EUROPEAN ACADEMIC RESEARCH
Vol. IV, Issue 5/ August 2016

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Colored Image Ciphering with Key Image

ZAINALABIDEEN ABDULLASAMD RASHEED
Education College, Kufa University
Iraq

Abstract:

Security is one of the most important things in current era especially in sending information in unsecured channel, because of the danger of attack the information during passing channel, many methods suggested to overcome this problem like cryptography, steganography, passwords, biometrics, barcode,……… each one of them contain a wide range of precise correct algorithms like public key algorithms, substitution algorithms, polyalphabetic algorithms, DES algorithms, ……… in cryptography and so on in other methods. The proposed system cipher colored image by using information scrambling between bands of colored image firstly, then x-or with number which is seen random but it is related to position of the pixel and the band of the colored image after that the result number will be x-ored with special key that discovered from another image. The key will be constructing by scanning image from start to end line after line and considering the sequence of pixels appearance as a colored key instead of original color of the pixel.

Key words: Cryptography, symmetric, asymmetric, block cipher, stream cipher.

1. INTRODUCTION

Cryptography is the science and art of hiding information meaning while the unreadable information is seen for all parties, also Cryptography can be defined as a technique, in which secret messages are transferred from one person to another over the communication channel, in cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge (key). The result of the process is encrypted information. The reverse process is referred to as decryption. There are two main algorithmic approaches to encryption information, these are symmetric and asymmetric. Symmetric-key algorithms are a class of algorithms for cryptography that use the same keys for both encryption of plaintext and decryption of cipher text, while Asymmetric or Public key encryption on the other hand is an encryption method where a message encrypted with a public key and ciphertext decrypted by private key.

Ciphering algorithms can be classified with respect to the mode of operation of the algorithms into block and stream cipher. A block cipher is a type of symmetric key algorithm that transforms a fixed length of plaintext into the same length ciphertext, while stream cipher typically operates on smaller units of plain text, usually bits. Each ciphering system consists of two stages as illustrated in fig. (1)

1- Cipher stage by sender where original image transferred to cipher image by using secret key (k) with the proposed suitable cipher algorithm.

2- Decipher stage by recipient where cipher image transferred to original image by using the same secret key (k) with the suitable decipher algorithm which work in inverse fashion than cipher algorithm.

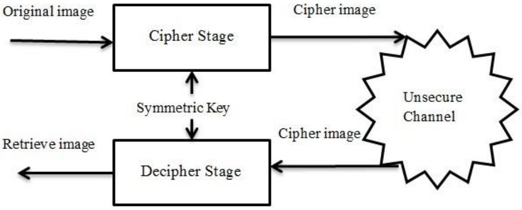


Fig. (1) Cipher symmetric system stages

Ciphering image is an important part of keeping information secure when the information is too big to hide in another media as in steganography.

2. PROPOSED SYSTEM

The proposed system as all cipher systems consist of two stages, the first one for cipher image and the as illustrated in fig. (2)

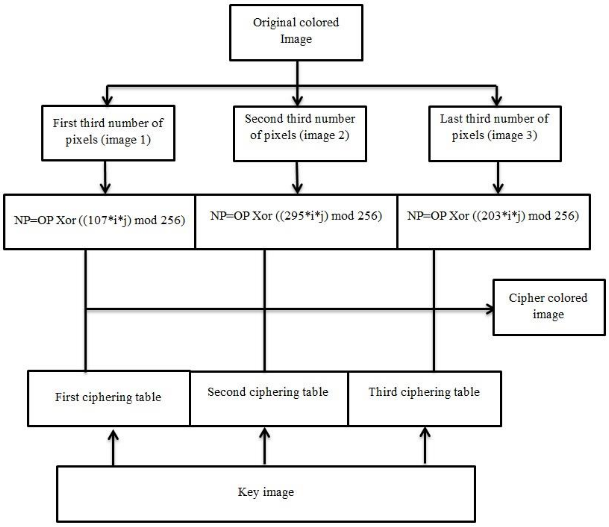

Original colored Image
First third number of pixels (image 1)
Second third number of pixels (image 2)
Last third number of pixels (image 3)
NP=OP Xor ((107*i*j) mod 256)
NP=OP Xor ((295*i*j) mod 256)
NP=OP Xor ((203*i*j) mod 256)
Cipher colored image
First ciphering table
Second ciphering table
Third ciphering table
Key image

