International Journal of Engineering & Technology, 7 (3.13) (2018) 104-107

SPC

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication

Musbah J. Aqel[1]*, Ziad ALQadi[2], Ammar Ahmed Abdullah[3]

[1]Department of Management Information System, School of Applied Sciences
Cyprus International University, Nicosia, Northern Cyprus
[2]Department of Computer Engineering, Albalqaa' Applied University,
Amman, Jordan
[3]Department of Computer Science, College of Information Technology
Applied Sciences University, Amman, Jordan
**Corresponding author E-mail: maqel@ciu.edu.tr:*

Abstract

Digital RGB color images are considered as the most widely used data type through the internet, so there is a need for efficient and secure techniques to transmit and protect these digital images and this is a matter of high priority process. Many researchers had developed different techniques to increase the security of image transmission, and most of these techniques suffer from the low speed of the encryption-decryption process. In this paper, a novel technique is proposed that could be used for digital color image encryption-decryption. The performance of this technique is compared with the performance of other techniques and it has shown the advantages of using this technique over other techniques in enhancing the throughput and speed of encryption-decryption process.

Keywords: : Digital RGB color Image; Image Segmentation; Private Key; Encryption; Decryption, Speedup; Throughput ; Hacking.

1. Introduction

Encryption is the process of conversion of a plain message (i.e. a matrix which represents digital RGB color image) into an encrypted form that is called a cipher text which is not possible to be used by any user without making the required decryption process for the text [15]. While, the decryption process is considered as the reverse of encryption process that includes of converting back the encrypted text into its original plain text, which enables the user to read it [15]. In RGB color images, the encryption process should be carried out before transmitting the image over the internet securely and to ensure that no any unauthorized user can perform any decryption process for this image. The encryption process for image, video and other chaos based techniques have many applications in many areas like medical imaging, internet communication, transmission, military Communication, etc. The progress in encryption techniques is moving towards a future of endless possibilities and applications. The image data have special features such as a huge capability, high correlation between the pixels, and a high redundancy. Encryption techniques are very useful tools to protect private information [3].

Data encryption is the main technique that used to secure the data resources over the internet, intranets and extranets and to provide an authentication process for the users' data resources from integrity, accuracy and safety perspectives [16].

2. Related Work

Many researchers proposed many techniques for image encryption- decryption. Guodong Ye [9] proposed an efficient image encryption algorithm based on digital matrix of the image confusion concept where the row and column are confused. The confusion concept is implemented by using the substitution process and by adopting Chen's system in order to diffuse the gray value distribution.

Haojiang Gao *et al*. [5] developed a Nonlinear Chaotic Algorithm (NCA) algorithm that based on using power and tangent functions. The encryption algorithm in its nature is a one-time-one-password system and after implementation it has shown that its performance is better than the DES security algorithm performance.

Jawahar Thakur *et al*. [17] proposed a comparison study between different symmetric key algorithms such as DES, AES, and Blowfish. Different parameters were considered like block size, key size, and speed in order to assess the performance of these algorithms. Blowfish has shown the best performance over other encryption algorithms and AES showed poorest performance based on the results of other compared algorithms and it was because it takes more power for processing.

Khaled Loukhaoukha *et al*. [9] proposed an image encryption-technique that used a Rubik's cube concept. Where the original image is scrambled based on the concept of Rubik's cube and then XORed with values in the columns and rows of the scrambled image by using two secret keys.

Liu Hongjun *et al*. [18] developed a stream-cipher algorithm is implementing one-time keys and robust chaotic maps. The algorithm then performs a piecewise linear chaotic map as the generator of a pseudo-random key stream sequence.

M. Zeghid *et al*. [19] conducted an analysis for the AES algorithm, and modified it by adding a key stream generator to AES to guarantee an enhancement in the performance of the encryption of the images. The technique overcomes many problems of textured zones that were available to other popular encryption algorithms.

Maniccam *el al*. [20] developed techniques for both video and image encryption that used the SCAN technique. The image encryption is performed by SCAN-based permutation of pixels and a substitution rule which are both forming an iterated product cipher. Accordingly, the pixels are rearranged by scanning the keys and the values of the pixels are changed by a substitution mechanism [16].

Mohammad Ali el al. [21] presented a block-based transformation technique which is by using the combination of image transformation and the Blowfish algorithm produces the best performance by finding the highest entropy and lowest correlation. The most important features of AES algorithm are the security and the resistance against attacks while the major characteristic of RC4 algorithm is its speed [11]. A hybrid cipher by combining the characteristics of AES and RC4 is proposed and implemented and it has shown that there are more than 20% enhancement in speed whenever it is compared to the original AES while it has also shown a higher security compared to the original RC4 [13].

Sanfu Wang *et al*. [21] proposed an image scrambling algorithm that is using a folding transform in order to fold a matrix which is an orthogonal matrix and that allows to fold images in either direction up-down or left-right. Whenever an image is folded by using this technique repeatedly, it results in a scrambled image. The scrambled algorithm then has an efficient hiding capability and a wide adaptability to images with many different scales.

Sathish kumar G.A *et al*. [14] proposed a pixel shuffling algorithm that uses a base-64 encoding strategy which is a combination of pixel permutation, value transformation, and block permutation. The encryption system is implemented by using a simple chaotic map for key generation and a logistic map to generate a pseudo random bit sequence and the total key length is 512 bits for each round.

Shao Liping *et al.* [4] presented a scrambling algorithm that is based on random shuffling principle which could scramble non equilateral images and has a low cost to implement a coordinate shifting path. The algorithm is based on permuting pixel coordinates and it may be used to scramble or recover image in real time.

T. Siva kumar, and R. Venkatesan [4] developed an image encryption technique by using matrix reordering. This technique was implemented and tested, and its performance was compared with other techniques.

Ziad A. Alqadi et.al., [1] and [2] developed a method for implementing a direct and inverse conversions to convert a RGB color image to gray image and vice versa, the method could be useful to implement RGB color image encryption- decryption.

3. Proposed Method

The proposed method consists of two phases, the encryption phase and the decryption phase. The encryption phase can be is implemented by carrying out the following steps:

1. Get the original RGB color image (3-D matrix).
2. Reshape the matrix obtained in step (1) as a one column matrix.
3. Find the nearest bigger number to the size of the column matrix.
4. Pad zeros to the column matrix to get a square size.
5. Reshape the column matrix to square 2-D matrix.
6. Select the number of segments to be used to separate the matrix obtained in step (5) into segments (this number is only known by the sender and receiver).
7. Generate one random square matrix for each segment to be used as a private key for encryption.
8. Encrypt each segment by applying matrix multiplication of the matrix segment and its private key.
9. Reshape each encrypted matrix to its original size.
10. Form the encrypted RGB color image from the segments.

While the decryption phase can be implemented by applying the following steps:

1. Get the decrypted RGB color image (3-D matrix).
2. Reshape the matrix obtained in step 1 as a one column matrix.
3. Find the nearest bigger number to the size of the column matrix.
4. Pad zeros to the column matrix to get a square size.
5. Reshape the column matrix to square 2-D matrix.
6. Use the number of segments to be used to separate the matrix obtained in step 5 into segments.
7. Use the private key for each segment.
8. Decrypt each segment by applying matrix multiplication of the matrix segment and the inverse of its private key.
9. Reshape each encrypted matrix to its original size.
10. Form the encrypted RGB color image from the segments.

4. Proposed Method Implementation

The proposed method was implemented by using MATLAB software. The implementation process includes tow phases. The first phase is the encryption phase where the following Matlab code can be used to implement this phase (for other images you have to change the numbers to match the image size).

```
%Encryption Phase
tic
a1=reshape(a,194*259,1);
%padding zeros
for i=50247:50625
   a1(i,1)=0;
end
%Reshape into square matrix
a2=reshape(a1,225,225);
%Get the segments (here 3 segments)
a21=a2(1:75,1:75);
a22=a2(76:150,76:150);
a23=a2(151:225,151:225);
%Generate 3 private keys
k1=rand(75,75);
k2=rand(75,75);
k3=rand(75,75);
% Encrypt each segment
e1=double(a21)*k1;
e2=double(a22)*k2;
e3=double(a23)*k3;
% Compose the encrypted image
ee(1:75,1:75)=e1;
ee(76:150,76:150)=e2;
ee(151:225,151:225)=e3;
dd1=reshape(ee,225*225,1);
%Omit the padded zeros
 for i=1:50246
   dd2(i,1)=d1(i,1);
end
% Get the encrypted image
dd3=reshape(dd2,194,259);
dd3=uint8(dd3);
toc
```

The following Matlab code can be used to implement the decryption phase (for other images you have to change the numbers to match the image size).

```
%Decryption phase
tic
dd3=reshape(dd3,194*259,1);
for i=50247:50625
   dd3(i,1)=0;
end
m2=reshape(dd3,225,225);
m21=m2(1:75,1:75);
m22=m2(76:150,76:150);
m23=m2(151:225,151:225);
```

```
de1=double(m21)*inv(k1);
de2=double(m22)*inv(k2);
de3=double(m23)*inv(k3);
dee(1:75,1:75)=de1;
dee(76:150,76:150)=de2;
dee(151:225,151:225)=de3;
de=reshape(dee,225*225,1);
for i=1:50246
    dd2(i,1)=de(i,1);
end
dde3=reshape(dd2,194,259);
dd3=uint8(dde3);
toc
```

4. Experimental Results

Before discussing the implementation of the proposed method, let us take a matrix of size 4096*4096 bytes and encrypt-decrypt it using segmentation. Table (1) shows the encryption and decryption processing times. The encryption processing time includes the segmentation time while the decryption processing time includes the time it takes to reconstruct the original matrix. The total time is obtained by multiplying the number of segments by the sum of the encryption and decryption processing times.

Table 1: Results of the Example

# of segments	Segment size	#of private keys	Encryption time(s)	Decryption time(s)	Total time(s)	Speedup
1	4096*4096	1	28.829000	61.371000	90.2000	1
2	2048*2048	2	3.666000	7.924000	23.1800	3.8913
4	1024*1024	4	0.468000	1.061000	6.1160	14.7482
8	512*512	8	0.063000	0.156000	1.7520	51.4840
16	256*256	16	0.015000	0.016000	0.4960	181.8548
32	128*128	32	0.000300	0.000300	0.0192	4697.9

Figure (1) shows the total processing time for each case with different number of segments, while figure (2) shows the speed up of each case with reference to each segment case.

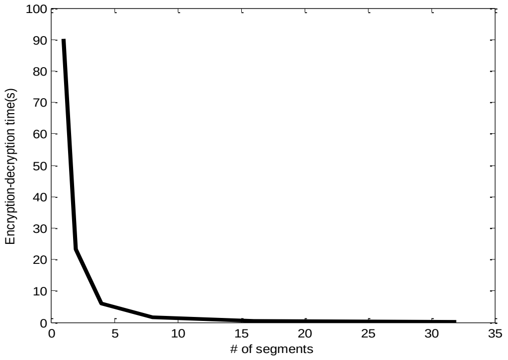

Figure (1): Total time

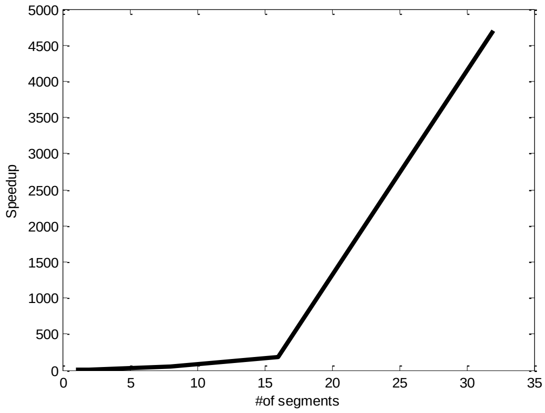

Figure (2): Speedup

The proposed method was implemented several times using different RGB color images with different sizes and the results always give a correlation coefficient that equals 1 between the original image and the decrypted one. Which means that the method produces a correct and reliable results and do not cause any damage of information? Figure (3) shows the original image and the decrypted one.

The proposed method is also very secure and it is impossible to hack the image because of the following features of the method:

1) The private key has the following features:

- 2-D matrix has a huge size.
- Each element in the private key is a random double number which makes it impossible to guess.

2) Secret key.

3) The number of segments is a secret number.

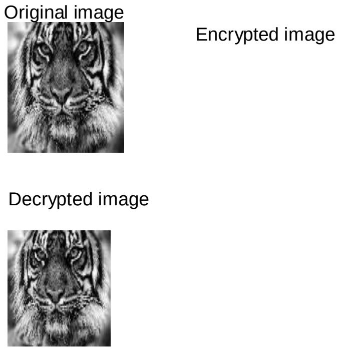

Figure (3): Sample of original and decrypted images

The encryption and decryption processing times, the speed up, and throughput were calculated and compared with other methods mentioned in the related works. These results are listed in Table 2. The speedup was calculated by dividing the total time of the method by the total time of proposed 1 (which was taken as a reference because it has the best efficiency).

The throughput was calculated by dividing the RGB color image size by the total time.

Table (2): Comparisons results (image size=725*725*3 bytes)

Method	Encryption time(s)	Decryption time(s)	Total time(s)	Speed up	Through put(MB/s)
Proposed 1	0.015000	0.020000	0.0350	1	45.0536
Ref.[4]	0.23	0.23	0.46	13.1429	3.4280
Ref.[5]	0.5	0.5	1.0	28.571	1.5769

				4	
Ref.[6]	0.12	0.12	0.24	6.8571	6.5703
Ref.[7], (A-I)	0.56	0.56	1.12	32	1.4079
Ref.[7],(A -II)	1.01	1.01	2.02	57.714 3	0.7806
Ref.[8]	0.4	0.4	0.8	22.857 1	1.9711

It is clear that the proposed method is taking less processing time compared with other works using the same image size. However, it also has the highest speed, and it shows the best throughput.

5. Conclusions

A method for encryption-decryption of RGB color image was proposed and implemented. A comparison analysis was carried out and it has shown that the proposed method has the best performance from the following perspectives:

- Best speed in encryption phase.
- Best speed in decryption phase.
- Best throughput.
- No any damage of information.
- Impossible to hack

References

[1] Ziad A. Alqadi ,Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, 2010, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952.

[2] Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173.

[3] Rojo, M.G., G.B. García, C.P. Mateos, J.G. García and M.C. Vicente, 2006. Critical comparison of 31 commercially available digital slide systems in pathology. Int. J. Surg. Pathol., 14: 285-305.

[4] T.Sivakumar , and R.Venkatesan , A Novel Image Encryption Approach using Matrix Reordering, WSEAS TRANSACTIONS on COMPUTERS, Issue 11, Volume 12, November 2013,pp 407-418.

[5] Haojiang Gao, Yisheng Zhang, Shuyun Liang and Dequn Li, "A New Chaotic Algorithm for Image Encryption", Elsevier Science Direct, vol. 29, no. 2, 2006, pp.393-399.

[6] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering, 2011, pp. pp.1-13.

[7] Xiaomin Wang, and Jiashu Zhang, "An Image Scrambling Encryption using Chaos- controlled Poker Shuffle Operation", IEEE International Symposium on Biometrics and Security Technologies, Islamabad, 23-24 April 2008, pp.1-6.

[8] G. Chen, Y. Mao, and C. K. Chui, "A Symmetric Image Encryption Scheme based on 3D Chaotic Cat Maps", Chaos, Solitons and Fractals, Vol. 21, No. 3, 2004, pp.749–761.

[9] Guodong Ye, "An Efficient Image Encryption Scheme based on Logistic maps", International Journal of Pure and Applied Mathematics, Vol.55, No.1,2009, pp. 37-47.

[10] Han Shuihua and Yang Shuangyuan, "An Asymmetric Image Encryption Based on Matrix Transformation", ECTI Transactions on Computer and Information Technology, Vol.1, No.2, 2005, pp. pp.126-133.

[11] Prabhudesai Keval Ketan and Vijayarajan V, "An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption", International Journal of Computer Applications, Vol.54, No.12, 2012, pp.29-36.

[12] S.A.M Rizvi, Syed Zeeshan Hussain and Neeta Wadhwa, "A Comparative Study of Two Symmetric Encryption Algorithms Across Different Platforms", International Conference on Security and Management (SAM'11), World Academy of Science, USA, 2011.

[13] Sanfu Wang, Yuying Zheng and Zhongshe Gao, "A New Image Scrambling Method through Folding Transform", IEEE International Conference on Computer Application and System Modeling, Taiyuan, 22-24 Oct. 2010, pp.v2-395-399.

[14] G.A. Sathishkumar and K.Bhoopathy Bagan, "A Novel Image Encryption Algorithm Using Pixel Shuffling and BASE 64 Encoding Based Chaotic Block Cipher, WSEAS Transactions on Computers, Vol.10, No. 6, 2011, pp. 169-178.

[15] John Justin M, Manimurugan S , "A Survey on Various Encryption Techniques ", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

[16] Ephin M, Judy Ann Joy and N. A. Vasanthi, " Survey of Chaos based Image Encryption and Decryption Techniques " , Amrita International Conference of Women in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA).

[17] Jawahar Thakur, and Nagesh Kumar, "DES, AES, and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol.1, No.2, 2011, pp.6-12.

[18] Liu Hongjun and Wang Xingyuan, "Color image encryption based on one-time keys and robust chaotic maps", Journal of Computers and Mathematics with Applications (Elsevier), Vol.59, 2010, pp. 3320-3327.

[19] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology, Vol.3, 2007, pp.526-531.

[20] S.S. Maniccam, and N.G.Bourbakis "Image and Video Encryption using SCAN Patterns", The Journal of the Pattern Recognition Society, Vol.37, 2004, pp.725-737.

[21] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, Vol.35, No.1, 2008, pp.3-11.