Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 12, Issue. 12, December 2023, pg.01 – 12

Mixed Chaotic Keys to Protect Digital Color Image

Prof. Ziad Alqadi; Prof. Akram Mustafa
Albalqa Applied University; Al Albayt University
Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2023.v12i12.001

Abstract:
A high speed and highly secure method of image cryptography will be introduced. The introduced method will decrease the encryption time and increase the throughput of image cryptography, and it will have a significant speed up comparing with other existing methods of data cryptography. The introduced method will use a complicated private key, which will provide a huge key space to resist hacking attacks, and the generated images will be very sensitive to the selected values of the private key. The private key will use two chaotic logistic map models and one chaotic tent map model to generate three 2D chaotic keys, these keys will be converted to integers and resized to match the size of the image.
The quality of the proposed method will be tested to insure that the introduced method will always produce an encrypted image with low quality and a decrypted image with high quality, the quality parameters calculated between the source images and the encrypted and decrypted images will be calculated to prove that the method will satisfy the quality requirements of good cryptography.

Keywords: Cryptography, DCI, PK, CK, SK, CTMM, CLMM, Throughput, speed up, quality, sensitivity**.**

Introduction
Digital color image (DCI) [25-30] is a big number of pixels arranged in a 3D matrix as shown in figure 1 (one channel or 2D matrix for each color: red, green and blue) [31-36]. Each of these channels can be separately extracted and treated alone [1-10].

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

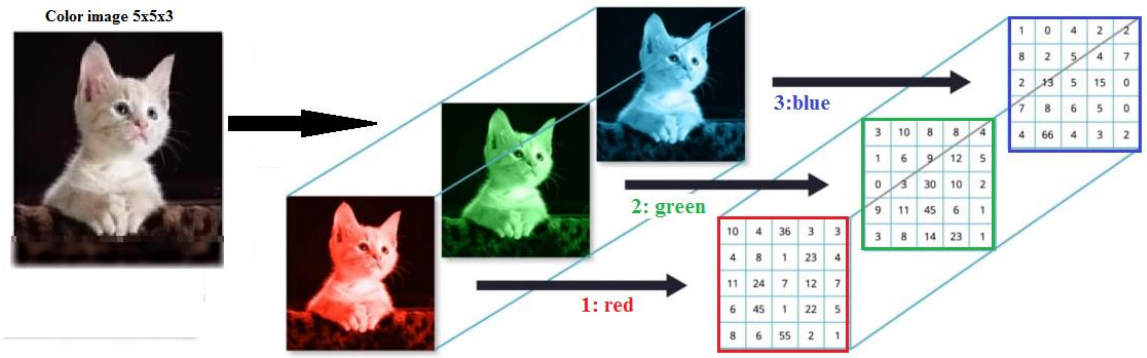

Figure 1: DCI color channels

DCI are used in many computer applications and they are transmitted via communication environments [37-42], thus they require high protection for many reasons such as: DCI may be secret, DCI may be private, DCI may hold secret information and used as a stego image, and the communication environment may be not safe [43-52]. DCI cryptography is one of the easiest techniques used to protect images [10-15].

Cryptography means encrypting the image before sending by converting it to a corrupted damaged image see figure 2, and decrypting the encrypted image after receiving by converting the damaged image to a clear image, which is identical to the source image[16-20].

Crypto system as shown in figure 3 contains encryption function (EF) and decryption function (DF), EF uses the private key (PK) to treat the source image to produce the encrypted image, while the DF uses the same PK to treat the encrypted image to produce the decrypted image[21-24].

A good crypto system must satisfy the quality requirements by producing an encrypted image with low quality and by producing a decrypted image with excellent quality, the quality parameters measured between the source DCI and between each of the encrypted and decrypted images must satisfy the quality requirements listed in table 1 [52-57]:

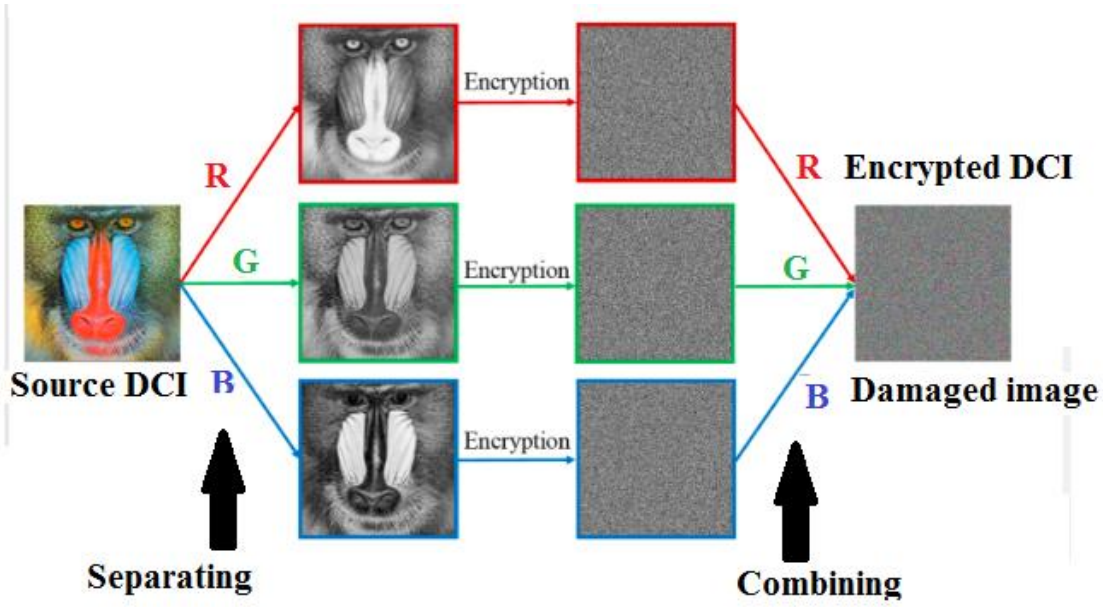

Figure 2: Damaged encrypted image

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

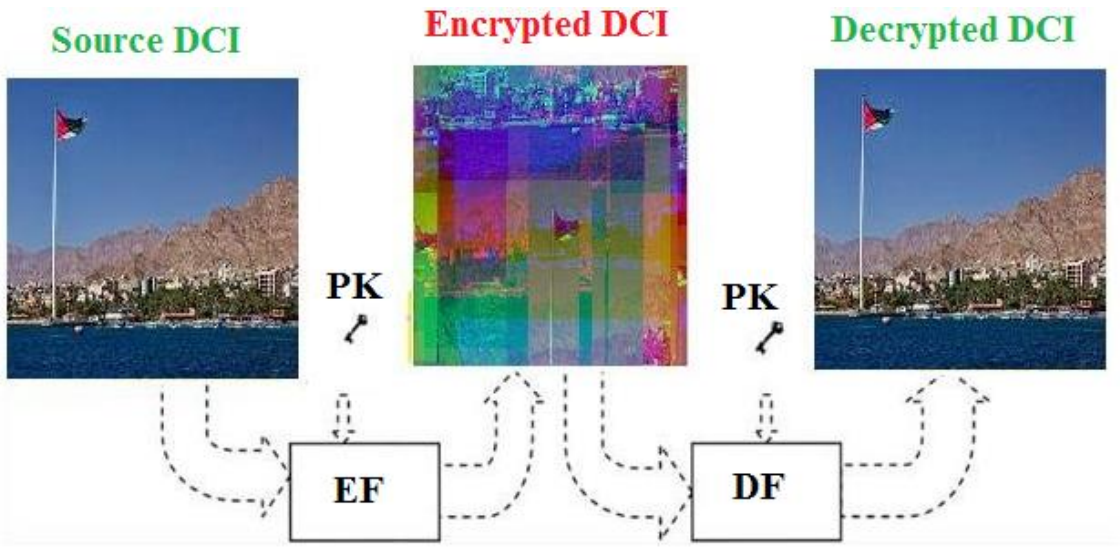

Figure 3: Crypto system diagram

Table 1: Quality requirements using quality parameters [12-20]

Quality parameter	Calculated between source and encrypted DCIs	Calculated between source and Decrypted DCIs
Mean square error (MSE)	High	Zero
Peak signal to noise ratio (PSNR)	Low	Infinity
Correlation coefficient (CC)	Low	One
Number of samples change rate (NSCR)	High	Zero

Many methods were proposed for data cryptography, a lot of these methods were based on the standard methods of data cryptography such as DES, 3DES, AES and blowfish (BF) methods. These methods share some features such as [24-34]:

- They provide good quality requirements.
- Good speed of cryptography when dealing with small data size such as short messages.
- Fixed and small length of data blocks size.
- Fixed length of PK.
- Fixed number of rounds.
- Required secret key for each round.
- Some of these methods are not secure.

Some authors tried to enhance the speed of data cryptography by producing chaotic and non chaotic methods of data cryptography, the proposed method will be compared with these method to show how the proposed method will improve the speed of DCI cryptography by decreasing the encryption time (ET) and increasing the throughput (TP) of DCI cryptography, table 2 shows the speed parameters of some of the proposed methods by variant authors.

Table 2: TP of some of the introduced methods

Method	Average throughput (K bytes per second)
Non-chaotic 18]	170.3906
Chaotic [18]	141.2305
Hyper chaotic [18]	636.3379
Introduced in [19]	888.8867
Introduced in [20]	911.0352
Introduced in [21]	638.4082

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

Introduced in [22]	360.4102
Introduced in [23]	384.9609

The aim of this paper research is to introduce a new method of DCI cryptography which satisfies the following:

- Increasing the level of security by using a complicated PK which will provide a huge key space capable to resist hacking attacks.
- Producing an encrypted image with low quality.
- Producing a decrypted image with excellent quality.
- Increasing the speed of image cryptography by decreasing ET and increasing TP.
- Simplifying both the EF and DF.

The Proposed Method

The proposed method as shown in figure 4 extracts the color channels [42-50] and each color 2D matrix is encrypted-decrypted using its own generated secret key. Two kinds of chaotic maps are used to generate the secret keys [57]. The first and the third keys are generated by running two chaotic logistic map models (CLMM) and the second key is generated by running chaotic tent map model (CTMM), the parameters of these chaotic models are included in the PK [50-57].

The PK will have a complicated structure shown in table 3, this structure will provide a huge key space making the method secure and making the hacking process impossible [45-49].

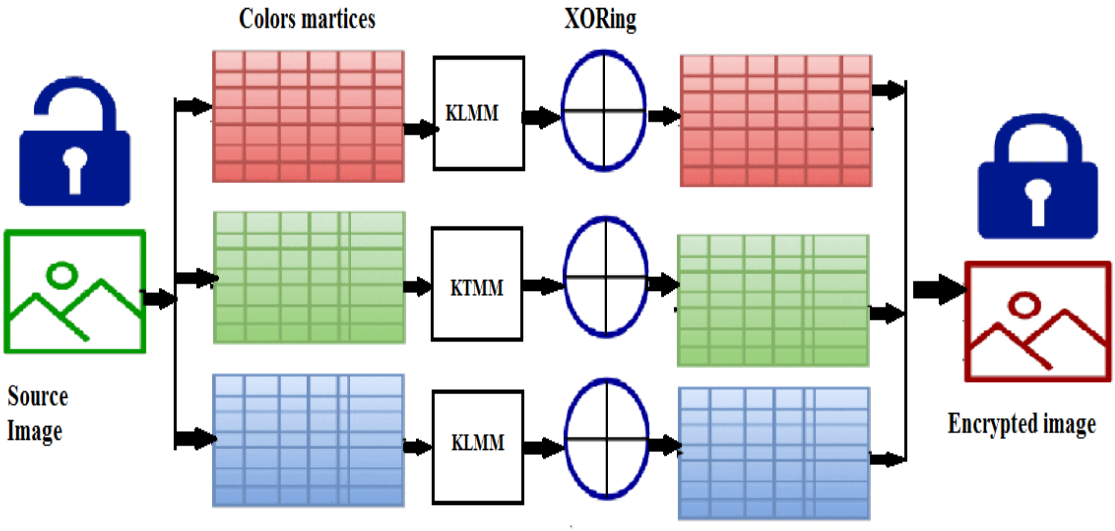

Figure 4: Proposed method diagram

Table 3: PK structure

Two CLMM parameters			
r1	**x1**	**R1**	**C1**
r2	**x2**	**R2**	**C2**
CTMM parameters			
A	**B and C**	**R3**	**C3**
Example			
3.77	0.15	45	75
3.82	0.11	19	70
0.95	0.77. 0.11	40	82

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

Each parameter (13 parameters) of the PK has a double data type, thus the key space provided by the proposed method will be calculated using equation 1:

$$\text{Key space} = 2^{13x64} = 2^{832} \text{ combimnations} \quad (1)$$

This key space will resist any hacking attempt.
The secret key generation will be implemented using a simple sequence of operations; the obtained 2D keys will be resized to match the dimensions of the image color matrix.
Below is a simple matlab sequence to generate a key using CLMM and CTMM:

```
%Using CLMM
for i=1:R1
   for j=1:C1
x2=r2*x2*(1-x2);
ck2(i,j)=x2;
   end
end
key22=uint8(255*ck2);
%Using CTMM
for i=1:R3
   ck(1)=A-B*C;
   for j=2:C3
    ck(j)=A-(B*abs(ck(j-1)));
   end
   ck44(i,:)=ck(:);
   B=B+0.005;
end
key44=uint8(255*ck44)
```

The generated keys are very sensitive to the selected values of the PK parameters, any minor changes in the PK will cause producing different key and thus the results of the encryption-decryption process will be affected.

The encryption function of the proposed method will be implemented applying the following steps:
Step 1:
Initialization:

1) Get the image
2) Retrieve the image size.
3) Extract the image color matrices.
4) Get the PK.

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

This step can be implemented applying the following sequence of mat lab operations:

```
%Image information
a1=imread('C:\Users\win 7\Desktop\Lena.jpg');
 [n1 n2 n3]=size(a1);Lm=n1*n2*n3;
%Color matrices extraction
a1r=a1(:,:,1);
a1g=a1(:,:,2);
a1b=a1(:,:,3);
%PK parameters values
r1=3.77;x1=0.15;R1=50;C1=20;
r2=3.67;x2=0.1;R2=29;C2=42;
r3=3.77;x3=0.15;R3=50;C3=20;
r2=3.67;x2=0.1;R3=69;C3=29;
A=0.95;B=0.77;C=0.11;R4=44;C4=15;
```

Step 2:

Secret key generation:

1) Run CLMM to get the secret key for the red color.
2) Run CTMM to get the secret key for the green color.
3) Run CLMM to get the secret key for the blue color.
4) Convert the keys to integers.
5) Resize the keys to match the size of the color image matrix.

This step can be implemented applying the following sequence of mat lab operations:

```
for i=1:R1
   for j=1:C1
x1=r1*x1*(1-x1);
ck1(i,j)=x1;
   end
end
key11=uint8(255*ck1);
for i=1:R2
   for j=1:C2
x2=r2*x2*(1-x2);
ck2(i,j)=x2;
   end
end
key22=uint8(255*ck2);
for i=1:R3
   ck(1)=A-B*C;
   for j=2:C3
    ck(j)=A-(B*abs(ck(j-1)));
   end
   ck44(i,:)=ck(:);
   B=B+0.005;
end
key44=uint8(255*ck44);
key1=imresize(key11,[n1 n2]);
key2=imresize(key22,[n1 n2]);
key3=imresize(key44,[n1 n2]);
```

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

Step 3:
Encryption:

1) XOR red color with key1.
2) XOR green color with key2.
3) XOR blue color with key 3.

This step can be implemented applying the following sequence of mat lab operations:

```
e(:,:,1)=bitxor(a1r,key1);
e(:,:,2)=bitxor(a1g,key2);
e(:,:,3)=bitxor(a1b,key3);
```

The decryption function can be implemented applying the same steps using the encrypted image as an input image.

Implementation and Results Discussion

The proposed method can be easily used to encrypt-decrypt DCI and gray images, the proposed method satisfied a good quality, the encrypted image was always damaged, while the decrypted image was always identical to the source image. Figure 5 and 6 shows some sample outputs of the proposed method execution, the obtained outputs here proved that the method satisfied the quality requirements; the gray image was XORed by the three keys:

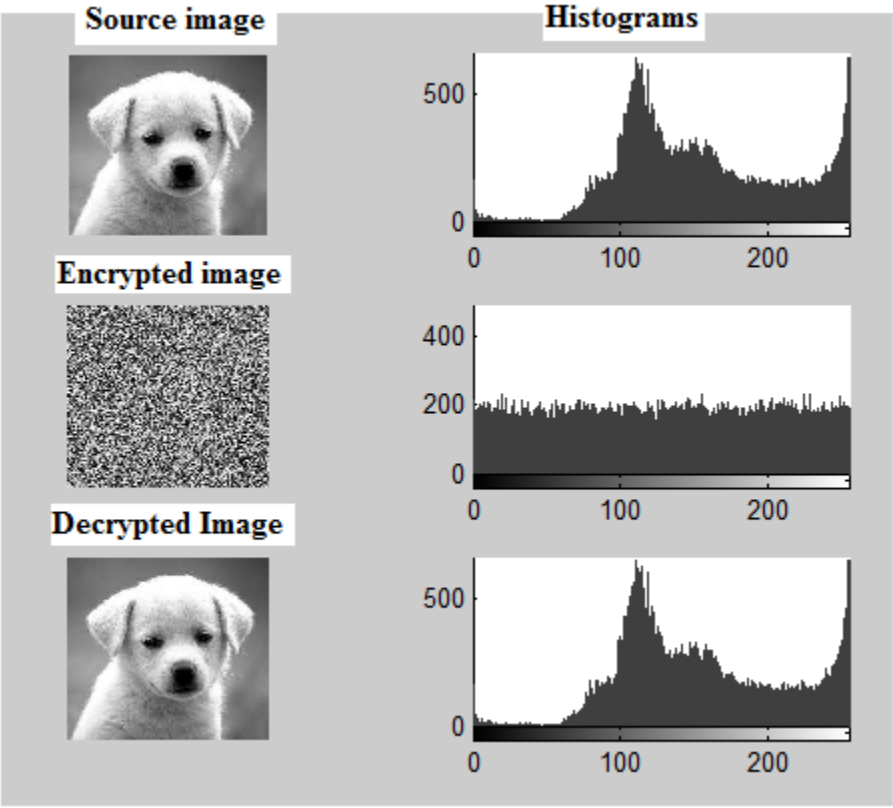

Figure 5: Encrypted and decrypted gray images samples

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

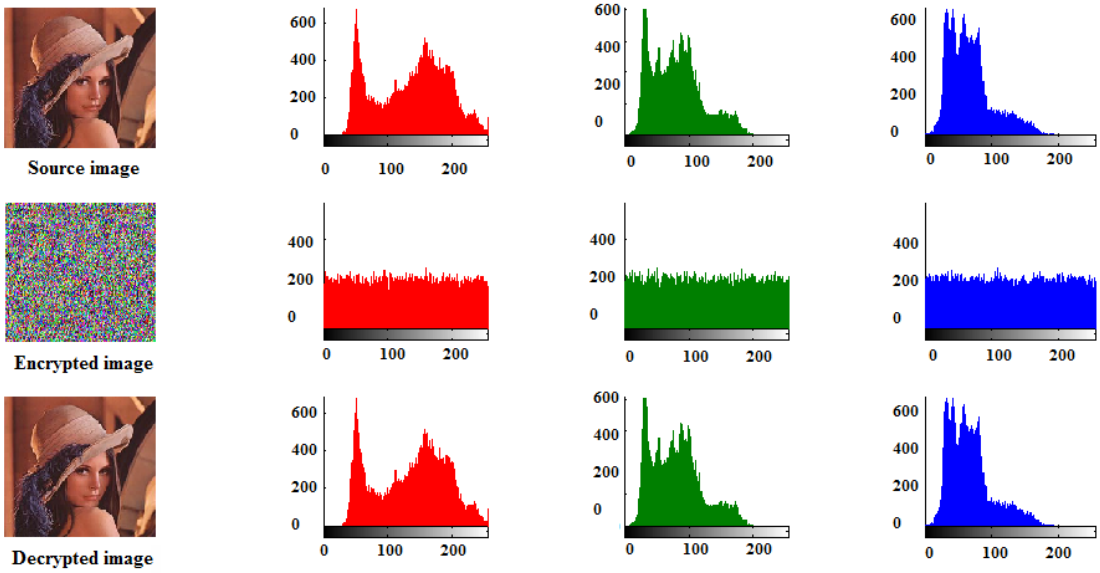

Figure 6: Encrypted and decrypted color images samples

The quality parameters calculated between the source and the decrypted images were always satisfy the quality requirements, the obtained values of the quality parameters calculated between the source and the encrypted images, which are shown in table 4 prove the fact that the proposed method satisfied the quality requirements or good crypto system:

Table 4: Quality parameters calculated between the source and the encrypted images

Image	Size (byte)	MSE	PSNR	CC	NSCR
1	77976	20160	11.7107	-0.2029	100
2	150849	16303	13.8342	-0.3215	100
3	172800	11657	17.1882	-0.1954	100
4	518400	15332	14.4483	-0.2244	100
5	1890000	14716	14.8583	-0.2959	100
6	4326210	11756	17.1043	-0.2373	100
7	5140800	11547	17.2836	-0.1856	100
8	6119256	8870.5	19.9204	-0.1428	100
Remarks		High	Low	Low	High
Satisfy quality requirements of Good crypto system					

The speed of the proposed method was tested, several images were selected and treated using the proposed method, ET and TP were calculated and table 5 shows the obtained speed results.

Table 5: Speed results

Image	Image size(byte)	ET(second)	TP(K bytes per second)
1	77976	0.0450	16662
2	150849	0.0470	30861
3	172800	0.0470	35352
4	518400	0.0480	103850
5	1890000	0.0540	336540
6	4326210	0.0640	649970
7	5140800	0.0660	748950
8	6119256	0.0910	646580
Average			321100

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

From table 5 we can see that the proposed method provides a good speed, the TP of the proposed method was compared with other methods TPs, and as a result of comparisons the proposed method provides a significant speed up (see table 6), the proposed method increases the TP of crypto process making it faster.

Table 6: TP comparisons

Method	Average throughput (K bytes per second)	Speed up of the proposed method (times faster)
Proposed method	321100	1
Non-chaotic 18]	170.3906	1884.5
Chaotic [18]	141.2305	2273.6
Hyper chaotic [18]	636.3379	504.6
Introduced in [19]	888.8867	361.2
Introduced in [20]	911.0352	352.5
Introduced in [21]	638.4082	503.0
Introduced in [22]	360.4102	890.9
Introduced in [23]	384.9609	834.1

The proposed method is very sensitive to the selected values of the PK, any changes in the PK in the decryption function will produce a damaged decrypted image, and it will be considered as a hacking attempt, to show this fact an image was encrypted using PK1 from the following list, the encrypted image was decrypted using each of PK1 and PK2, as shown in figure 7 changing the PK in the decryption function produced a damaged decrypted image, which means that the method is sensitive to the selected PK.

PK1:
r1=3.77;x1=0.15;R1=50;C1=20;
r2=3.67;x2=0.1;R2=29;C2=42;
r3=3.77;x3=0.15;R3=50;C3=20;
r2=3.67;x2=0.1;R3=69;C3=29;
A=0.95;B=0.77;C=0.11;R4=44;C4=15;
PK2:
r1=3.66;x1=0.15;R1=50;C1=20;
r2=3.67;x2=0.1;R2=29;C2=42;
r3=3.77;x3=0.15;R3=50;C3=20;
r2=3.67;x2=0.1;R3=69;C3=29;
A=0.95;B=0.77;C=0.11;R4=44;C4=15;

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

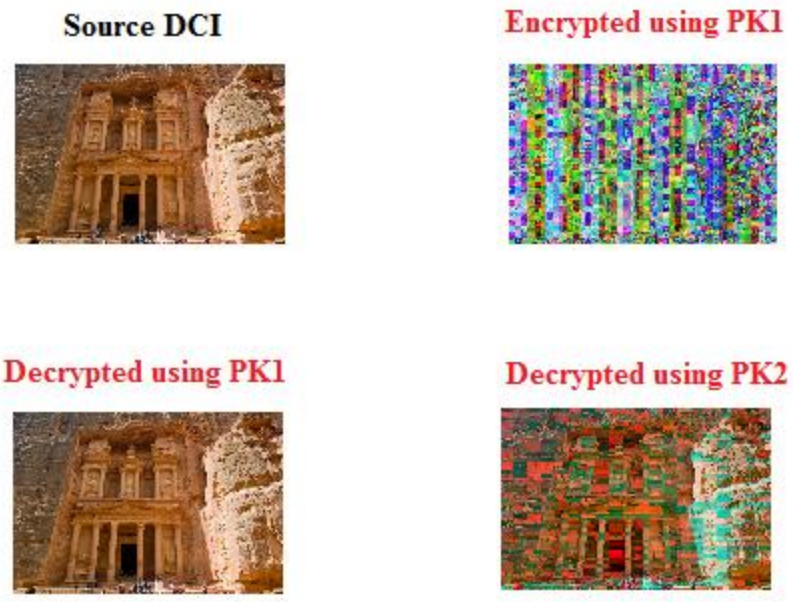

Figure 7: Method sensitivity

Conclusion

A simplified and highly secure method of image cryptography was proposed, the method used a complicated PK to protect the image, the PK contains the parameters of two CLMMs and the parameters of CTMM, these parameters were to generate 3 2Ds chaotic keys, which were converted to keys of integers and resized to match the dimensions of the color image channels. Each color matrix was XORed with one key to apply image encryption-decryption, the PK provided a huge key space and the obtained images were very sensitive to the selected value of the PK parameters. The encryption and decryption functions were simplified and they were used to encrypt-decrypt any image with any size and any type (color or gray image).

The quality of the proposed method was examined and it was shown that the proposed method always gave an encrypted image with low quality and a decrypted image with high quality, the quality parameters were calculated and the obtained quality parameters results showed that the proposed method satisfied the quality requirements of good crypto system.

He speed of the proposed method was tested, for the selected images the encryption time and the throughput of data cryptography were calculated, the obtained speed results showed that the proposed method provided a good speed and it speeded up the process of image cryptography by increasing the throughput of image cryptography.

References

[1]. Rashad J Rasras, Mutaz Rasmi Abu Sara, Ziad Alqadi, Enhanced Efficiency and Security in LSB2 Steganography: Burst Embedding and Private Key Integration, Traitement du Signal, vol. 40, issue 5, 2023.

[2]. Mua'ad Abu-Faraj, Abeer Al-Hyari, Charlie Obimbo, Khaled Aldebei, Ismail Altaharwa, Ziad Alqadi, Orabe Al manaseer, Protecting digital images using keys enhanced by 2D chaotic logistic maps, Cryptography, vol. 7, issue 2, 2023.

[3]. Prof. Ziad Alqadi, Improved and Secure LSB2 of Message Steganography, International Journal of Computer Science and Mobile Computing, vol.12, issue 11, 2023.

[4]. Prof. Ziad Alqadi, Hybrid, Secure and Highly Speed Method for Color Image Cryptography, International Journal of Computer Science and Mobile Computing, vol. 12, issue 9, 2023.

[5]. Adnan Manasreh, Nasser Abdellatif, Ziad A. Alqadi, SPEECH FILES CRYPTOGRAPHY USING IMAGE KEY AND INDICES KEY, ARPN Journal of Engineering and Applied Science, vol. 18, issue 13, 2023.

[6]. Ziad Alqadi, Mohammad Sleman Khrisat, Analysis of Methods used to Create Digital Signals Fingerprints, International Journal of Computer Science and Mobile Computing, vol. 12, issue 8, 2023.

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

[7]. Prof. Ziad Alqadi, Comparative Analysis of using SIK for Message Cryptography, International Journal of Computer Science and Mobile Computing, vol.12, issue 8, 2023.
[8]. Mohamad Al-Laham, Mohammad Al-Ma'aitah, Ziad Alqad, A Simple and Stable Method of Creating Fingerprint Features With Image Rotation, The International Arab Journal of Information Technology, vol. 20, issue 4, 2023.
[9]. Ziad A. Alqadi Nasser Abdellatif , Adnan Manasreh , Mohammad S. Khrisat , Hatim Ghazi Zaini, MULTIPLE ROUNDS USING MIXED CHAOTIC KEYS METHOD FOR SECURE MESSAGE CRYPTOGRAPHY, ARPN Journal of Engineering and Applied Science, vol. 18, issue 8, 2023.
[10]. Ziad Alqadi, Simplified and Improved LSB2 (SILSB2) Method of Secret Message Steganography, International Journal of Computer Science and Mobile Computing, vol. 12, issue 5, 2023.
[11]. Nasser Abdellatif and Ziad A. Alqadi Adnan Manasreh, SECURING LSB STEGANOGRAPHY USING BITE SUBSTITUTION AND IMAGE BLOCKING, ARPN Journal of Engineering and Applied Science, vol. 18, issue 7, 2023.
[12]. Prof. Ziad AlQadi, Complex CLMM Private Keys to Secure Digital Color Images, International Journal of Computer Science and Mobile Computing, vol. 12, issue 5, 2023.
[13]. Prof. Ziad Alqadi; Mohammad Al-Raqqad, Securing Message Steganography by using Modified LSB Method, International Journal of Computer Science and Mobile Computing, vol. 12, issue 4, 2023.
[14]. Ziad Alqadi, Mohammad Al-Raqqad, Simple and Efficient Chaotic Based Method of Message Cryptography, International Journal of Computer Science and Mobile Computing, vol. 12, issue 4, 2023.
[15]. Prof. Ziad Alqadi, Multiple Blocks, Multiple Rounds Method for Image Cryptography, International Journal of Computer Science and Mobile Computing, vol. 12, issue 4, 2023.
[16]. Akram Naser Adam Mousa, Talal Bukewitin, Amna MM Salem, Ziad Alqadi, Triple Rounds to Protect Text Files, International Journal of Computer Science and Mobile Computing, vol. 12, issue 4, 2023.
[17]. M Khrisat, Ziad Alqadi, Performance evaluation of ANN models for prediction, Acadlore Trans. Mach. Learn, vol. 2, issue 1, 2023.
[18]. M. Bala Kumara, P. Karthikkab , N. Dhivyac , T. Gopalakrishnan, A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014.
[19]. Lee Mariel Heucheun Yepdia, Alain Tiedeu, and Guillaume Kom, A Robust and Fast Image Encryption Scheme Based on a Mixing Technique, Security and Communication Networks, Volume 2021 |Article ID 6615708 | https://doi.org/10.1155/2021/6615708.
[20]. Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," Information Sciences, vol. 480, pp. 403–419, 2019.
[21]. M. Asgari-chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," Signal Processing, vol. 157, p. 1, 2019.
[22]. X. Zhang and X. Wang, Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System, Springer, New York, NY, USA, 2019.
[23]. J. S. Zhenjun and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," Optics and Lasers in Engineering, vol. 80, pp. 1–11, 2016.
[24]. Kaur, R. Dhir, & G. Sikka,"A new image steganography based on first component alteration technique", International Journal of Computer Science and Information Security (IJCSIS), 6, pp.53-56, 2009.http://arxiv.org/ftp/arxiv/papers/1001/1001.1972.pdf
[25]. Alvaro Martin, Guillermo Sapiro, &GadielSeroussi,"Is Steganography Natural", IEEE Transactions on Image Processing, 14(12), pp.2040-2050, 2005.doi: 10.1109/TIP.2005.859370
[26]. Bhattacharyya, A. Roy, P. Roy, & T. Kim,"Receiver compatible data hiding in color image", International Journal of Advanced Science and Technology, 6, pp.15-24, 2009.http://www.sersc.org/journals/IJAST/vol6/2.pdf
[27]. EE. KisikChang, J. Changho, & L. Sangjin,"High Quality Perceptual Steganographic Techniques", Springer. 2939, pp.518-531, 2004.doi: 10.1007/978-3-540-24624-4_42, http://www.springerlink.com/content/c6guuj5xnyy4wj3c/
[28]. C. Kessler,"Steganography: Hiding Data within Data" An edited version of this paper with the title "Hiding Data in Data", Windows & .NET Magazine, 2001. [Online] Available: http://www.garykessler.net/library/steganography.html (October 4,2011)
[29]. Gandharba Swain, &S.K.lenka,"Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking. 2(1), pp.35-39, 2010. ISSN: 0975-7163. http://www.serialspublications.com/journals1.asp?jid=436&jtype
[30]. Hideki Noda, MichiharuNimi, &EijiKawaguchi,"High- performance JPEG steganography using Quantization index modulation in DCT domain", Pattern Recognition Letters, 27, pp.455-46, 2006.http://ds.lib.kyutech.ac.jp/dspace/bitstream/10228/450/1/repository6.pdf
[31]. Kathryn,"A Java Steganography Tool", 2005.http://diit.sourceforge.net/files/Proposal.pdf
[32]. Motameni, M.Norouzi, M.Jahandar, & A. Hatami,"Labeling method in Steganography", Proceedings of world academy of science, engineering and technology, 24, pp.349-354, 2007. ISSN 1307-6884. http://www.waset.org/journals/waset/v30/v30-66.pdf
[33]. Mohammed A.F Al Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography", International Journal of Advanced Computer Science and Applications, 3(3): 57-62, 2012.http://www.ijacsa.thesai.org

