Classification of Matrix Multiplication Methods Used to Encrypt-decrypt Color Image

Jihad Nadir, Ziad Alqadi* and Ashraf Abu Ein
Computer Engineering Department
Albalqa Applied University
Amman - Jordan
*Email: natalia_maw [AT] yahoo.com

Abstract—**The digital color images are the most important types of data is now circulating on the Internet, so the protection and security of the image transition has the top priorities of the computer experts. Many researcher had developed diffident techniques to increase the security of image transmission and most of these techniques suffer from the slow of the encryption - decryption process , In this paper we will produce a classification of the most popular encryption-decryption techniques and suggest the most efficient one, the suggestion will based in many factors such as speedup, throughput, encryption-decryption error and the hacking factor.**

Keywords*: *Encryption, decryption, speedup, throughput, hacking.

I. INTRODUCTION

Encryption is defined as the conversion of plain message(matrix which represents digital color image) into a form called a cipher text that cannot be read by any people without decrypting the encrypted text [15]. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be

read [15] . Color image encryption is to be done before transition the image and it has to be done securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, transmission, medical imaging .Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption techniques are very useful tools to protect secret information[3].

Encryption of data [16] has become an important way to protect data resources especially on the internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources[16].

II. RELATED WORKS

Guodong Ye [9] have presented an efficient image encryption algorithm 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*. [5] have presented an algorithm 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*. [17] 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.* [9] 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*. [18] 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*. [19]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.* [20] 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. [21] introduced a 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 [11]. 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 [13].

Rizvi *et al.* [12] 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*. [21] 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*. [14] 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.* [4] 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 [4] proposed a novel image encryption approach using matrix reordering this approach was tested and some comparisons with other techniques were done.

Ziad A. Alqadi and others in[1] and [2] have presented a technique using direct and inverse conversions to convert a color image to gray image and vice versa, this technique can be useful to be used in color image encryption decryption.

III. PROPPED METHODS

A. First method(proposed 1):Using each of the components of the color image

This method for encryption can be implemented in the following steps:

1. Get the original color image.
2. Extract the red, green, and blue matrices from the original color image(each of them is 2 dimensional matrix),
3. Reshape each matrix in step 2 to square matrix.
4. Generate one random square matrix for each component to be used as a private key.
5. Encrypt each component by applying matrix multiplication of the matrix component and it's private key.
6. Reshape each encrypted matrix to it's original size.
7. Form the encrypted color image.

The decryption phase can by implemented applying the following steps:

1. Get the decrypted color image.
2. Extract the red, green, and blue matrices from the original color image(each of them is 2 dimensional matrix),
3. Reshape each matrix in step 2 to square matrix.
4. Use each private key
5. Decrypt each component by applying matrix multiplication of the matrix component and the inverse it's private key.
6. Reshape each decrypted matrix to it's original size.
7. Form the decrypted color image.

The following matlab code was written to implement this method

```
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)
imhist(a(:,:,3)), title 'Blue component histogram'
tic
b1=a(:,:,1);
b2=a(:,:,2);
b3=a(:,:,3);
b1=reshape(b1,200*300,1);
b2=reshape(b2,200*300,1);
b3=reshape(b3,200*300,1);
for i=60001:60025
   b1(i,1)=0;
   b2(i,1)=0;
   b3(i,1)=0;
end
```

```
c1=reshape(b1,245,245);
c2=reshape(b2,245,245);
c3=reshape(b3,245,245);
k1=rand(245,245);
k2=rand(245,245);
k3=rand(245,245);
c1=double(c1);
c2=double(c2);
c3=double(c3);
e1=c1*k1;
e2=c2*k2;
e3=c3*k3;
toc
tic
d1=e1*inv(k1);
d2=e2*inv(k2);
d3=e3*inv(k3);
d11=reshape(d1,245*245,1);
d12=reshape(d2,245*245,1);
d13=reshape(d3,245*245,1);
for i=1:60000
   d21(i,1)=d11(i,1);
   d22(i,1)=d12(i,1);
   d23(i,1)=d13(i,1);
end
d31=uint8(d21);
d32=uint8(d22);
d33=uint8(d23);
d41=reshape(d31,200,300);
d42=reshape(d32,200,300);
d43=reshape(d33,200,300);
d4(:,:,1)=d41;
d4(:,:,2)=d42;
d4(:,:,3)=d43;
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'
```

B. Second method(proposed 1):Converting color image to 2 dimensional matrix

The encryption phase here is consisted of 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.

The following matlab code was written to implement this method

```
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)
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'
```

C. Third method(proposed 1):Converting color image to Gray image

This method can be implemented as first method but the color image is is to converted to gray image using direct conversion proposed by the author in [1], then the gray image can be encrypted as in method 1, after that the encrypted gray image can be decrypted and converted to color image using the inverse conversion mentioned in[1].

IV. EXPERIMENTAL RESULTS

The proposed methods were implemented several times using different color images with different sizes and the results always give a correlation coefficient equal 1 between the original image and the decrypted one, which means that the methods are 100% correct and do not lead to any damage of information, figure 1 and 2 show the original image and the decrypted one with the histogram of each component of the color image.

The proposed method are also very secure and it is implausible to hack the image because the private key has the following features:

- Private key is a 2 dimensional matrix with a huge size.
- Each element in the private key is a random double number which make it impossible to guess.

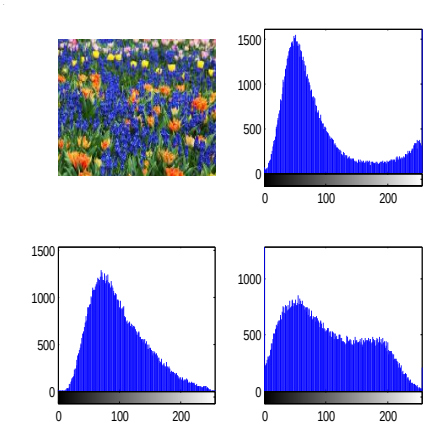

Figure 1: sample of the original color image

The encryption and decryption times were calculated and compared with other methods mentioned in the related works, these results are listed in table 1. 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 color image size by the total time.

For clarity we can represent the data in table 1 by figure 3 and 4.

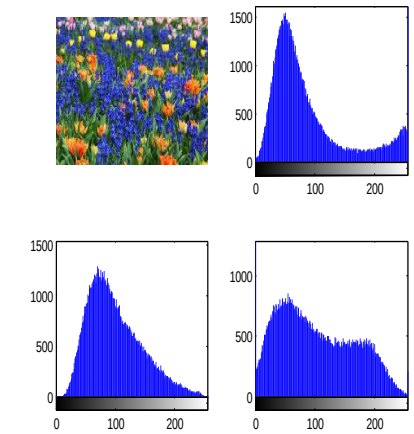

Figure 2:Decrypted color image.

Table 1: Comparisons results

Method	Direct conversion time(s)	Inverse conversion time(s)	Encryption time(s)	Decryption time(s)	Total time (s)	Speed up	Throughput(MB/s)
Proposed 1	0	0	0.006207	0.067798	0.0740	1	21.2549
Proposed 2	0	0	0.027985	0.156311	0.1843	2.4905	8.5343
Ref[1] HSI	0.078	0.032	0.02032	0.02541	0.1557	2.1041	10.1019
REF[1]R'G'B'	0.015	0.015	0.02032	0.02541	0.0757	1.0230	20.7776
Ref.[4]	0	0	0.23	0.23	0.46	6.2162	3.4193
Ref.[5]	0	0	0.5	0.5	1.0	13.5135	1.5729
Ref.[6]	0	0	0.12	0.12	0.24	3.2432	6.5536
Ref.[7], (A-I)	0	0	0.56	0.56	1.12	15.1351	1.4043
Ref.[7],(A-II)	0	0	1.01	1.01	2.02	27.2973	0.7786
Ref.[8]	0	0	0.4	0.4	0.8	10.8108	1.9661

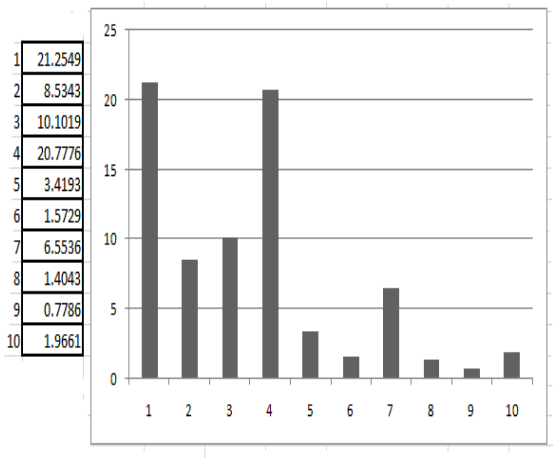

Figure 3: Methods throughput

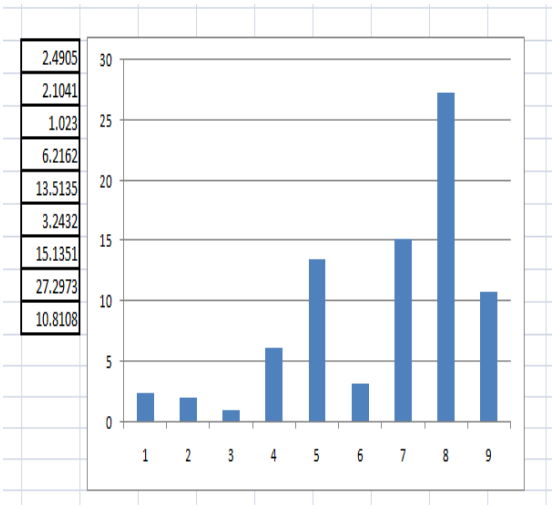

Figure 4: Speedup of the method reference to proposal 1

From the above results we can see that the proposal method 1 has the best efficiency.

V. CONCLUSIONS

A methods of encryption-decryption of color image were proposed and a survey analysis was done and it was shown that proposed 1 method has the best performance because it characterized with following features:

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

REFERENCES

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