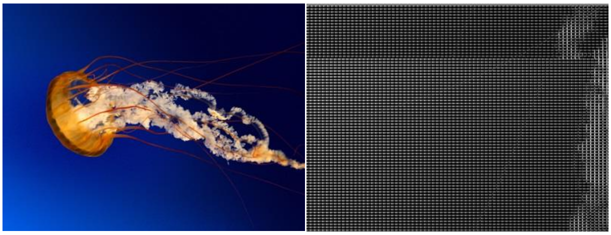
Fig. (2) Cipher stage of the proposed system

The second stage of the proposed system is for deciphering image consists of the same process in ciphering stage but in reverse sequence of the processes. To illustrate the proposed system each proses will be illustrated in details for each stage as follows:

a- cipher stage:- the input of this stage is original colored image and the output is cipher colored image, this stage done in sender position and consist of the following processes

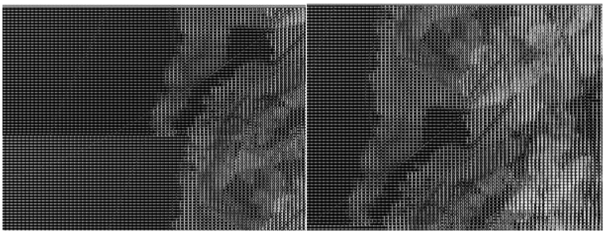
1- Split colored image into three images as illustrated in fig. (3) and (4) by dividing all pixels of all bands in data region (which start from byte 55 to end of image file in file RGB image format) into three separated successive gray scale images. in this processes each image of three was ciphered by re- arranged pixels within each image

Colored Image data											
Red	green	blue	red	green	blue	red	green	blue	red	green	blue
100	50	20	10	10	70	255	255	200	175	175	100
First image				Second image				Last image			



a-original colored image b-First Image

Fig. (3) Split colored image into three gray scale images



c- Second Image **d-Third Image**

Fig. (4) Split colored image into images

2- **Cipher pixels color in each image:** in this process each image from three images will be ciphered by changing the value of each pixel by applying the following equations for each one of the gray scale images

$\text{NPV} = \text{OPV Xor } ((107 \times \text{NPR} \times \text{NPC}) \text{ Mod } 256)$ …(1)

$\text{NPV} = \text{OPV Xor } ((295 \times \text{NPR} \times \text{NPC}) \text{ Mod } 256)$ …(2)

$\text{NPV} = \text{OPV Xor } ((203 \times \text{NPR} \times \text{NPC}) \text{ Mod } 256)$ …(3)

Where

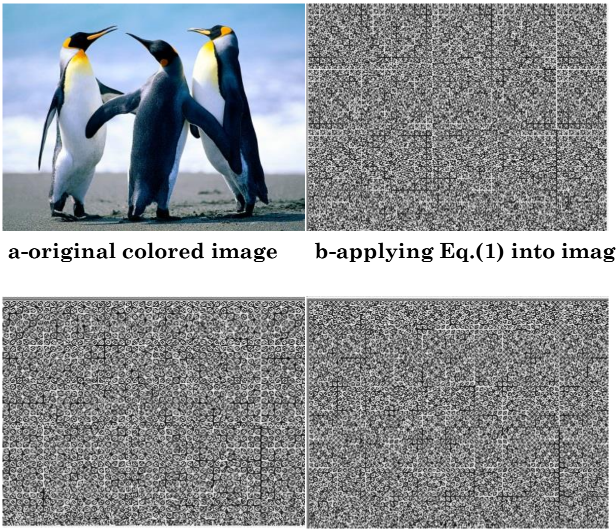
NPV is the new value of the pixel

OPV is the old value of the pixel

NPR is the number of the row of the pixel

NPC is the number of the column of the pixel

Each one of the previous equation will be applied to one image of the three gray scale images, this mean that equation (1) will be applied to first image, equation (2) will be applied to second image, and equation (3) will be applied to third image. The result of applying above equations will be illustrated in figure (5)