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

[34]. Mohammed A.F Al Husainy, "Developed Segmented LSB Image Steganography", International Science and Technology Conference (ISTEC 2012), Dubai, December 13-15, 2012. http://www.iste-c.net.
[35]. Rashad J. Rasras1, Mutaz Rasmi Abu Sara2, Ziad A. AlQadi3, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3 ,2019, https://doi.org/10.30534/ijatcse/2019/64832019
[36]. 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 Journal8 (10): 1175-1182, ISSN 1818-4952.
[37]. Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction, Eur. J. Sci. Res., 27: 167-173.
[38]. Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, 2009 ISSN 1549-3636.https://doi.org/10.3844/jcs.2009.250.254
[39]. Musbah J. Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering & Technology, 7(3.13) (2018) 104-107.https://doi.org/10.14419/ijet.v7i3.13.16334
[40]. Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein,A COMPARISON BETWEEN PARALLEL ANDSEGMENTATIONMETHODS USED FOR IMAGE ENCRYPTION-DECRYPTION International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5,October 2016.
[41]. Khaled Matrouk, Abdullah Al- Hasanat, HaithamAlasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi, Analysis of Matrix Multiplication Computational Methods, European Journal of Scientific Research, ISSN 1450-216X / 1450-202X Vol.121 No.3, 2014, pp.258-266.
[42]. Ziad A.A. Alqadi, Musbah Aqel, and Ibrahiem M. M. ElEmary, Performance Analysis and Evaluation ofParallel Matrix Multiplication Algorithms, World Applied Sciences Journal 5 (2): 211-214, 2008.
[43]. Rashad J. Rasras1, Mutaz Rasmi Abu Sara2, Ziad A. AlQadi3, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3 ,2019, https://doi.org/10.30534/ijatcse/2019/64832019
[44]. 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 Journal8 (10): 1175-1182, ISSN 1818-4952.
[45]. Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction, Eur. J. Sci. Res., 27: 167-173.
[46]. Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, Journal of Computer Science 5 (4): 250-254, 2009 ISSN 1549-3636.https://doi.org/10.3844/jcs.2009.250.254
[47]. Musbah J. Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering & Technology, 7(3.13) (2018) 104-107.https://doi.org/10.14419/ijet.v7i3.13.16334
[48]. Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein,A COMPARISON BETWEEN PARALLEL ANDSEGMENTATIONMETHODS USED FOR IMAGE ENCRYPTION-DECRYPTION International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5,October 2016.
[49]. Khaled Matrouk, Abdullah Al- Hasanat, HaithamAlasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi, Analysis of Matrix Multiplication Computational Methods, European Journal of Scientific Research, ISSN 1450-216X / 1450-202X Vol.121 No.3, 2014, pp.258-266.
[50]. Ziad A.A. Alqadi, Musbah Aqel, and Ibrahiem M. M. ElEmary, Performance Analysis and Evaluation ofParallel Matrix Multiplication Algorithms, World Applied Sciences Journal 5 (2): 211-214, 2008.
[51]. Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, 2005.
[52]. Musbah J. Aqel , Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science Vol. 2,No. 4, 2007, pp. 288-298.
[53]. J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Abu-Zaher, A Novel zero-error method to create a secret tag for an image, Journal of Theoretical and Applied Information Technology, Vol. 96. No. 13, pp. 4081-4091, 2018.
[54]. Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.
[55]. Abdullah N Olimat, Ali F Al-Shawabkeh, Ziad A Al-Qadi, Nijad A Al-Najdawi, Ahmed Al-Salaymeh, Experimental study and computational approach prediction on thermal performance of eutectic salt inside a latent heat storage prototype, Thermal Science and Engineering Progress, vol. 37, 2023.
[56]. Abdullah N Olimat, Ali F Al-Shawabkeh, Ziad A Al-Qadi, Nijad A Al-Najdawi, Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence, Case Studies in Thermal Engineering, vol. 38, 2022.
[57]. Ziad Alqadi, Simple and Efficient Chaotic Based Method of Message Cryptography, International Journal of Computer Science and Mobile Computing, vol. 12, issue 4, 2023.

© 2023, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden