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. 13, Issue. 6, June 2024, pg.37 – 49

Three Rounds Cryptography to Protect Secret Message

Prof. Ziad Al Qadi

Al-Balqa Applied University, Faculty of Engineering Technology, Jordan-Amman

DOI: https://doi.org/10.47760/ijcsmc.2024.v13i06.006

Abstract:
A simple three rounds method of message cryptography will be introduced, the message will be encrypted-decrypted by apply XORing operation of the message with the secret KEY1 in the first round, in the second round the message will be shuffled using the secret key KEY2, while in the third round the message binary matrix will be rotated left to a number of selected digits. The introduced method will be very secure it will use a secret kept digital color image as an image_key, this image will be used to generate KEY1 and KEY2. KEY1 will be extracted from the image from a selected position, while KEY2 will be an indices key obtained by sorting a number of bytes extracted from the image from another position determined by the user. In addition to the image_key the method will use the values of POS1, POS2, and NORLD to determine the starting position of key1, the starting position of key2 and the number of rotate left digits. The produced decrypted message will be very sensitive to the selected image_key, POS1, POS2 and NORTD. The encryption function will be simplified and it will be implemented using three simple tasks: XORing, shuffling and rotating left, while the decryption function will be implemented by applying rotate left, shuffling back and XORing operations.
The proposed method will be implemented and tested using various messages, the results will be studied and analyzed to prove the achievements provided by the method in: quality, speed, security and sensitivity.
Keywords: Cryptography, SM, MBM, DCI, image_key, secret keys, shuffling, rotate left, XORing.

Introduction

Secret message (SM) [20-25] is a set of characters arranged in one row matrix, this message can be easily presented by the array of decimals (ASCII values) within the range 0 to 255 [26-30], the message binary matrix (MBM)(see figure 1). MBM is a 2D matrix with 8 columns and one row for each character and each row represents the binary number of the message character [31-35].

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

```
Message='ABCD'
m1=uint8(Message)
m1 =
  65  66  67  68
MBM=dec2bin(m1,8)
MBM =
01000001
01000010
01000011
01000100
```

Figure 1: SM presentation

Digital color image (DCI) [36-40]is a set of color values arranged in 3D matrix (one 2D matrix for each color: red, green and blue) (see figure 2), and it has the following good features [41-50]:

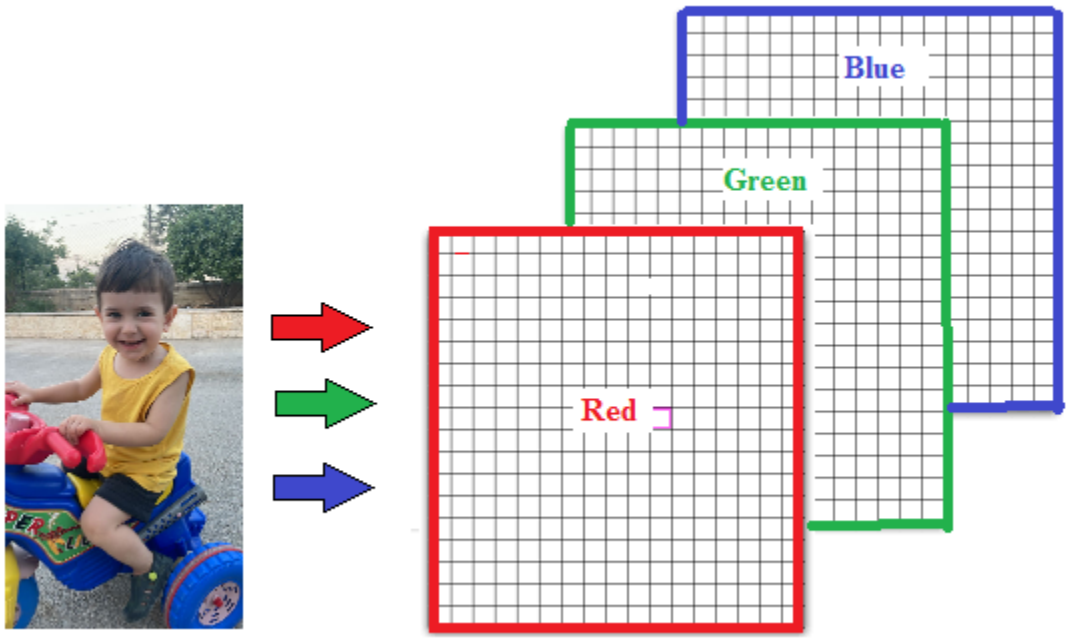

Figure 2: DCI presentation

- The color values are similar to the characters values, the values are unsigned decimal integers and within the range 0 to 255 [51-55].
- Easy to reshape the image matrix to one row matrix [56-60].
- Easy to extract and use any part of the image [61-66].
- Easy to get and store.

DCI can be easily used as an image_key; this key can be used to generate any secret key needed for message cryptography [67-72]. In this paper research the image_key will be used to generate two secret keys, the first key will be used to apply XORing operation, while the second secret key will be used to apply message shuffling operation. The image_key must be kept in secret and from a selected position the required bytes from the image will be extracted to be used to generate the secret keys. Changing the image or and changing the position will lead to change the secret key. Figures 3 and 4 show how the generated keys are sensitive to the selected image_key and the selected position in the reshaped to one row image. Key1 is a set of bytes extracted from the image with length equal SM length, while Key2 is an indices key obtained by sorting the extracted bytes from an image_key [73-78].

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

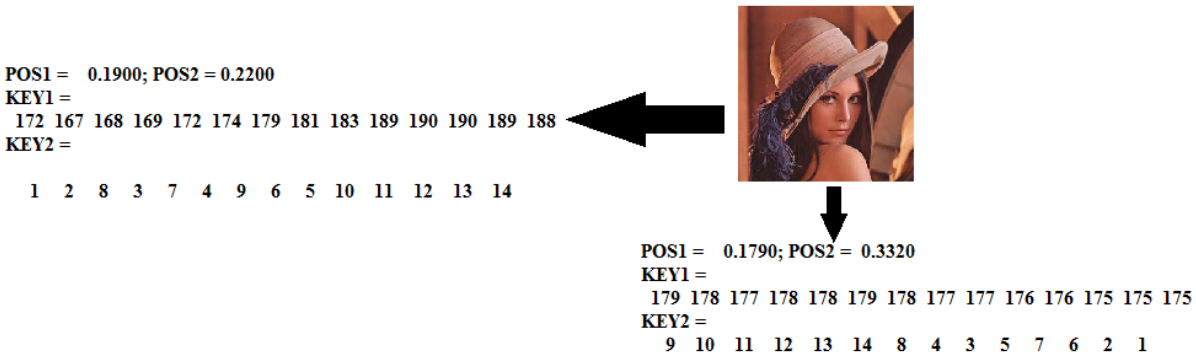

Figure 3: Changing the positions changes the keys

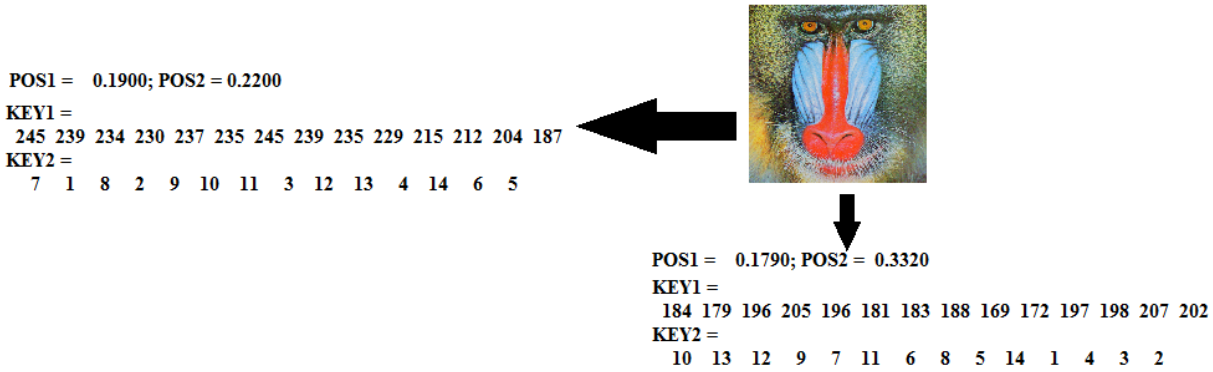

Figure 4: Changing the image_key changes the generated keys

SM cryptography is a simple way to protect secret and private messages, this process is applied by implementing encryption and decryption functions (see figure 5) [1-10].

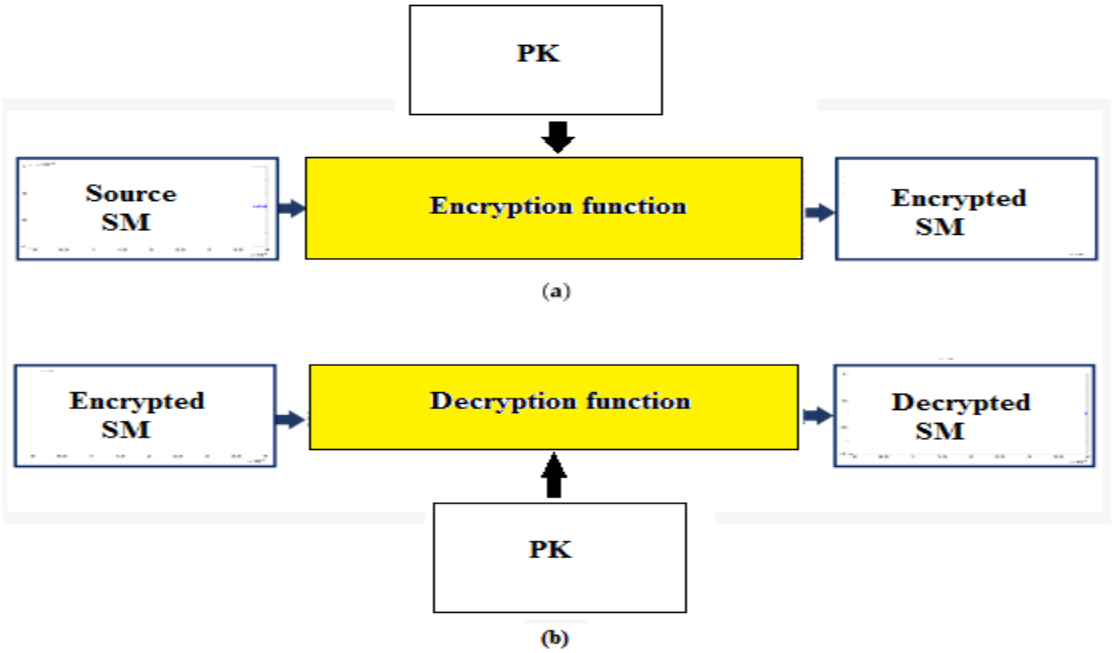

Figure 5: Crypto system diagram

The encryption function processes the SM and the PK to produce a damaged encrypted message, while the decryption function processes the encrypted message and the private key to produce a decrypted identical to source message SM [11-20].

Many method were introduced by various authors, a lot of these methods were based on standard methods of data cryptography DES and AES methods. These methods provide a good quality (see table for quality requirements) and speed, but they share some features, which are considered as a disadvantage, some of these features are [25-30]:

- A lot of rounds are required [77-82].
- Each round requires a secret key generated from the private key [31-35].
- Each round requires a complex of logical operations to apply blocks encryption-decryption.
- Private Key length is fixed and short (For DES method [1-10].
- Message is divided into equal blocks, and block size is fixed.
- Encryption-decryption times increase rapidly when increasing message length.

Table 1: Crypto system quality requirements [41-50]

Quality parameters	Measured between the source and the encrypted SMs	Measured between the source and the decrypted SMs
(Mean square error(MSE)	High	Zero
Peak signal to noise ratio(PSNR)	Low	Infinity
Remarks	Encrypted message must be damaged and unreadable	Decrypted message must be identical to the source message

The Proposed Method

The proposed method provides a high degree of message protection based on a complicated used private key (PK). The PK contains image_key, POS1, POS2 and NORLD. The image_key is used to generate two secret keys: KEY1 and KEY2. KEY1 is used in the first round to apply XORing with the message; this key is to be extracted from a position calculated by using the fractional value of POS1. KEY2 is an indices key generated by sorting an extracted array from the starting from a position calculated by the value of POS2; this key is to be used to shuffle the message in the second round. The NORLD defines the number of rotating left digits; this key is used in round 3 to rotate the MBM rows.

The proposed method is implemented in three rounds, each round will be used to apply one task, these tasks are:

- Message XORing: the message will be XORed with key1, this key will be extracted from the image_key with length equal message length, the starting position of the image bytes will be calculated using the value of POS1, figure 6 shows an example of implementing this task:

Figure 6: XORing task example

- MBM columns shuffling: this operation will be implemented using the second secret key, this key will generated by sorting an extracted bytes from the image_key from a starting position defined by the value of POS2, this key is to

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

be treated as an indices key and it will be used to shuffle the columns in the MBM in the decryption function and shuffle back the columns in the decryption function, figure 7 shows how this task can be implemented:

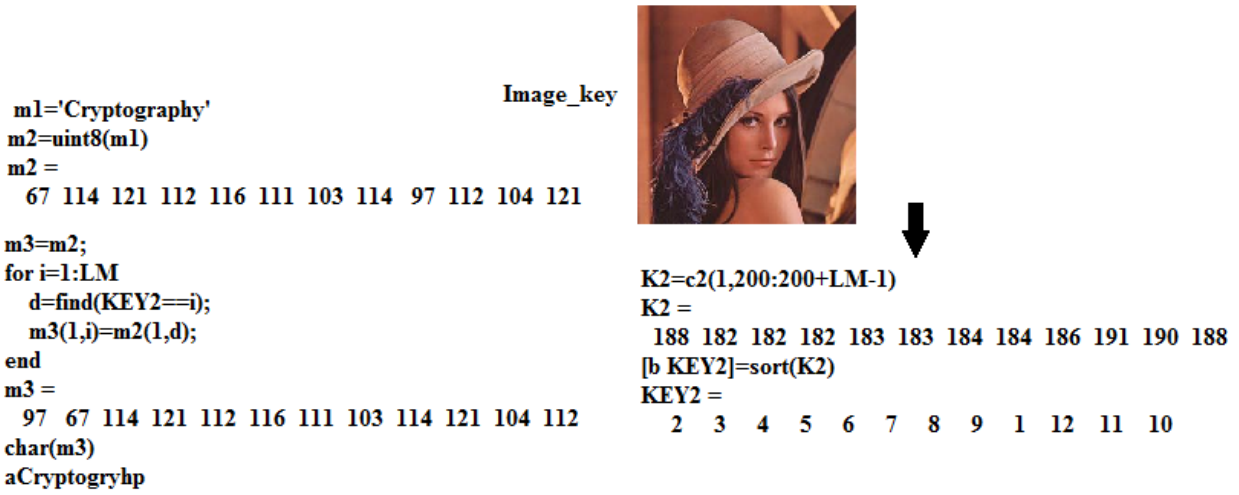

Figure 7: MBM columns shuffling example

- MBM rotating left task, this task will be implemented to rotate left each row in the MBM for a selected number of digits, figure 8 shows an example of implementing this task (in the encryption function the row of MBM will be rotated left to a number of digits equal the value of NORLD, while in the decryption function the rotating number will be equal NORLD subtracted from 8).

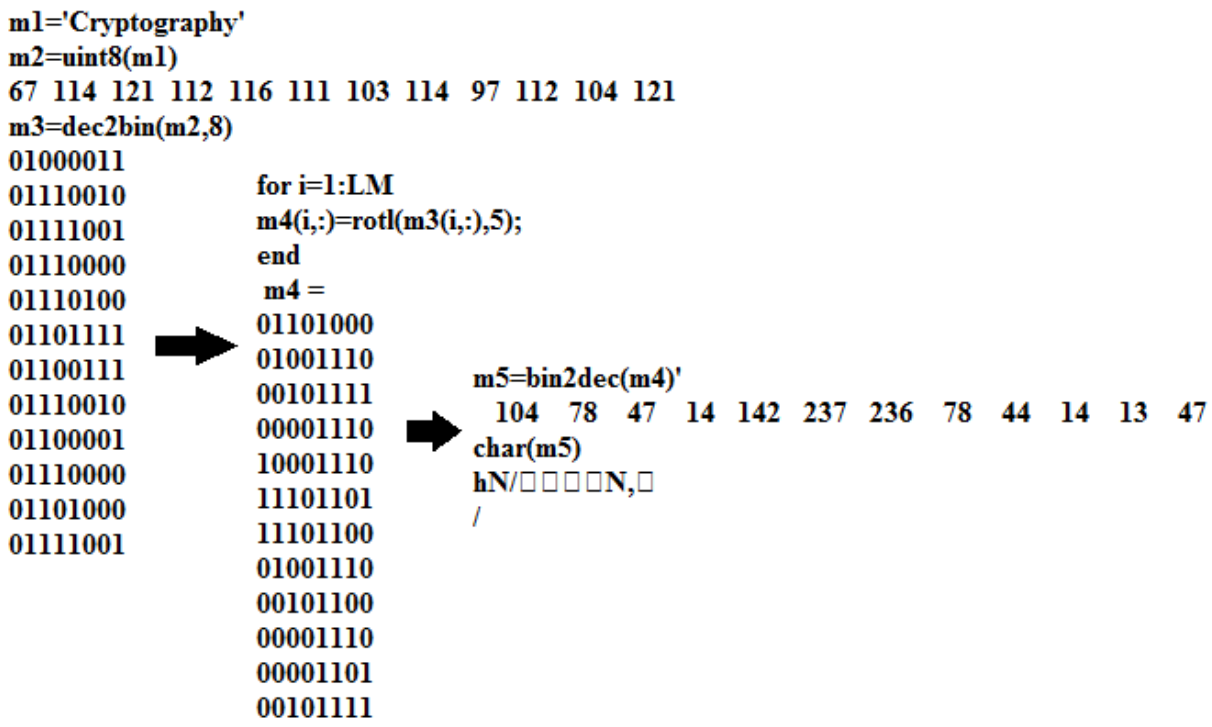

Figure 8: Rotate left task example

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

The proposed method encryption function will be implemented applying the following steps:

Step1: Inputs preparation:

1) Get the image_key, get the image size, reshape the image to one row matrix.
2) Get the message, convert the message to decimal, get the message length, this step can be implemented by executing the following mat lab code:

```
c1=imread('C:\Users\win 7\Desktop\Lena.jpg');
[n1 n2 n3]=size(c1);L=n1*n2*n3;
c2=reshape(c1,1,L);
message='Secret message';
m1=uint8(message);
LM=length(m1);
```

Step2: Secret keys generation:

1) Get the values of POS1, POS2 and NORLD.
2) Calculate position1 and position2.
3) Extract the secret key1 from the image_key starting from position1 with length equal message length.
4) Extract an array from image_key with length equal message length, sort this array to form the second secret key.

This step can be implemented by executing the following mat lab code:

```
POS1=0.179;POS2=0.332;NORLD=5;
P1=fix(L*POS1);P2=fix(L*POS2);P3=fix(L*POS3);
KEY1=c2(1,P1:P1+LM-1);
K2=c2(1,P2:P2+LM-1);
[bb KEY2]=sort(K2);
```

Step3: Message XORing with secret key1.

This step can be implemented by executing the following mat lab operation:

```
m2=bitxor(m1,KEY1);
```

Step4: Message shuffling:

Use the secret key2 to rearrange the message characters by shuffling them using the values of key2 as indexes, the following mat lab code can be used to implement this step:

```
m3=m2;
for i=1:LM
   d=find(KEY2==i);
   m3(1,i)=m2(1,d);
end
```

Step5: MBM crows left rotation:

1) Convert the message to binary to form MBM.
2) Use NORLD to rotate left each row in the MBM.

This step can be implemented executing the following mat lab code:

```
m3=m2;
for i=1:LM
   d=find(KEY2==i);
   m3(1,i)=m2(1,d);
end
```

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

The decryption function can be implemented in the same manner as for encryption function but the sequence of round must be round3, round 2 then round 1: the following code can be used to implement the decryption function:

```
c1=imread('C:\Users\win 7\Desktop\Lena.jpg');
[n1 n2 n3]=size(c1);L=n1*n2*n3;
c2=reshape(c1,1,L);
mes=m7;
LM=length(mes);
m11=uint8(mes);
POS1=0.179;POS2=0.332;KEY3=5;
P1=fix(L*POS1);P2=fix(L*POS2);P3=fix(L*POS3);
KEY1=c2(1,P1:P1+LM-1);
K2=c2(1,P2:P2+LM-1);
[bb KEY2]=sort(K2);
m8=dec2bin(m11,8);
m9=m8;
for i=1:LM
      m9(i,:)=rotl(m8(i,:),8-KEY3);
end
m10=bin2dec(m9)';
m11=m10;
for i=1:LM
   d=find(KEY2==i);
   m11(1,d)=m10(1,i);
end
m11=uint8(m11);
m12=bitxor(m11,KEY1);
m13=char(m12)
```

Implementation and Results Discussion

The proposed method satisfied the quality requirements, the proposed method was implemented using various messages, the decrypted message was always identical to the source message, the obtained results of the quality parameters measured between the source and the encrypted messages prove the quality of the encrypted message, and table 2 shows the obtained quality parameters:

Table 2: Quality parameters measured between the source and encrypted messages

Message length (K bytes)	MSE	PSNR
1	10829	17.9257
2	10737	18.0111
4	10908	17.8530
5	10805	17.9476
10	10804	17.9481
15	10806	17.9463
25	10968	17.7980
50	10899	17.8606
100	10911	17.8501
Remarks	High	Low

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

The speed of the proposed method was tested, the obtained values of the encryption time in seconds (ET) and the decryption time in seconds (DT) were acceptable and they are better than the results obtained for DES and AES methods, table 3 shows the obtained speed results of the proposed method after executing a selected messages:

Table 3: Obtained speed results

Message length (bytes)	ET	DT
10	0.0170	0.0030
20	0.0210	0.0050
50	0.0210	0.0060
75	0.0240	0.0070
100	0.0250	0.0090
200	0.0350	0.0140
250	0.0390	0.0170
500	0.0630	0.0310
750	0.0840	0.0480
1000	0.1400	0.0840
Average	0.0469	0.0224

For short messages (with length less or equal 500 characters) the ET and DT grow slowly when increasing the message length, and for longer messages the ET and DT will rapidly grow (see figure 9), in this case we recommend dividing the message into blocks with block size less or equal 500 characters.

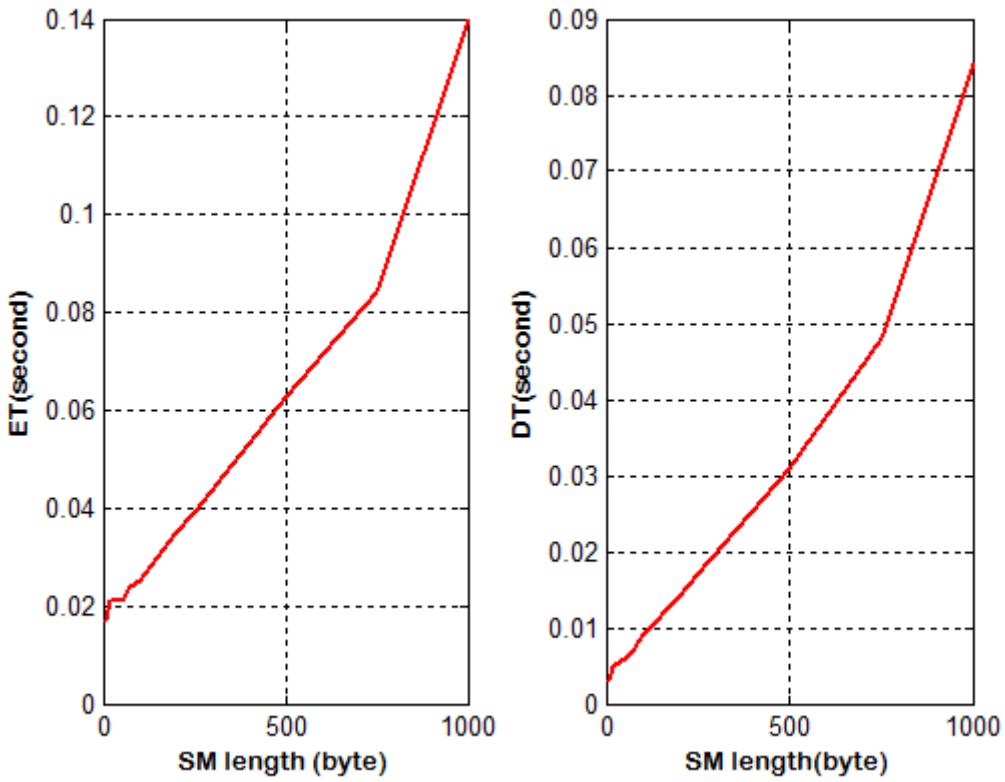

Figure 9: ET and DT vs SM length

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

The method was tested for sensitivity; the message 'Secret message security' was encrypted using the following PK:

PK:

```
c1=imread('C:\Users\win 7\Desktop\Lena.jpg');
POS1=0.179;POS2=0.332;
NORLD=5;
```

The encrypted message was decrypted using the PK changes shown in table 4, the obtained quality parameters measured between the source and the decrypted message proves the method sensitivity, making any changes in the PK in the decryption function will produce a damaged decrypted message.

Table 4: Method sensitivity

Changes in the PK	MSE	PSNR	Remarks
No changes	0	Infinity	Correct
Changing image_key to image 4.2.03.tiff	47266	11.3061	Damaged
POS1=0.279	932.2857	26.6954	Damaged
POS2=0.232	101.8571	50.6480	Damaged
NORTD=3	11008	17.3654	Damaged

Conclusion

A simple, secure and efficient method of message cryptography was proposed. The method used a complicated private key to protect the message, this cannot be hacked and it contained: secret image_key, and the values of the double variable POS1, POS2 and NORLD, the produced decrypted message was very sensitive to the selected PK, any minor changes in this key produced a damaged decrypted message. The method was implemented in three simple rounds using simple operations: XORing, columns shuffling and message binary matrix row left rotation.

The proposed method was tested using various messages. The quality of the encrypted and decrypted messages was examined and the obtained results showed that the proposed method satisfied the quality requirements of good crypto system.

The speed of the proposed method was tested and it was shown that the proposed method required small times for message encryption and decryption especially for short messages, long message can be divided into blocks to keep the method efficient. The method sensitivity was tested and it was shown that the encryption and decryption functions must use the same PK to produce a correct decrypted messages.

References

[1]. 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

[2]. 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

[3]. 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

[4]. 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/

[5]. 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)

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

[6]. 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

[7]. 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

[8]. Kathryn,"A Java Steganography Tool", 2005.http://diit.sourceforge.net/files/Proposal.pdf

[9]. 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

[10]. 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

[11]. 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

[12]. Afjal H. Sarower; Rashed Karim; Maruf Hassan, An Image Steganography Algorithm using LSB Replacement through XOR Substitution, Computer Science:2019 International Conference on Information and Communications Technology (ICOIACT), DOI:10.1109/icoiact46704.2019.8938486.

[13]. 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

[14]. 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.

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

[16]. 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

[17]. 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

[18]. 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.

[19]. 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.

[20]. 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.

[21]. Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, Journal of Engineering, 2005.

[22]. 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.

[23]. 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.

[24]. 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.

[25]. M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014.

[26]. Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science &Applications,1(7), pp. 361-366, (2016). https://doi.org/10.14569/IJACSA.2016.070350

[27]. Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC, Vol. 8, Issue.2, February 2019, pg.93 – 103

[28]. Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Engineering Technology & Applied Science Research, Vol.9 Issue 1, Pages 3681-3684, 2019.

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

[29]. Zhou X, Gong W, Fu W, Jin L. 2016An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15thInt. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp. 1–4 .https://doi.org/10.1109/ICIS.2016.7550955

[30]. Wu D-C, Tsai W-H. A stenographic method for images by pixel value differencing. Pattern Recognition. Lett. 24, 1613–1626. 2003https://doi.org/10.1016/S0167-8655(02)00402-6

[31]. Das R, Das I. Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In Proc. 2nd Int. Conf. on Research in Computational Intelligence and Communication Networks, Kolkata, India, pp. 296–301, 2016.https://doi.org/10.1109/ICRCICN.2016.7813674.

[32]. M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[33]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[34]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022.

[35]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Pur- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[36]. M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.

[37]. M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[38]. M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.

[39]. 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, Volume 38, 2022, 102379, ISSN 2214-157X, https://doi.org/10.1016/j.csite.2022.102379.

[40]. M. Abu-Faraj, and Z. Alqadi, "Image Encryption using Variable Length Blocks and Variable Length Private Key," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 11, Iss. 3, pp. 138-151, 2022.

[41]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Dual Approach for Audio Cryptography," Journal of Southwest Jiaotong University, vol. 57, no. 1, pp. 24-33, 2022.

[42]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022.

[43]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purr- posed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022.

[44]. M. Abu-Faraj, Khaled Aldebe, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," Journal of Southwest Jiaotong University, vol. 56, no. 6 , pp. 685-694, 2021.

[45]. M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Meth- odds for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12 , pp. 451-458, 2021.

[46]. J. Vilkamo and T. Bäckström, "Time-Frequency Processing: Methods and Tools," in Parametric Time-Frequency Domain Spatial Audio, V. Pulkki, S. Delikaris-Manias, and A. Politis, Eds. Wiley, 2017, pp. 3–24.

[47]. K Matrouk, A Al-Hasanat, H Alasha'ary, Ziad Al-Qadi, H Al-Shalabi, Speech fingerprint to identify isolated word person, World Applied Sciences Journal, 31 (10), 1767-1771, 2014.

[48]. Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.

[49]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh, A Novel Based On Image Blocking Method to Encrypt-Decrypt Color, International Journal on Informatics Visualization, vol. 3, issue 1, pp. 86-93, 2019.

[50]. Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7. Issue 3.13, pp. 104-107. 2018.

[51]. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.

[52]. Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, International Journal of Computer Applications, vol. 975, pp. 8887, 2018.

[53]. Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9. Issue 9, pp. 4092-4098, 2019.

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

[54]. Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8. Issue 5, pp. 2780-2787, 2018.

[55]. Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.

[56]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016.

[57]. Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.

[58]. Jihad Nader Ahmad Sharadqh, Ziad Al-Qadi, Bilal Zahran, Experimental Investigation of Wave File Compression-Decompression, International Journal of Computer Science and Information Security, vol. 14m issue 10, pp. 774-780, 2016.

[59]. Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[60]. Majed O Al-Dwairi, A Hendi, Z AlQadi, an efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology &Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.

[61]. Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, a novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp, 232-238, 2019

[62]. Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TOCREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.

[63]. M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Ex- Traction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.

[64]. Alqadi, Z. (2019). A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE), 9(5): 4092-4098.https://doi.org/10.11591/ijece.v9i5.pp4092-4098.

[65]. Alqadi, Z. (2009). A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image. Journal of Computer Science, 5(5): 355-362.

[66]. Zaini, H., Alqadi, Z.A. (2021). Efficient WPT based speech signal protection. IJCSMC, 10(9): 53-65.https://doi.org/10.47760/ijcsmc.2021.v10i09.006.

[67]. Zneit, R.A., Khrisat, M.S., Khawatreh, S.A., Alqadi, Z.(2020). Two ways to improve WPT decomposition used for image features extraction. European Journal of Scientific Research, 157(2): 195-205.

[68]. Hindi, A., Qaryouti, G.M., Eltous, Y., Abuzalata, M.,Alqadi, Z. (2020). Color image compression using linear prediction coding. International Journal of Computer Science and Mobile Computing, 9(2): 13-20.

[69]. Zaidan, A.A., Majeed, A., Zaidan, B.B. (2009). High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Academy of Science Engineering and Technology(WASET), 54: 468-479.

[70]. Zaidan, A.A., Zaidan, B.B. (2009). Novel approach for high secure data hidden in MPEG video using public key infrastructure. International Journal of Computer and Network Security, 1(1): 1985-1553.

[71]. Khalifa, O.O., Naji, A.W., Zaidan, A.A., Zaidan, B.B.,Hameed, S.A. (2010). Novel approach of hidden data inthe (unused area 2 within EXE file) using computation between cryptography and steganography. Int. J. Comput.Sci. Netw. Secur, 9(5): 294-300.

[72]. Majeed, A., Mat Kiah, M.L., Madhloom, H.T., Zaidan,B.B., Zaidan, A.A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and technology, 1(2): 63-69.http://eprints.um.edu.my/id/eprint/4951.

[73]. Zaidan, A.A., Othman, F., Zaidan, B.B., Raji, R.Z.,Hasan, A.K., Naji, A.W. (2009). Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In Proceedings of the World Congress on Engineering, 1: 1-7.

[74]. Aos, A.Z., Naji, A.W., Hameed, S.A., Othman, F.,Zaidan, B.B. (2009). Approved undetectable-antivirussteganography for multimedia information in PE-file. In 2009 International Association of Computer Science and Information Technology-Spring Conference, pp. 437-444. https://doi.org/10.1109/IACSIT-SC.2009.103.

[75]. Zaidan, A.A., Zaidan, B.B., Abdulrazzaq, M.M., Raji,R.Z., Mohammed, S.M. (2009). Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen,Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex, 19: 482-489.

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden

[76]. Naji, A.W., Zaidan, A.A., Zaidan, B.B., Muhamadi, I.A.(2010). Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proceeding of World Academy of Science Engineering and Technology (WASET), 56(5): 498-502.

[77]. 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.

[78]. 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.

[79]. Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," Information Sciences, vol. 480, pp. 403–419, 2019.

[80]. 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.

[81]. X. Zhang and X. Wang, Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System, Springer, New York, NY, USA, 2019.

[82]. 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.

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden