International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

PERFORMANCE ANALYSIS OF COLOR IMAGE ENCRYPTION\DECRYPTION TECHNIQUES

Jihad N. Abdel-Jalil

Abstract

Digital color image usually has a huge size, thus image security must be very essential and the hacking process must eliminated. This paper proposes a novel technique, which allows the users to encrypt-decrypt different sizes color images, this technique has to provide confidentiality service for images with less computational overhead. The proposed technique is to be implemented and tested, and the obtained experimental results must be compared with other available techniques results. A comparative analysis will be performed for this technique and other available techniques used for encryption-decryption, the encryption time must be calculated in order to find the speedup of the proposed technique comparing with other techniques.

Keywords: Image Security, Image Encryption, Image decryption, encryption time, decryption time, private key, speedup, throughput.

Introduction

In today's corporate world, information including digital color images travel widely and rapidly, in multiple manifestations, through email and across the Internet. Controlling and protecting sensitive or confidential documents and images has become next to impossible. Corporations have very little visibility into exactly where their documents are being accessed or by whom. So it is essential to find a technique which can be used to keep the transmitted image secure and confidential.

The conventional algorithms like Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Advanced Encryption Standard (AES) have certain limitations in data encryption because of the high values of encryption and decryption times and there is a need to develop specific encryption technique for images encryption-decryption [6, 7, 8]. Position change, value transformation and visual transformation are the different types of image encryption methods introduced by numerous researchers [9, 10, 11, 12]. Chaos based image encryption using wavelet transforms, vector quantization, and random phase encoding for color image encryption are some of the existing image encryption algorithms available in the literature [1, 2, 3, 4, 5]. The advantage of an image encryption over traditional text encryption is that the decrypted image is tolerant with small distortion due to human perception.

Related works

Guodong Ye [6] presented an efficient image encryption scheme using double logistic maps, in which the digital matrix of the image is confused from row and column respectively. Confusion effect is carried out by the substitution stage and Chens system is employed to diffuse the gray value distribution. Haojiang Gao et al. [2] presented a Nonlinear Chaotic Algorithm (NCA) by using power and tangent functions instead of linear function. The encryption algorithm is a one-time-one-password system and is more secure than the DES algorithm. Jawahar Thakur et al. [13] presented a comparison between symmetric key algorithms such as DES, AES, and Blowfish. The parameters such as speed, block size, and key size are considered to evaluate the performance when different data loads are used. Blowfish has a better performance than other encryption algorithms and AES showed poor performance results compared to other algorithms due to more processing power.

Khaled Loukhaoukha et al. [3] introduced an image encryption algorithm based on Rubik’s cube principle. The original image is scrambled using the principle of Rubik’s cube and then XOR operator is applied to rows and columns of the scrambled image using two secret keys. Liu Hongjun et al. [14] designed a stream-cipher algorithm based on one-time keys and robust chaotic maps. The method uses a piecewise linear chaotic map as the generator of a pseudo-random key stream sequence.

M. Zeghid et al. [15] analyzed the AES algorithm, and added a key stream generator (A5/1, W7) to AES to ensure improved encryption performance mainly for the images. The method overcomes the problem of textured zones existing in other known encryption algorithms. Maniccam el al. [16] presented a method for image and video encryption and the encryption methods are based on the SCAN methodology. The image encryption is performed by SCAN-based permutation of pixels and a substitution rule which together form an iterated product cipher. The pixel rearrangement is done by scanning keys and the pixel values are changed by substitution mechanism. Figure 1 shows the basic SCAN patterns used in [16]. Mohammad Ali el al. [17] introduced a

ISSN:2319-7900

block-based transformation algorithm based on the combination of image transformation and the Blowfish algorithm. The algorithm resulted in the best performance by the lowest correlation and the highest entropy. The characteristics of AES are its security and resistance against attacks and the major characteristic of RC4 algorithm is its speed [8]. A hybrid cipher by combining the characteristics of AES and RC4 is developed and 20% improvement in speed is achieved when compared to the original AES and a higher security compared to the original RC4 [10].

Rizvi et al. [9] analyzed the security issues of two symmetric cryptographic algorithms Blowfish and CAST algorithm and then compared the efficiency for encrypting text, image, and audio with the AES algorithm across different widely used Operating Systems. For text data, all algorithms run faster on Windows XP but Blowfish is the most efficient and CAST run slower than AES. Blowfish encrypts images most efficiently on all the three platforms. For audio files, CAST performs better than Blowfish and AES on Windows XP but on Windows Vista and Windows 7, there is no significant difference in the performance of CAST and AES; however, Blowfish encrypts audio files at less speed.

Sanfu Wang et al. [18] presented an image scrambling method based on folding transform to folding matrix which is orthogonal and enables to fold images either up-down or left-right. When an image is folded this way repeatedly, it becomes scrambled. The scrambling algorithm has an effective hiding ability with small computation burdens as well as wide adaptability to images with different scales.

Sathishkumar G.A et al. [11] presented a pixel shuffling, base 64 encoding based algorithm which is a combination of block permutation, pixel permutation, and value transformation. The crypto system uses a simple chaotic map for key generation and a logistic map was used to generate a pseudo random bit sequence. The total key length is 512 bits for each round and the key space is approximately 2512 for ten rounds. Shao Liping et al. [19] proposed a scrambling algorithm based on random shuffling strategy which could scramble non equilateral images and has a low cost to build coordinate shifting path. The algorithm is based on permuting pixel coordinates and it could be used to scramble or recover image in real time. T.Sivakumar , and R.Venkatesan [1] proposed a novel image encryption approach using matrix reordering this approach was tested and some comparisons with other techniques were done.

The proposed technique

The proposed technique for encryption phase can be implemented applying the following steps:

1. Get the original digital color image as a 3 dimensional matrix(m).
2. Reshape m into 1 column matrix(r).
3. Get the size of r (s).
4. If s is a square number proceed to step 6.
5. Find the nearest square number to s and adjust s to this number, adjust r by padding zeros.
6. Reshape r to square matrix (r1).
7. Generate a double random square matrix with size equal r1 size, this matrix will be used as a private key for encryption-decryption (k).
8. Save k to be used in the decryption phase.
9. Get the encrypted image (e) by applying matrix multiplication of r1 and k.
10. Reshape e into 1 column matrix (e1).
11. Omit the padded zeros from e1.
12. Reshape e1 into 3 dimensional matrix to get the encrypted color image.

The decryption phase can be implemented applying the following steps:

1. Get the encrypted digital color image as a 3 dimensional matrix (en1).
2. Reshape en into 1 column matrix (en2).
3. Get the size of en2 (s).
4. If s is a square number proceed to step 6.
5. Find the nearest square number to s and adjust s to this number, adjust en2 by padding zeros.
6. Reshape en2 to square matrix (en3).
7. Use the private key k.
8. Get the decrypted image (di) by applying matrix multiplication of r1 and the inverse of k.
9. Reshape di into 1 column matrix (di1).
10. Omit the padded zeros from di1.
11. Reshape di1 into 3 dimensional matrix to get the decrypted original color image.

Proposed technique implementation

The following matlab code was written and used to implement the proposed technique:

```
clear all
close all
a=imread('C:\Users\User\Desktop\flower-color-
combinations.jpg');
subplot(2,2,1)
imshow(a), title 'Original image'
subplot(2,2,2)
imhist(a(:,:,1)), title 'Red component histogram'
subplot(2,2,3)
imhist(a(:,:,2)), title 'Green component histogram'
subplot(2,2,4)
```

ISSN:2319-7900

```
imhist(a(:,:,3)), title 'Blue component histogram'
tic
b=reshape(a,200*300*3,1);
for i=180001:180625
 b(i,1)=0;
end
c=reshape(b,425,425);
k=rand(425,425);
c=double(c);
e=c*k;
toc
tic
d=e*inv(k);
d1=reshape(d,425*425,1);
for i=1:180000
 d2(i,1)=d1(i,1);
end
d3=uint8(d2);
d4=reshape(d3,200,300,3);
toc
figure
subplot(2,2,1)
imshow(d4), title 'Decrypted image'
subplot(2,2,2)
imhist(d4(:,:,1)), title 'Decrypted red component histogram'
subplot(2,2,3)
imhist(d4(:,:,2)), title 'Decrypted green component
histogram'
subplot(2,2,4)
imhist(d4(:,:,3)), title 'Decrypted blue component histogram
'
```

This code was tested several times using digital color images with defirent sizes and it was seen that the original and decrypted images all the are identical and the correleation coefecient between the original image and the decrypted image was always equal 1. Figure 1 and show the identity bgetween the original image and the decrypted one.

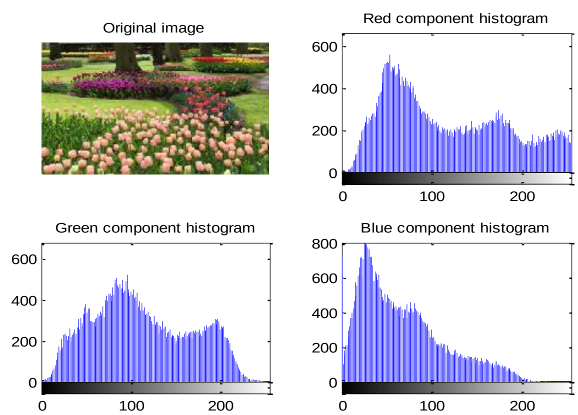

Figure 1: Original color image

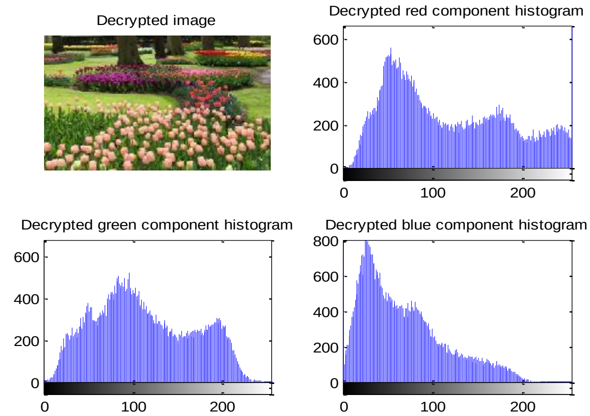

Figure 2: Decrypted color image

Comparative analysis

The proposed technique with the related techniques mentioned in table 1 were implemented and the implementation results were compared.

First of all I will focus on the following two advantages of the proposed technique comparing with related ones:

1. The proposed technique does not cause any damage of information, thus there is no loss of information during the encryption and decryption phases, and the decrypted image and the original one always identical.
2. The proposed technique is highly secure and it is impossible to hack the huge private key with double elements.

To apply comparative analysis we will use the following parameters:

1. Throughput: The throughput for encryption as well as decryption is calculated one by one. Encryption time is used to calculate the throughput of an encryption technique .The throughput of the encryption technique is calculated by dividing the size of wave file in MB by total encryption time in second. If the throughput value is increased, the power consumption of this encryption technique is decreased .Similar procedure has been followed to calculate the throughput of decryption technique. For my experiment. The performance metrics are analyzed by :

(a) Encryption/decryption time.
(b) CPU process time – in the form of throughput.

Throughput = image size (MB) / Encryption or decryption time (Sec.)

ISSN:2319-7900

The selected image size=256*256*3*8= 1572864 bytes= 1.5729 MB.

Table 1: Comparative results analysis

Method	Encryption time(s)	Decryption time(s)	Speed up (comparing with proposal)	Throughput (MB per second)
Proposed(1)	0.006469	0.062727	1	25.0748
Ref.[1](2)	0.23	0.23	3.6667	6.8385
Ref.[2](3)	0.5	0.5	7.9710	3.1457
Ref.[3](4)	0.12	0.12	1.9131	13.1072
Ref.[4], (A-I)(5)	0.56	0.56	8.9276	2.8087
Ref.[4],(A-II)(6)	1.01	1.01	16.1015	1.5573
Ref.[5](7)	0.4	0.4	6.3768	3.9322
DES(8)	30	30	478.2629	0.0524
AES(9)	40	40	637.6839	0.0393
IDEA(10)	80	80	1275.4	0.0197

Table 1 shows the comparative results analysis of the proposed technique and the relative ones.

Figure 3 shows the throughputs of the techniques used for encryption-decryption.

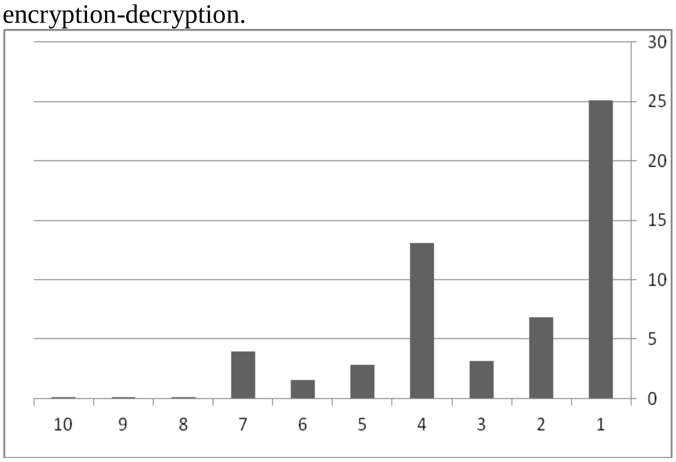

Figure 3: Throughput

From figure 3 we can see that the proposed technique has the highest throughput, thus more efficient comparing with any other technique.

2. Speedup: Speedup means how many time the proposed technique faster than any other related technique and it is calculated as follows:

Speedup= encryption time of related technique/encryption time of proposed technique.

A 256*256 color image was selected, encrypted decrypted using the proposed method and the related ones. The encryption-decryption time was obtained by implementing a matlab code, the results of implementation are shown in table 1.

Here I will notice that the differences between the encryption time and decryption time is due to calculating inverse matrix during the decryption phase.

The speed up was calculated and as shown in table 1 the proposed technique has the falsest speed.

Figure 4 shows the speedup of the proposed technique comparing with each related technique(here we omit the last three ones because they are very slow)

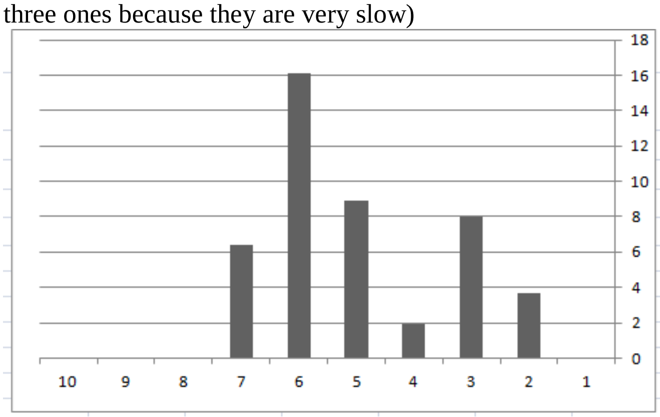

Figure 4: Speedup of proposed technique compared to related technique

Conclusions

A new technique for color image encryption decryption was proposed, implemented and tested. Experimental results showed that the proposed method was very secure and it gave a high performance.

Speedup and throughput for the proposed technique and the related ones were calculated and it was shown that the proposed technique has the highest throughput and highest speed of encryption-decryption.

ISSN:2319-7900

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] G.A Sathishkumar, K.Bhoopathy and R.Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps", I*nternational Journal of Network Security & its Applications*, Vol.3, No.2, 2011, pp. 181-194.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] Shao Liping, Qin Zheng, Qin Jun, and Li Huan, "Image Scrambling Algorithm Based on Random Shuffling Strategy", *IEEE International Conference on Industrial Electronics and Applications*, Singapore, 3-5 June 2008, pp.2278-2283.

JIHAD N. ABDEL-JALIL received his B.S. degrees in Electronic Computer Complexes & Networks from Moscow state university of communications means, Russia, in 1994, and the Ph.D. degree in computer engineering from Kursk State Technical University of Kursk, Russia, in 2006. His research interests include computer networks and routing.