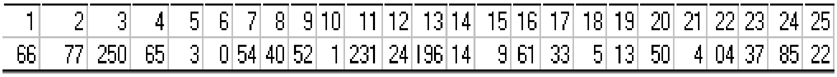


a-original colored image **b-applying Eq.(1) into image (1)**

b-applying Eq.(2) into image (2) **b-applying Eq.(3) into image (3)**

Fig.(5) Cipher pixel color in all gray scale image

3- **Constructing Cipher Tables:** in this process the key image will be loaded and separated into three bands (Red, Green, Blue) and each one of the gray scale image will be exploits in constructing ciphering table by scanning image from left to right and row by row with reporting pixels color in the same sequence of the appearance of the color in scanned image until the end of the image pixels as illustrated in figure (6).

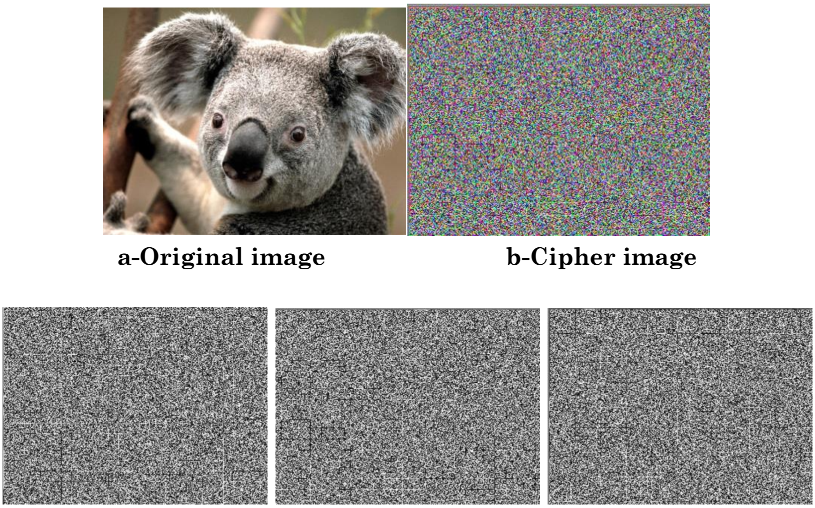


1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
66	77	250	65	3	0	54	40	52	1	231	24	196	14	9	61	33	5	13	50	4	04	37	85	22

Fig. (6) Ciphering table

The first row represents the color of the old image pixel value while the second row represents the new image pixel value, this mean if pixel value is (13) then this pixel becomes (196) in ciphered image.

4- **Ciphering with cipher tables and constructing colored cipher image:** in this process each image will be ciphered with one cipher table by replacing pixels values and final ciphered image will be constructed as illustrated in figure (7)



a-Original image **b-Cipher image**

c-Cipher of image (1) **d-Cipher of image (2)** **e-Cipher of image (3)**

Fig. (7) Ciphering images after constructing cipher table

b- decipher algorithm : this algorithm applied the same process as in cipher algorithm but in reverse fashion as follows:

1- Loading cipher image and construct cipher table for each image.

2- Applying cipher table on each image to retrieve previous pixels values .

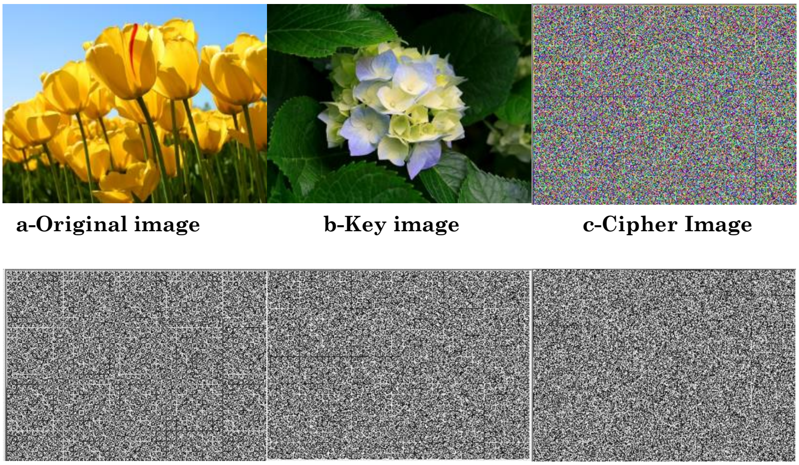
3- Applying equations (1), (2), and (3) on each pixel.

4- Construct colored decipher image file by taking pixels of image1 firstly then pixels of image 2 then and last pixels of image 3.

3. RESULTS

After applying the proposed system the following results will be obtained

Results (1)

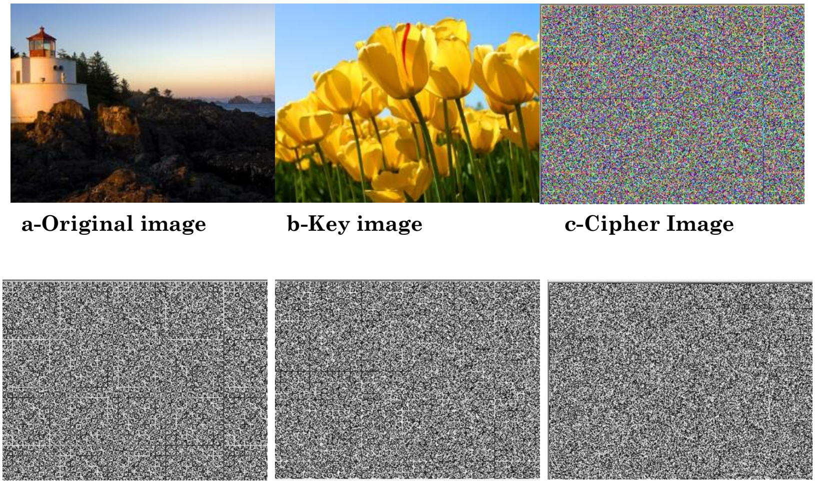


a-Original image **b-Key image** **c-Cipher Image**

d-Image (1) ciphering **e-Image (2) ciphering** **f-Image (3) ciphering**

Fig. (8) Results (1)

Results (2)

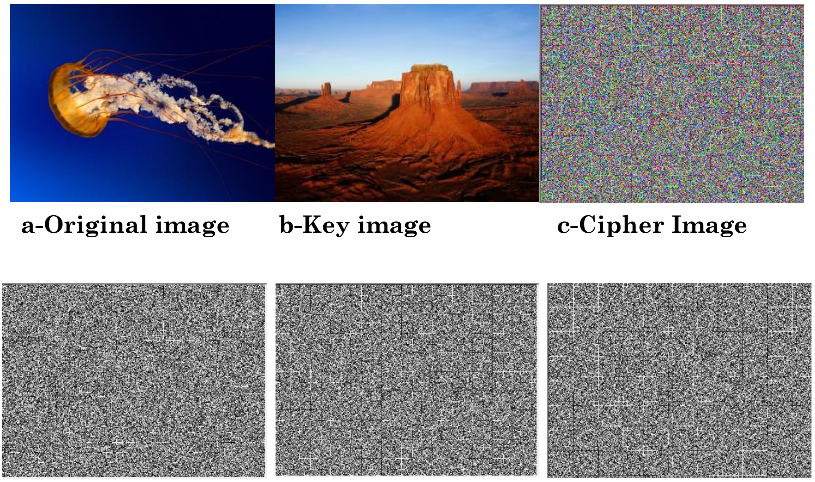


a-Original image **b-Key image** **c-Cipher Image**

d-Image (1) ciphering **e-Image (2) ciphering** **f-Image (3) ciphering**

Fig. (9) Results (2)

Results (3)



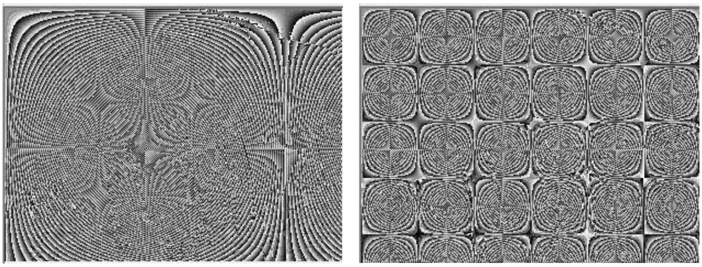
a-Original image **b-Key image** **c-Cipher Image**

d-Image (1) ciphering **e-Image (2) ciphering** **f-Image (3) ciphering**

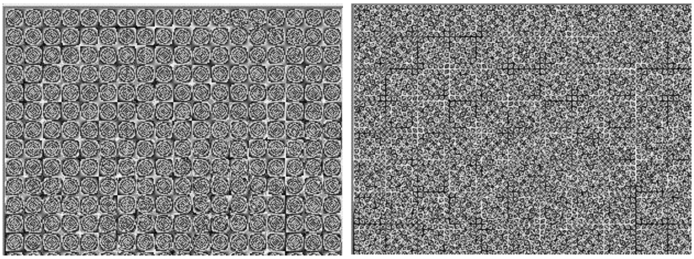
Fig. (10) Results (3)

4. CONCLUSION

1- The constant numbers used in Equations (1), (2), and (3) effect on the size of repetition of colored in ciphered image, this mean that if the proposed system select small number then the image will be separated into small number of rectangular pieces as illustrated in figure (11)



a-N=1 **b-N=5**



c-N=15 **d-N=203**

Fig. (11) Ciphering of same image with different constant value

2- Equations (1), (2), and (3) cipher pixels that have the same values in different result depending on the position of the pixel.

3- In some cases the ciphering tables have spaces in some colors because these color not found in key image, so we fill these spaces with fixed constant value like (0).

4- In ciphering image the scrambling of the pixels give power effect in final result than substitution cipher.

5- The using of the system with different results for same outputs has strong ciphering properties on the cipher image which make it stronger against unwanted attack.

REFERENCES

[1] Ali Abdul Azeez Mohammad Baker, Zainalabideen Abdullasamd Rasheed "Image Ciphering Using Position Related Matrix", *International Journal Of Advances in Engineering and Management (IJAEM)* 2015, Iraq.,

[2] Zainalabideen Abdullasamd Rasheed, Ali Abdul Azeez Mohammad Baker, "A Novel Method of Generating (Stream Cipher) Keys for Secure Communication", IOSR Journal of Computer Engineering, 2015, Iraq.

[3] Ali Abdul Azeez Mohammad Baker, Zainalabideen Abdullasamd Rasheed" Secure Keys Constructing", Education College, Kufa University, International Journal of Advanced Research in Computer Science and Software Engineering ,2014, Iraq.

[4] Nesir Rasool Mahmood, Ali Abdul Azeez Mohammad baker, Zahraa Nesir Rasool " Public Key Steganography", Kufa University ,Education College, International Journal of Computer Applications,2014, Iraq.

[5] Aphetsi Kester "A Hybrid Cryptosystem Based on Vigenère Cipher and Columnar Transposition Cipher", International Journal of Advanced Technology & Engineering Research (IJATER),2013, India.

[6] Alireza Jolfaei, Abdolrasoul Mirghadri "An Image Encryption Approach Using Chaos And Stream Cipher", Journal of Theoretical and Applied Information Technology,2010, Iran.

[7] Ahhyun Ahn and Dooyoung Kim and Taeseon Yoon "Key-Amplified Cipher", Lecture Notes on Information Theory, 2014, Korea.

[8] Mona F. M. Mursi, HossamEldin H. Ahmed, Fathi E. Abd El-samie, Ayman H. Abd El-aziem" Image Security With Different Techniques Of Cryptography And Coding: A Survey", IOSR-JCE,2014, Egypt.

[9] Lalita Gupta, Rahul Gupta and Manoj Sharma "Low Complexity Efficient Image Encryption Technique Based on Chaotic Map", International Journal of Information & Computation Technology, 2014, India.

ABOUT THE AUTHOR

Zainalabideen Abdullasamd Rasheed University of Kufa, College of Education, Najaf /Iraq. He has a BSc (Baghdad University, Iraq), and a MSc (Buckingham University, United Kingdom). He has a long experience in teaching various computing practical courses at Baghdad University, at AL Kufa University. Mr. Rasheed teaches different courses like computer organization, operating system and computer architecture. He supervises undergraduate projects. He is interested in data security (steganography and cryptography) and digital image processing (biomedical image and edge detection, de-noising images). E-mail: zain9999@live.com, Tel: 009647711131246 Iraq.