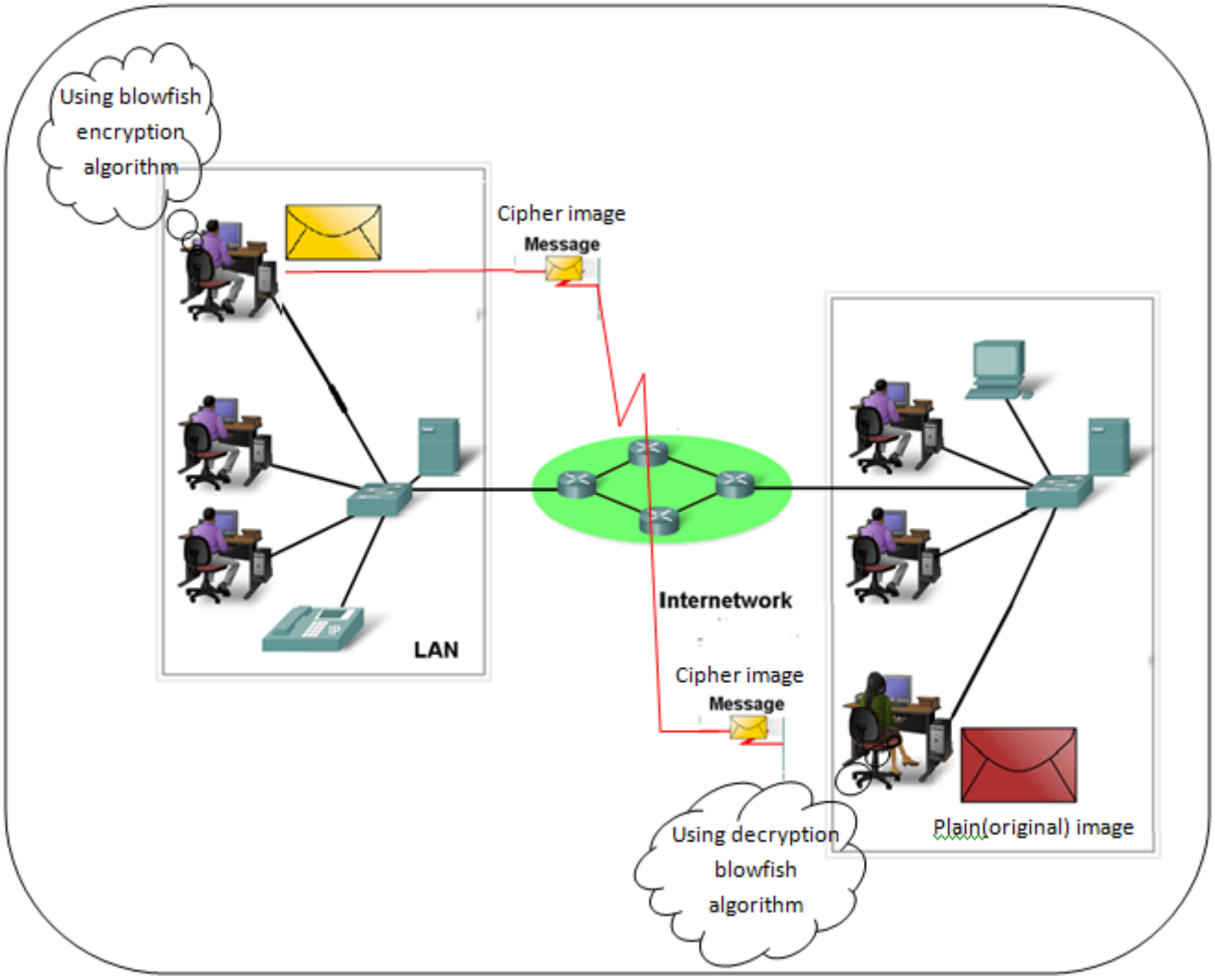


Figure 1: Encryption and Decryption system architecture using Blowfish algorithm

3. Literature Survey

When we illustrate the studies and application these are related to the proposed system, we illustrate very much papers and researches. Some depending on the cryptography algorithms used with data and modified to be able deal with digital image such as Ch. Samson and Dr. V. U. K. Sastry in 2012 presented Advance Hill cipher system to encrypted and decrypted digital image [1,4]. Others depending on the algorithms these deal with feature of images to change the image color value such as Chaos algorithm based on diffusion concept [5]. While in [6] blowfish algorithm used because of variable and longest key size to enhance the security level of the encrypted images by reducing the relationship between image pixels and to increase information entropy of it. Actually, blowfish algorithm takes large space of researches to be security and confidence. The proposed system employ the blow fish algorithm to encrypted digital image after many pre-process steps ;scrambling one of these steps; done to be become suitable with digital image. The proposed cipher system gives a good results as shown in encrypted image and return the origin image by decryption algorithm without losing the feature of image and it's resolution. These methods evaluated and analysis using Entropy function to evaluate the quantity of information in encrypted image and Autocorrelation function to evaluated the similarity between the encrypted and decrypted image.

4. Materials and Methods

The proposed system in this paper employed the Blowfish algorithm with 3D logistic function to encrypt digital image depending on some pre and post processes materials. This algorithms already used with text data, in this project we represent the plain image with matrix of dimension (256*256*3) where 256 represents both rows and column values of image and make some transformation in digital image to be suitable with blowfish algorithm and to increase the randomness of original image pixels by using Arnold Cat Map with row-column wise methods. Then, converts this information to text data and finally, converts them to binary sequence. These steps are implemented firstly as preprocess to original image. The second step is the implementation of blowfish scheme after dividing the binary sequence which represents the image to blocks of size with 64 bits. Each block inters to blowfish algorithm as plaintext. The output of this algorithm is representing the cipher text. Then we perform X_OR operation with the key sequences that generated by using 3D logistic mapping. The final step of encryption process of proposed system is the post-process to cipher text and obtained the cipher image. The binary data of

cipher text converted to ciphered text data which represent the information of encrypted image. Then this text converted to pixels which represent the cipher image. Finally the encrypted image sends through the network. These three steps illustrate the Encryption process and done in sender side. In other side, receiver side these steps (encryption steps) done with decryption algorithm.

Figure (2) shows block diagram of suggested method.

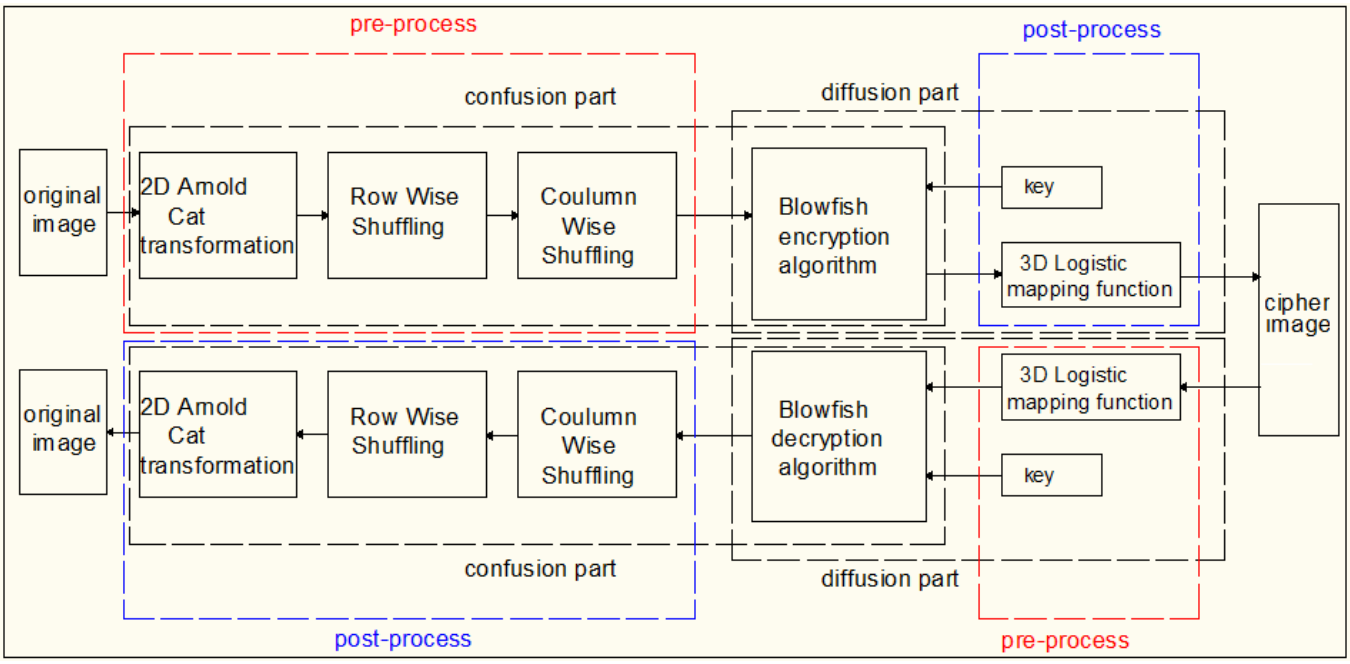


Figure2: Block diagram Image Encryption and decryption System

4.1 Arnold Cat Map System

Arnold's Cat Map transformation use for shuffling the pixels of color image and to perform extra security of cipher system. The 2D Arnolds cat transform does not alter the gray scale value of the image pixels but it only scramble the image data as shown in equation(1) for image encryption and equation(2) for image decryption.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix} * \begin{bmatrix} X \\ Y \end{bmatrix} \bmod 256 \quad ...(1)$$

$$\begin{bmatrix} X \\ Y \end{bmatrix}' = \begin{bmatrix} 1 & p \\ q & p*q+1 \end{bmatrix}^{-1} * \begin{bmatrix} X' \\ Y' \end{bmatrix} \bmod 256 \quad ...(2)$$

Where:
p,q: represents the positive secret keys.
X,Y : original position of the image pixel before scrambling.
X',Y': new position of the image pixel after scrambling [7].

After applying 2D Arnold cat transformation for several iterations, the relationship between the neighboring pixels is entirely destroy and the original image seems deformation and meaningless Actually, for iterating it to many times it will return to original look. this mean that Arnold cat map is a periodic transform. After image shuffling the statistical features are same for encrypt image and original image to increase the security of encryption system [8].

4.2 Row- Column Wise Scrambling

Actually, the main aim of image shuffling is to decrease the relationship of adjacent pixels location and gray values until they are unrelated for each other. Although the image is scrambled, the pixels of it will remain have same gray values. Therefore, by use information entropy and graphical shape of encrypted image histogram, cryptanalysis can perform statistical and structural attacks which lead to make the system vulnerable. The row wise shuffled image is the movement of a row set to the summation of values on that row and can performs by using equation(3).

$$I'(X, Y) = I((X + R(X)) \bmod 256, Y)$$
$$R(X) = \sum_{Y=0}^{256} I(X, Y) \quad ...(3)$$

Where:
I(X,Y): the original image coordinate.
I'(X,Y): row wise shuffled image coordinate.
R(X) : summation of all elements in x row of I image.
While, column wise shuffled image is the displacement of a column set to the summation of elements in that column as shown in equation(4).

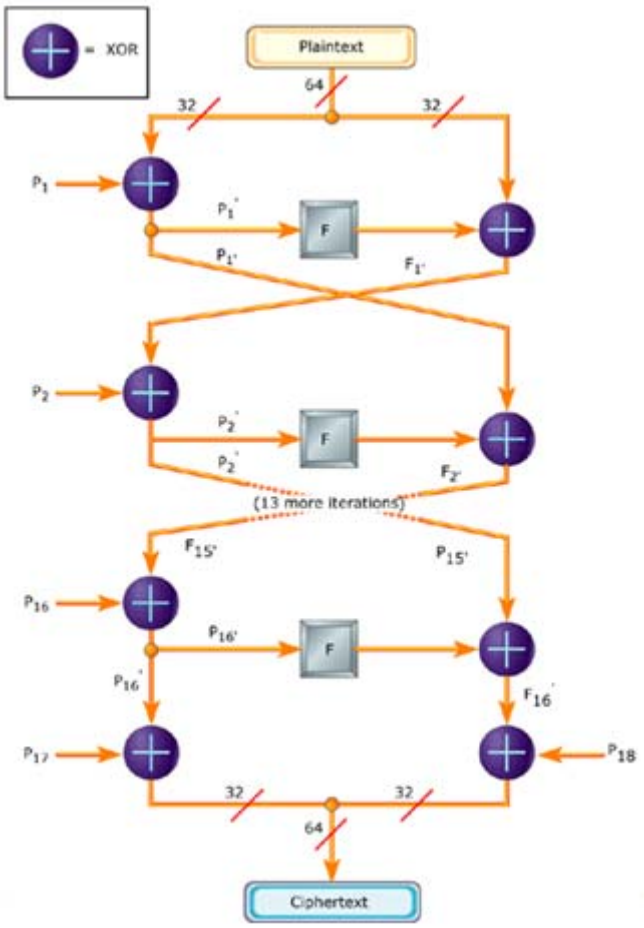
$$I'(X, Y) = I(X, (Y + C(Y)) \bmod 256)$$
$$C(Y) = \sum_{X=0}^{256} I(X, Y) \quad ...(4)$$

Where C(y) is the summation of all values in the Y column [9].

4.3 Blowfish Algorithm

Blowfish algorithm is a cipher algorithm deals with blocks of bits with symmetric key. The block size encrypted and decrypted is 64 bits. The performance of this algorithm divided to two sub-algorithms works synchronously. First

algorithm deals with data to encryption from during 16 round. The bits pass in permutation step dependent on key and substitution step dependent on together data and key. The second algorithm deals with the key which process the key to expansion and generate sub-keys whose used in rounds of encryption. Figure (3) illustrates the Blowfish encryption algorithm steps [10].



While Figure (4) illustrate the Blowfish F-function Steps to generate sub-keys which computed and initialized from key algorithm of Blowfish. These sub- keys classified to two kinds each one consisting of many arrays these are:

- The P-array: consists of 18 sub-arrays (sub-key) [P1, P2... P18]. The length of each array is 32-bits.
- S-boxes: consists of 4 S-boxes [S1, S2, S3, S4]. Each S-box has 256 entries. Such that:

S1,0, S1,1,..., S1,255;
S2,0, S2,1,..,, S2,255;
S3,0, S3,1,..., S3,255;
S4,0, S4,1,…, S4,255.

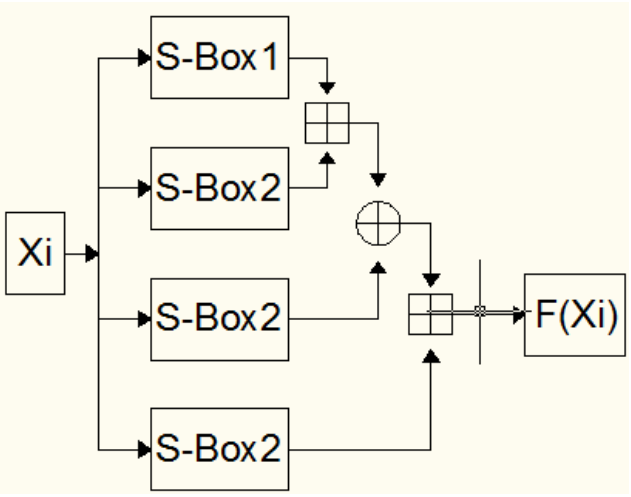


Figure4: Block diagram of Blowfish F function

Blowfish encryption algorithm consists from following steps:
Step1: Read color image (bmp 256 color image), and apply pixels shuffling by using Arnold Map and Row_column wise methods to provide a permutation of image pixels.
Step2: Convert scrambling image into file and open it as text.
Step3: Converting image text data to binary by ASCII code.
Step4: input the key must be less than 448
Step5: extract 64 bit block orderly from binary sequence
Step6: apply Blowfish encryption to this extracting block
Step7: gathering the obtained cipher block in cipher text
Step8: if the original binary sequence not finished (there other blocks) go to step 5 to extract other block.
Step9: converting all cipher text binary sequence to cipher text data by using ASCII code.
Step10: convert cipher text data to image by saving it in file.
Step11: open the file as image and display encrypted image [11].

In other hand, the same algorithm used in decryption part and the same encryption key used to decrypt image but reverse sub-keys and without any pre-process to an encrypted image. Finally the post-process is done to return the original image. The encrypted image is divided into the same block length of Blowfish algorithm from top to bottom. Each block is entered to the decryption function with same key but the application of sub keys is reversed to decrypt the image. The process of decryption is continued with other blocks of the image from top to bottom. After all blocks completed, the plaintext obtained represent the information of image in binary. This binary sequence converted to text then saved as mage. The output is scrambling image. Therefore the decryption process wanted post-process to return the original image [12].

4.4 3D Logistic Function

In this paper, 3D logistic map have been suggested for diffusion technique to increase the security of encryption method. The 3D Logistic map described in equation (5).

$$X_{i+1} = \lambda X_i(1-X_i) + \beta Y_i^2 X_i + \alpha Z_i^3$$
$$Y_{i+1} = \lambda Y_i(1-Y_i) + \beta Z_i^2 Y_i + \alpha X_i^3$$
$$Z_{i+1} = \lambda Z_i(1-Z_i) + \beta X_i^2 Z_i + \alpha Y_i^3 \quad ...(5)$$

Three quadratic coupling constant factors are presented to strengthen the difficulty and security of 3D Logistic map and system provide chaotic behavior when $3.53<\lambda<3.81$, $0<\beta<0.022$, $0<\alpha<0.015$. So for encryption system we first generate keys sequence by using 3D logistic map that needs three secret factors λ,β,α such λ =3.8414991, β=0.022 and α =0.015 with initial value of x0 = 0.976, y0 = 0.677 and z0 = 0.973 represented as a secret keys to generate the next keys of Xi, Yi and Zi using the previous equation[7].

5. Experimental Analysis and Results

The strongest of any cipher system measured corresponding to the hardest breaking and cryptanalysis. The main concepts used in proposed system are the diffusion and confusion [13]. The diffusion provides the propagation manner to the plain space so that the cipher space becomes smoother. The combinations of the items in the Blowfish cipher system in F-function gives excellent spate to the relation between original space and cipher space. The concept of confusion provides permutation state to the original space. This permutation done by scrambling or shuffling the location of original image without any changed in the values of the colored pixels. Therefore the contacts between a cryptogram and the corresponding key are complex. Figure (5) shows the experimental work of the proposed system.

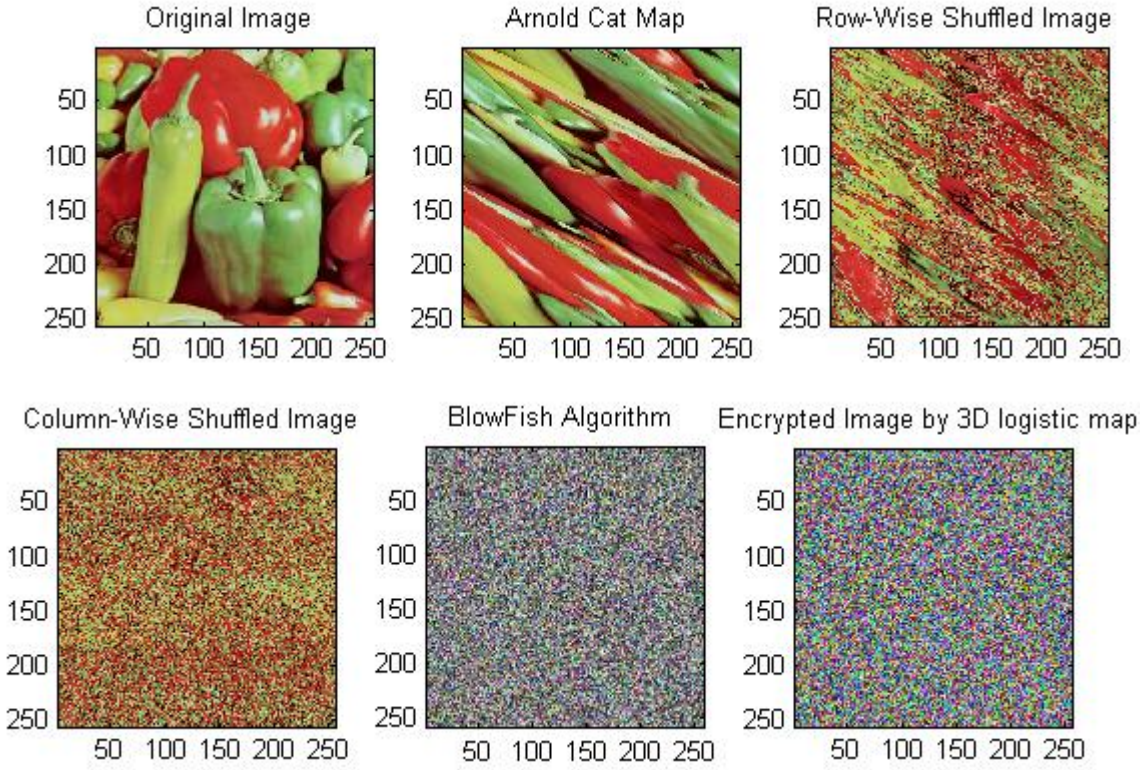


Figure 5: Experimental results of proposed encryption system

5.1 Histogram Analysis

The histogram provides the comparison between the original image and cipher image. The histogram of the cipher image must be uniform and the cryptanalysis can't interpret any information about it. Figure (6) depicts the histograms of Red, Green and Blue components of original and encrypted images. From all figures, it is obviously that there is a perceptual difference in graphical representation of all color's channels histogram and fairly uniform distribution of frequencies values among the plain image and it encrypted image pixels. Therefore histogram criteria can't give any clue to statistical cryptanalysis for breaking the encryption scheme so it is a good method for hide any countenance of the original image [14].

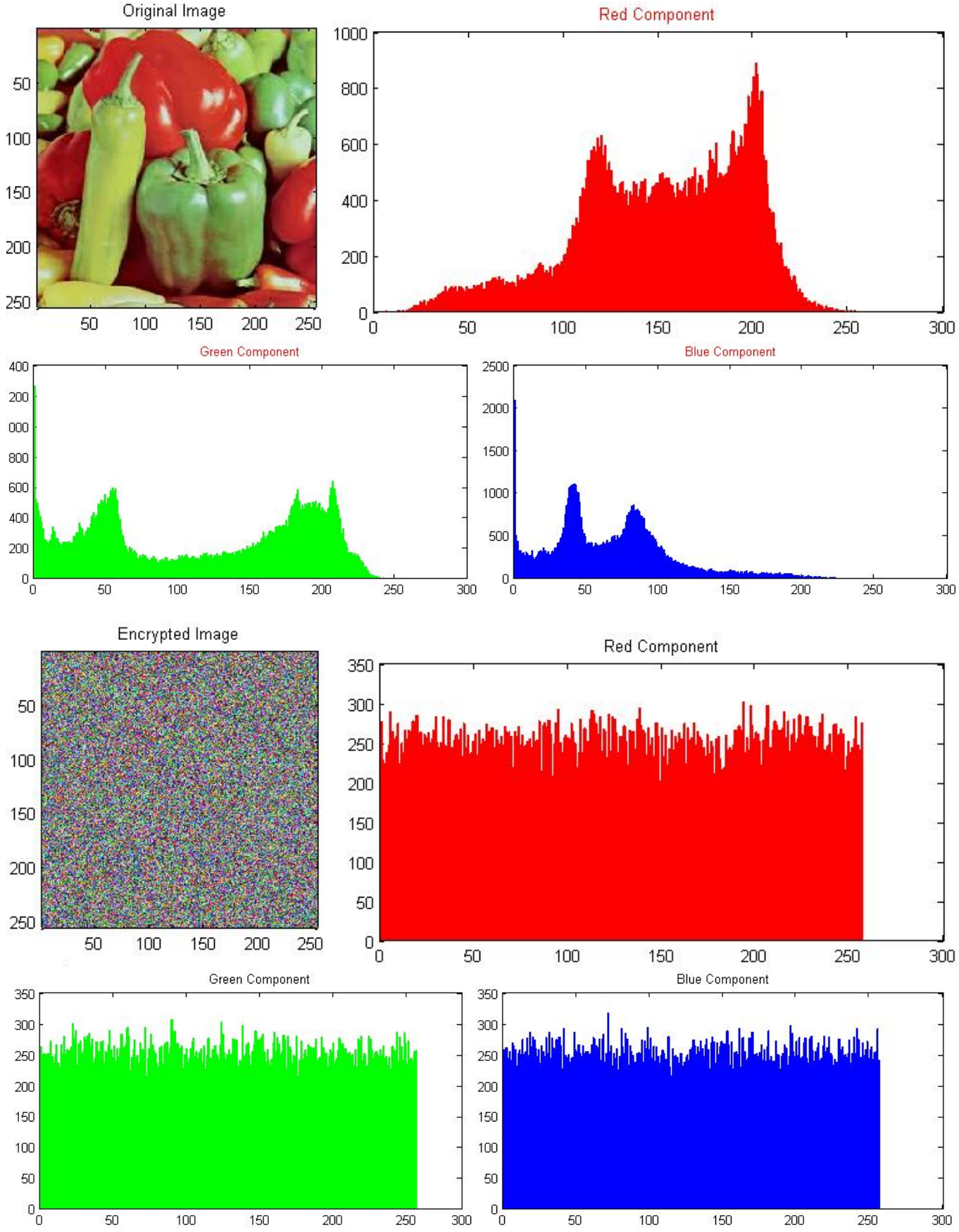


Figure 4: Plain &cipher image with histogram for color components

5.2 Information Entropy

It is well known, information entropy is a concept of measuring the degree of randomness in the encryption system. Actually, for any image encryption scheme it should decreases the connect information among encrypted Image pixels and this mean rises the entropy value also, It must fulfil a rule that the information entropy value for encrypted image should not offer any clue about the plain image [15]. Image entropy is computed by equation(6).

$$\text{entropy} = \sum_{i=1}^{256} P(i) * \log \frac{1}{P(i)} \quad ...(6)$$

Where P(i) is the probability of existence of pixel i.

Truly, the ideal entropy value of random system is equal to 8. In general, if calculated entropy value is very close to ideal value this mean that the cipher system is protect upon the entropy attack [15].

5.3 NPCR and UACI Factors

There are two criteria to assess the differences among the original image and the encrypted image, the Number of Pixels Change Rate (NPCR) and the Average Changing Intensity (UACI). Equation (7) gives the mathematical formula of the NPCR measure.

$$NPCR = \frac{\sum_{i=1}^{256}\sum_{j=1}^{256} Dif(i,j)}{65536} * 100\%$$

$$\text{Dif} = \begin{cases} 1 & \text{I(i, j)} \sim= \text{I'(i, j)} \\ 0 & \text{I(i, j)} = \text{I'(i, j)} \end{cases} \quad ...(7)$$

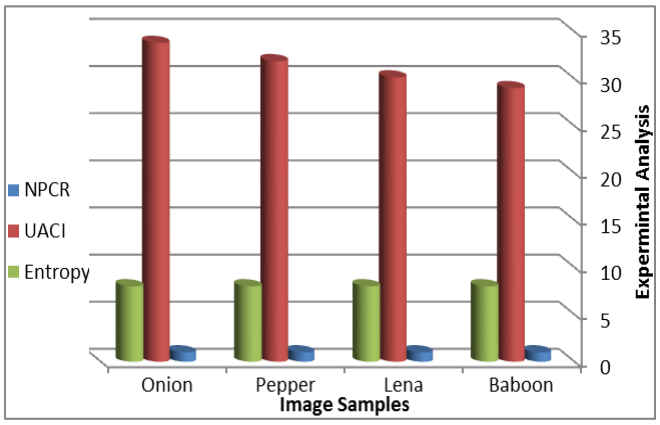
Where:
I(i,j) represent the original image
I'(i,j) represent the encrypted image. NPCR value indicates the different average of the number of pixels of the encrypted image when only one pixel of the plain image is adapted. It is obviously that NPCR value should be as big as possible to reach the performance of an ideal digital image encryption scheme. Equation (8) shows the mathematical expression of the UACI measure.

$$UACI = \frac{1}{65536}\left[\sum_{i=1}^{256}\sum_{j=1}^{256}\frac{|I(i,j) - I'(i,j)|}{256}\right] * 100\% \quad ...(8)$$

UACI measures the intensity rate of differences between the original image and ciphered image.

Tables 1: NPCR & UACI for encryption images

Images	NPCR	UACI	Entropy
Baboon	0.9960	29.0201	7.9991
Lena	0.9958	30.1578	7.9991
Pepper	0.9961	31.8751	7.9991
Onion	0.9961	33.8115	7.9991



In general, the NPCR and UACI of the suggested scheme being all close to unity and a good obvious that the encryption image scheme have a highly confidential security [16].

6. Conclusion

The suggestion system presented one text encryption algorithm (Blowfish algorithm) with digital color image. Blowfish is an encryption algorithm that its strongest against broken. The main points we can determined in this research:

- Proposed system provided high security to image data from illegal steals.
- The proposed algorithm has fast performance to encrypt and decrypt the image.
- Despite the relative complexity of the algorithm, but the decryption process does not occur any loss or modify of image data.
- Its provide diffusion manner by scrambling the blocks of images in addition to the diffusion presented inside the construction of Blowfish algorithm which increase the randomness and permutation to the cipher image.

7. Future Work

Proposed system provides diffusion and confusion concepts which presented good security. Therefore the working and developing on it is very visible. We can suggest some future works:

- Random key generation: which make the system able to generate efficient random key (the key has good randomness) without selected it.
- Hashing: The proposed system ought to be proficient in being changed to a one-way hash function.

Acknowledgment

We would like to thank anonymous referees for their constructive comments.

References

[1] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[2] B. Acharya, S. K. Panigrahy, S. K. Patra, and G. Panda, " Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, India, 2009.
[3] I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, pp.38, 2004.
[4] Ch. Samson and Dr. V. U. K. Sastry, " Cryptography Of A Gray Level Image And A Color Image Using Modern Advanced Hill Cipher Including A Pair Of Involuntary Matrices as Multiplicand And Involving A Set Of Functions", Hyderabad, India, 2012.
[5] I. A. Ismail1, M. Amin, and H. Diab, "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps", International Journal of Network Security, July 2010.
[6] D.M.Torgalkar, N.B.Sambre," Blowfish Encryption Using Key Secured Block Based Transformation", International Journal Of Engineering Sciences & Research Technology, volume 3 Issue 3, p1774-p1780, March- 2014.
[7] P.N.Khade, M.Narnaware,"3D Chaotic Functions for Image Encryption", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, N`o 1 p323-p328, May 2012.
[8] Z. Lv, Lei Zhang, J.Guo,"Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System",ISBN 978-952-5726-07-7 (Print), 978-952-5726-08-4 (CDROM) Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangsha, P.R. China, 26-28, pp. 191-194,Dec. 2009.
[9] S. Rakesh, Ajitkumar A Kaller, B. C. Shadakshari, B. Annappa,Multilevel Image Encryption,cornell university library,fep-2012.
[10] Yarmolik, V. N.& S. N Demidenko, " Generation and Application of Pseudo Random Sequences for Random Testing " , John Wiley & Suns, 1988.
[11] Serberry, Jennifer and Joserf Pieprzyk, " Cryptography, An Introduction to Computer Security", Prentice Hall, 1989.
[12] Schneier, Bruce, "Applied Cryptography, Protocols, Algorithms, and Source Codes in C" , Second Edition, John Wiley & Sons, 1996.
[13] W. Stalling, "Cryptography and Network Security Principle and Practices, Fourth Edition", Prentice Hall, November 16, 2005.
[14] Beker, Henry and F. Piper, "Cipher Systems, The Protection of Communications", Northwood Books, London, 1982.
[15] S.K.Bandyopadhyay, D. Bhattacharyya, P. Das, S. Mukherjee, D. Ganguly, "A Secure Scheme for Image Transformation", IEEE SNPD, pp. 490-493, August 2008.
[16] A.B.Abugharsa,A.S.Basari,H.Almangush,"A New Image Scrambling Approach using Block-Based on Shifted Algorithm",Australian Journal of Basic and Applied Sciences, 7(7): 570-579, 2013.

Author Profile

Asia Mahdi is awarded her B. Sc, and M. Sc, at University of Babylon, College of Science, Department of Computer Science in 1997 and 2002 respectively. She is an lecturer at Karbala University, Collage of Science, Computer Department. Here research interests include: Computational Geometry and Object Modeling, Image processing such as Segmentation and Steganography , Speech signal processing, Computer Graphics and Data Security.

Noor is Awarded her B.Sc, and M.Sc, at University of Technology, Department of Computer Science and information systems-information systems in 2000 and 2003 respectively. She is a lecturer at Karbala University, Collage of Science, Computer Department. Here research interests include: Object Modeling, Image processing such as Segmentation and Steganography, Data Security, Artificial intelligent, artificial intelligent applications and information systems.