ENCRYPTION-DECRYPTION RGB COLOR IMAGE USING MATRIX MULTIPLICATION

Mohamad M. AL-Laham

Computer Science Dept- Zarqa University, Zarqa, Jordan

ABSTRACT

An enhanced technique of color image encryption based on random matrix key encoding is proposed. To encrypt the color image a separation into Red Green and Blue (R, G, B) channels will applied. Each channel is encrypted using a technique called double random matrix key encoding then three new coding image matrices are constructed. To obtain the reconstructed image that is the same as the original image in the receipted side; simple extracted and decryption operations can be maintained. The results shown that the proposed technique is powerful for color image encryption and decryption and a MATLAB and simulations were used to get the results.

The proposed technique has high security features because each color component is separately treated using its own double random matrix key which is generated randomly and make the process of hacking the three keys very difficult.

KEY WORDS

Encryption- decryption, double random matrix key, encryption time, decryption time, MSE

1. INTRODUCTION

Information security plays a vital role in different fields, especially those that require high confidentiality levels such as private businesses and military affairs.

Data security is protecting data from unwanted operations by unauthorized users. Encryption is a vital security technique, which works by converting the data into unreadable form and then using a key to decode it for reading. Image or video entities encryption has certain requirements as such entities have built-in characteristics such as mass data capacity and high redundancy. (1),(2)

Image encryption methods work on altering an image into another image that is difficult to recognize, so as to keep it confidential among users. It is important that no one is able to understand the content without using a decryption key (3),(4)and (5). Moreover, several applications need certain and consistent "security in storage and transmission of digital images", "such as pay-TV, medical imaging systems, military image communications and confidential video conferences, etc". Lots of image encryption methods have been suggested to complete this mission, but some of them were known for being insecure (5), which resulted in the need of continuous development of further methods of image encryption.

Conventional data encryption methods are classified into two categories which can be used independently or in association in each "cryptographic algorithm: substitution and transposition". In substitution method, one symbol in the data is regularly replaced with another symbol according to a certain algorithm, while in transposition method; the location of symbols is

DOI:10.5121/ijcsit.2015.7508

rearranged in the data corresponding to a certain rule. (6). A brief discussion of some image encryption techniques is given in the following paragraphs:

In 2009 Musheer Ahmad et al (22) introduce a new algorithm .In this study, the new image encryption algorithm based on three chaotic maps is discussed. In the proposed algorithm, the plain-image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out using 2D Cat map. Also, the control parameters of shuffling are randomly generated by employing 2D coupled Logistic map. After that the shuffled image is encrypted using chaotic sequence created by one dimensional Logistic map. The experimental results show that the proposed algorithm can encrypt/decrypt the images successfully with same secret keys, and the algorithm had good encryption effect, large key space and high sensitivity to small change in secret keys.

A chaotic logistic map was used by Yoon and Kim in 2010 (7), (19), and (20) to generate a small matrix. The two Authors constructed a permutation matrix from generated small matrix which is used to permute plain image pixels. Moreover, Ismail et al (9), (19) suggested a new chaotic image cipher in which they used an external secret key with 104 -bits size and two chaotic logistic maps and they generated control parameters from the external secret key for both chaotic logistic maps. In order to make system more secure; they employed a feedback mechanism in their image cipher.

Sakthidasan developed in 2011 a new image encryption scheme (23) which employs one of the three non static chaotic systems (Lorenz or Chen or LU chaotic system selected depends on 16-byte key) to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to conflict the relationship between the cipher image and the plain-image (pixel value diffusion), thereby significantly increasing the resistance to attacks. The proposed system has the advantage of larger key space; smaller iteration times and high security analysis such as key space analysis, statistical analysis and sensitivity analysis were carried out. The results demonstrate that the proposed system is highly efficient and a robust system.

In 2013 Hema et al proposed a method (24) that provides a high security for an image with minimum memory usage.Implemented security for image considering an image read its pixels and converts it into pixels matrix of order as height and width of the image. Replace that pixel into fixed numbers, create the key using random generation technique .Encrypting the image using this key, performing random transposition on encrypted image, converting it into one dimensional encrypted array and finally applied Huffman coding on that array, due this size of the encrypted image is reduced and image is encrypted again .The decryption is reverse process of encryption.

In 2013 , Quist-Aphetsi studied cryptography application(26) to set out to contribute to the general body of knowledge in this area of cryptography and by developing a cipher algorithm for image encryption of x*y size by shuffling the RGB pixel values. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel. The algorithm was implemented using MATLAB. And his finding leads to that the transposition and reshuffling of the RGB values of the image in steps has proven to be really effective in terms of the security analysis. The extra swapping of RGB values in the image file after R G B component shifting has increased the security of the image against all possible attacks available currently.

Kaladharan in 2014 presented (25) the performance of encryption and decryption of an image using a one key algorithm and tested on many images and shows fine results. In Greek, crypto refers “hidden‟ and graphy refers “script‟. Cryptography has two processes namely encryption and decryption. Encryption achieves the conversion by possessing a key of original data into unreadable form called encoding. Restoring of encrypted data in to original is decoding or decryption. Key, code or password represents the important role in cryptography.

Finally, there are many research papers which studied the expansion of the importance of security in the images because it is being used in many areas of the life and must not be used by unauthorized persons

2. TECHNIQUE DESCRIPTION

Before describing the proposed technique of image encryption-decryption let us define some terminologies that are used in the technique such that:

- Encryption: essential to let nobody knows the content of any message without a key for decryption .It is the process of converting original image to another image that is difficult to understand; to keep the image confidential between users.
- Decryption: getting the original contents from the encrypted contents using the decryption key.
- Encryption time: A time of implementing encryption process.
- Decryption time: A time of getting the original image from the encrypted one.
- Double random matrix key: it is a two dimensional matrix generated randomly with double values to minimize the probability of key hacking. The matrix is a square matrix and it must cover the color image component matrix, so it is a nxn matrix, where n=max{row, column} in the color image component matrix.
- MSE: the error between original and encrypted image is called Mean square error.
- MSE=sum (sum (sum (obtained image - original image)))/original image size.
- RGB color image: A three dimensional matrix, the first two dimensional matrix is the red component, the second is the green component and the third is the blue component.

In (21) Sharadqa proposed a method for color image encryption decryption. This method has based on converting color image to grey image then grey image was encrypted.

This method has some disadvantages such as:

1. The red and green components obtained in direct conversion phase must be saved because they are used to construct the color image in inverse conversion phase.
2. The saved components in the previous disadvantage require an extra memory space.
3. The saved components in 1 require an extra time for data transmission.
4. The red and green components obtained in direct conversion phase must be sent and they are not secure.

Taking these disadvantages into consideration we can conclude that the proposed method is not secure and there is no need to apply direct and inverse conversion.

The proposed technique is suggested in order to eliminate the previous disadvantages and it is to be implemented into two phases:

The first phase is an encryption phase which contains the following sequence of steps:

1. Get the original RGB color image rgb.
2. Change the three dimensional image rgb to one dimensional array ar.
3. Resize array ar to nearest square number by expanding ar to square size and adding zero elements.

4. Generate and save a double random key drm.
5. Reshape array ar into two dimensional matrix tdm.
6. Multiply tdm by drm to get the encrypted version of the two dimensional matrix ei.
7. Convert the two dimensional matrix to one dimensional array ear.
8. Resize ear and eliminate the expanded elements.
9. Reshape the array obtained in step 8 into 3 dimensional matrixes to get the encrypted color image.
10. Send the encrypted image.

The second phase is a decryption phase which contains the following sequence of steps:

1. Get the encrypted RGB color image rgb.
2. Change the three dimensional image rgb to one dimensional array ar .
3. Resize array ar to nearest square number by expanding ar to square size and adding zero elements.
4. Use a saved double random key drm.
5. Reshape array ar into two dimensional matrix tdm.
6. Multiply tdm by inverse of drm to get the decrypted version of the two dimensional matrix ei.
7. Convert the two dimensional matrix to one dimensional array ear.
8. Resize ear and eliminate the expanded elements.
9. Reshape the array obtained in step 8 into 3 dimensional matrixes to get the decrypted original color image.

3. TECHNIQUE IMPLEMENTATION

To illustrate the correctness of the proposed technique let us take the following worked example.

- Let us take the following 9 color pixels:

```
ci(:,:,1) =

   232    13    49
    59    20   215
    61   163    44


ci(:,:,2) =

    44    87   100
   254    80   151
   112    93    31


ci(:,:,3) =

    10   238   223
   117    67    61
   222    41   165
```

- Convert 3 dimensional matrixes to one dimensional array:

```
Columns 1 through 16

 232    59    61    13    20   163    49   215    44    44   254   112    87    80    93   100

Columns 17 through 27

 151    31    10   117   222   238    67    41   223    61   165
```

- Reshape array into square 2 dimensional matrixes and setting the expanded elements to zeros:

232	49	87	10	223	0
59	215	80	117	61	0
61	44	93	222	165	0
13	44	100	238	0	0
20	254	151	67	0	0
163	112	31	41	0	0

- Generate and save random matrix key:

0.9669	0.4302	0.1556	0.4608	0.2974	0.4001
0.6649	0.8903	0.1911	0.4574	0.0492	0.1988
0.8704	0.7349	0.4225	0.4507	0.6932	0.6252
0.0099	0.6873	0.8560	0.4122	0.6501	0.7334
0.1370	0.3461	0.4902	0.9016	0.9830	0.3759
0.8188	0.1660	0.8159	0.0056	0.5527	0.0099

- Get the encrypted matrix:

232.0000	49.0000	87.0000	10.0000	223.0000	0
59.0000	215.0000	80.0000	117.0000	61.0000	-0.0000
61.0000	44.0000	93.0000	222.0000	165.0000	0
13.0000	44.0000	100.0000	238.0000	-0.0000	-0.0000
20.0000	254.0000	151.0000	67.0000	-0.0000	-0.0000
163.0000	112.0000	31.0000	41.0000	0	-0.0000

- Get the decrypted matrix:

232	49	87	10	223	0
59	215	80	117	61	0
61	44	93	222	165	0
13	44	100	238	0	0
20	254	151	67	0	0
163	112	31	41	0	0

- Reshape the decrypted matrix into 1 dimensional array:

```
Columns 1 through 16

 232    59    61    13    20   163    49   215    44    44   254   112    87    80    93   100

Columns 17 through 32

 151    31    10   117   222   238    67    41   223    61   165     0     0     0     0     0

Columns 33 through 36

   0     0     0     0
```

- Eliminate expanded elements and reshape the array into 3 dimensional matrixes to get the original image matrix:

```
dd(:,:,1) =

   232    13    49
    59    20   215
    61   163    44


dd(:,:,2) =

    44    87   100
   254    80   151
   112    93    31


dd(:,:,3) =

    10   238   223
   117    67    61
   222    41   165
```

Here we see that the original image is the same as decrypted image which shows the correctness of the proposed technique.

4. EXPERIMENTAL RESULTS

A MAT lab code was written and tested several times using various color images, the experimental results where compared with the results of other techniques such as in (19) ;(it is called technique 1) and in (20) (it is called technique 2) and in(21) (it is called technique 3).

The programs where tested using i3 computer with 4G Byte memory and 2.5 GHz processor.

Matlab codes were implemented several times with color images with various sizes, each time MSE was calculated and the results show that in each time the decrypted image 100% matches the original image(MSE=0) as shown in figures 1 to figures 2.

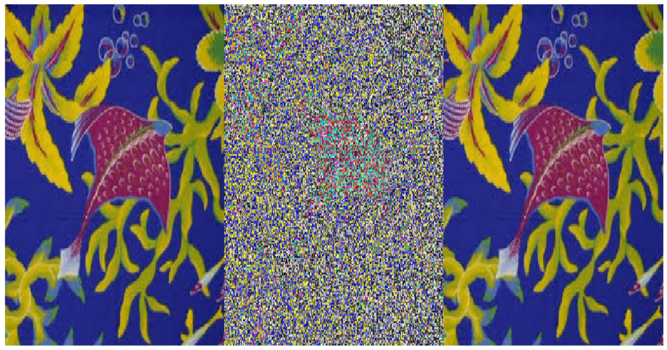

Figure 1: Original 256x256x3 image, encrypted image and decrypted image.

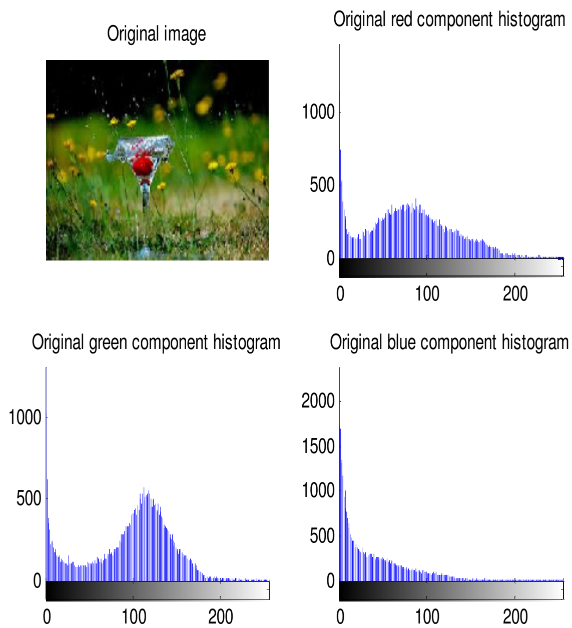

Figure 2: Original 183x276x3 image and component histograms

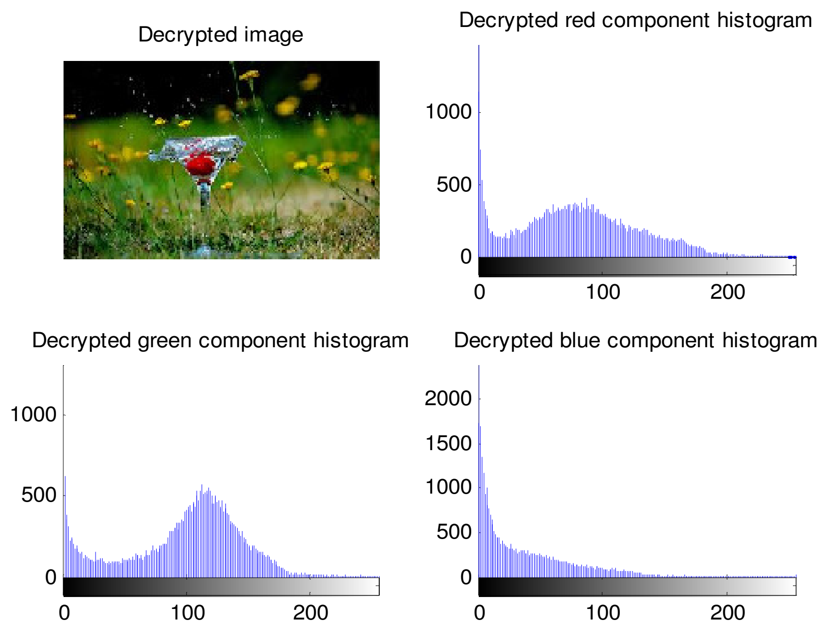

Figure 3: Decrypted 183x276x3 image and component histograms

Encryption/decryption rate of the proposed technique is also an important aspect for a good image cipher. Time taken by the proposed technique to encrypt/decrypt various different sized color images has been measured. The time analysis has been done on a personal computer with Intel i3 duo 2.5Ghz processor and 4GB RAM. The results are summarized in Table 1, which clearly predicts an average encryption-decryption rate of proposed technique is 0.4046 seconds.

Table 1: Encryption-decryption rates

Image size	Encryption time(sec.)	Decryption time(sec.)	Total time
183*276*3	0.059000	0.059000	0.1180
726*600*3	1.03000	1.03000	2.0600
186 * 270 * 3	0.062000	0.062000	0.1240
225 * 225* 3	0.015300	0.015300	0.0306
214* 235* 3	0.023200	0.023200	0.0464
256*256*3	0.02400	0.02400	0.0480
Average	0.2023	0.2023	0.4046

The encryption-decryption rate of the proposed technique was compared with the rates for technique1, technique 2 and technique 2. Table 2 shows the results of comparisons using 256*256*3 image:

Table 2: Comparisons results using 256*256*3 image

Technique	Encryption time (sec.)	Decryption time(sec.)
Proposed technique	0.02400	0.02400
Technique 1	0.22500	0.22500
Technique 2	2.515000	2.453000
Technique 3	0.026000	0.070000

The results of comparisons using 800*600*3 image are show in the following table 3:

Table 3: Comparisons results using 800*800*3 image

Technique	Encryption time (sec.)	Decryption time(sec.)
Proposed technique	1,012000	1,012000
Technique 1	3.24	3.24
Technique 2	10.537000	19.425000
Technique 3	1.269000	1.278000

5. RESULTS DISCUSSION

The obtained experimental results prove that the proposed technique is more effective and secure by taking the following:

- The proposed technique uses one large matrix with double values which minimizes the probability of key hacking.
- The proposed technique minimizes MSE to zero which means that there is no any loss of information due the process of encryption-decryption.
- The proposed technique enhances the performance of encryption-decryption process by decreasing the total encryption-decryption time.
- The proposed technique is very confidence and accurate.

6. CONCLUSIONS

The security of digital images is an important issue since the communications of digital products over open network occur more and more frequently. In this paper, a new technique of image encryption-decryption technique has been proposed which utilizes matrix multiplication and inverse matrices.

According to the results of our experiments the proposed technique rapidly increases the image transmission security and enhances the encryption-decryption process by eliminating the mean square error and maximizing the speed of the encryption decryption process.

ACKNOWLEDGEMENT

"This research is funded by the Deanship of Research in Zarqa University /Jordan"

REFERENCES

[1] Z.Guan, F.Huang and W. Guan, "Chaos-Based Image Encryption Algorithm," Physics Letters A, Vol. 346, No. 1-3, 2005, pp. 153-157. doi:10.1016/j.physleta.2005.08.006

[2] H.H.Nien, C.K.Huang, S.K.Changchien, H.W.Shieh, C.T.Chen and Y.Y.Tuan, "Digital Color Image Encoding and Decoding Using a Novel Chaotic Random Generator," Chaos Solitons and Fractals, Vol. 32, No. 3, 2005, pp. 1070-1080. doi:10.1016/j.chaos.2005.11.057

[3] Q.Alsafasfeh and A. Alshabatat, "Image Encryption Based on Synchronized Communication Chaotic Circuit," Journal of Applied Sciences Research, Vol. 7, No. 4, 2011, pp. 392-399..

[4] V.Patidar, N. K. Pareek and K. K. Sud, "A New Substitution-Diffusion Based Image Encrypete Using Chaotic Standard and Logistic Maps," Communications in Non-Linear Science and Numerical Simulation, Vol. 14, No. 7, 2009, pp. 3056-3075. doi:10.1016/j.cnsns.2008.11.005

[5] Li.Shujun, and X. Zheng "Cryptanalysis of a chaotic image encryption technique," Inst. of Image Process, Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. IEEE International Symposium on Publication Date: 2002, Vol. 2, 2002, pp. 708-711.

[6] F.Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni and M. Reginelli, "A New Chaotic Algorithm for Video Encryption" ,IEEE Transactions on Consumer Electronics, Vol. 48, No. 4, 2002, pp. 838-844. doi:10.1109/TCE.2003.1196410

[7] Giesl, J., Vlcek, K., "Image Encryption based on strange attractor", ICGST-GVIP Journal, ISSN 1687-398X, Volume (9), Issue(II), April 2009

[8] M. Francois, T.Grosges, D.Barchiesi, R.Erra," A new image encryption scheme based on a chaotic function", 2012, Signal Processing: Image Communication 27 (2012)249–259

[9] Ismail, I., Amin M., and Diab H.,"A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps",International Journal of Network Security, Vol.11, No.1, PP.1–10, July 2010.

[10] Droogenbroeck, M., and Montefiore, R., "Techniques for a selective encryption of uncompressed and compressed images", In ACIVS Advanced Concepts for Intelligent Vision Systems, Ghent, Belgium, pages 90-97, September 2002.

[11] Wong k., Kwok B., and Law W., "A Fast Image Encryption Scheme based on Chaotic Standard Map", CoRR abs/cs/0609158: (2006), City University of Hong Kong, arXiv:cs/0609158v1[cs.CR], http://arxiv.org/abs/cs/0609158.

[12] Xin Ma, Chong Fu, Wei-min Lei and Shuo Li, (2011) "A novel chaos-based image encryption scheme with an improved permutation process", International Journal of Advancements in Computing Technology, Vol. 3, No. 5, pp 223-233.

[13] Ahmed H, Kalash H, and Farag Allah O., "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption", Informatica 31 (2007) 121–129.

[14] G A.Sathishkumar, K. Bhoopathy bagan and N. Sriraam, (2011) "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network Security & its Applications, Vol. 3, No. 2, pp 181-194.

[15] Mehrzad Khaki Jamei, Rasul Enayatifar and Hamid Hassanpour, (2011) "Hybrid model of chaotic signal and complete binary tree for image encryption", International Journal of the Physical Sciences, Vol. 6, No. 4, pp. 837-842.

[16] S.V.Sathyanarayana, M. Aswatha Kumar and K.N. Hari Bhat, (2011), "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points", International Journal of Network Security, Vol. 12, No. 3, pp.137-150.

[17] N.K.Pareek, Vinod Patidar and K.K. Sud, (2011) "A symmetric encryption scheme for colour BMP images", International Journal on Computer Application, NSC(2), pp. 42-46.

[18] Soheil Fateri and Rasul Enayatifar, (2011) "A new technique for image encryption via standard rules of CA and logistic map function", International Journal of Physical Sciences, Vol. 6, No. 12, pp. 2921-2926.
[19] Narendra K Pareek,(2012), " Design And Analysis Of A Novel Digital Image Encryption Scheme", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2.
[20] 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.
[21] Ahmad Sharadqa," RGB Color Image Encryption-Decryption Using Gray Image ", IJCSI International Journal of Computer Science Issues, Volume 12, Issue 3, May 2015 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org 137
[22] Musheer Ahmad et al ,2009, " A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping ", International Journal on Computer Science and Engineering, Vol.2 (1), 2009, 46-50)
[23] K. Sakthidasan and B. V. Santhosh Krishna ,2011, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images " , International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011
[24] Hema Suresh Yaragunti et al,2013, " An Effective Algorithm of Encryption and Decryption of Images Using Random Number Generation Technique and Huffman coding" , Int.J.Computer Technology & Applications , Vol 4 (6),883-891 IJCTA | Nov-Dec 2013
[25] Kaladharan N, 2014, "Unique Key Using Encryption and Decryption of Image ", ,International Journal of Advanced Research in Computer and Communication Engineering , Vol.3, Issue 10, October 2014)
[26] Quist-Aphetsi Kester, 2013," Image Encryption based on the RGB PIXEL Transposition and Shuffling ", I.J.Computer Network and Information Security, 2013, 7, 43-50 Published Online June 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.07.05

AUTHOR

Mohamad Al-Laham is an Associate Professor of Computer Information Systems at Zarqa Private University in computer science dept for sabbatical and has research interests in the areas of networking, Internet and distributed systems.