Image Encryption Using Chaotic Cat Mapping in the Discrete Fourier Transform

Mohammed Alzain

Department of Information Technology, College of Computers and Information Technology, Taif University

Abstract—The paper presents an secure image using the two dimensional chaotic cat mapping (2D-CCM) in the Discrete Fourier Transform domain (DFT). The ciphering phase begins by applying theDFT on the plainimage to be encrypted and the resulted Fourier transformed image are scrambled using the 2D-CCM and finally an inverse DFT is applied to obtain the final encrypted image. The decryption phase applies a reverse procedure to get the original plainimage. A set of encryption test experiments are employed to inspect the proposed DFT based 2D-CCM image cryptosystem. The experimental results verified and confirmed the superiority of the proposed DFT based 2D-CCM image cryptosystem.

Keywords—Image cipher, 2D-CCM, DFT.

1. INTRODUCTION

Nowadays, due to the large utilization of digital images over telecommunication media, it is necessary to develop efficient and robust security techniques to secure them during transmission through communication systems [1-4]. The requirements to satisfy and fulfill the security requirements of digital images resulted in development of different encryption methods[4-10]. Within the last decade, several encryption methods have been suggested in the literature and they may be categorized into traditional and chaos based encryption methods. Traditional encryption methods may include DES, Double DES, Triple DES, IDEA, RC5, RC6 and [11-14]. But, these traditional methods does not allow a satisfactory outcomes due to of image intrinsic properties like large bulky capacity, high correlation, and redundancy [14-16].Chaos based encryption methods may be regarded as good practical tool as suchmethodspresent a good mix of high speed, and security, less complexity, allowable computational power and overheads [17-18].

The aim of this study is to introducing a secure DFT based 2D-CCM image cryptosystem that is efficiently capable of encrypting and decrypting digital images through secure or unsecure telecommunication networks. The encrypting phase starts through employing the DFT on the source plainimage and the obtained discrete Fourier transformed image is shuffled by a 2D-CCM and finally applying an inverse DFT to get the final ciphered image. The decrypting phase starts through employing the DFT on the encrypted image and the obtained discrete Fourier transformed image is inversely shuffled by an inverse 2D-CCM and finally applying an inverse DFT to get the final original image.

The paper reminder is marshaled as follows: Sect. 2 explores the basic knowledge about the 2D-CCM and the DFT. Sect. 3 is presents the details of the proposed DFT based 2D-CCM image cryptosystem. Experimental testing and the security description of the proposed DFT based 2D-CCM image cryptosystemare exploredin Sect. 4, Sect. 5 gives the concluding remarks regarding the proposed DFT based 2D-CCM image cryptosystem.

2. Basic Knowledge

This section is dedicated to the basic tools that are employed in proposed DFT based 2D-CCM image cryptosystem. This tools may involve the 2D-CCM and the DFT.

2.1 2D-CCM

The 2D-CCM (chaotic map called Arnold's Cat mapping)is developed by the Russian mathematician Vladimir I. Arnold [19-20], who discovered it by using cat image, as described in Fig. 1. The 2D-CCM may be described for NxN image as:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod m \qquad (1)$$

where mod, p, q are the modulo operation and control variables of the 2D-CCM which can be utilized as its secret keys.

After a set number of iterations m (modulo) of the 2D-CCM, the original image will return. The random relationship between the size of the image and the numbers of iterations which takes to return to the original image is depicted in Table 1 [21].

Table 1: $n\ x\ n$ Dimension images to return to its original image.

Dimension of $n \times n$ matrix (pixel values)	Number of iterations to return to original image (m)
300 × 300	300
183 × 183	60
124 × 124	15
100 × 100	150
150 × 150	300
257 × 257	258
157 × 157	157
147 × 147	56

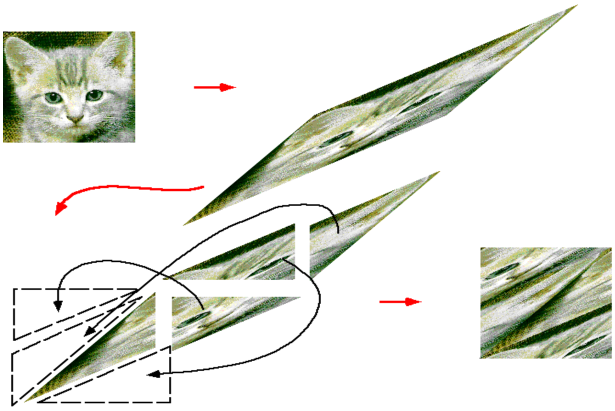


Fig. 1: The 2D-CCM

2.2 The DFT

The DFT may be regarded as an essential tool in digital signal processing. For two dimensional signal $z(x, y)$ of size M x N, the DFT and its inverse can be represented by [22]:

$$Z(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} z(x,y)e^{-j2\Pi(ux/M+vy/N)} \qquad (2)$$

$$z(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} Z(u,v)e^{j2\Pi(ux/M+vy/N)} \qquad (3)$$

3. The Proposed DFT based 2D-CCM Image Cryptosystem

The proposed DFT based 2D-CCM image cryptosystem utilizes the 2D-CCM and FT. The ciphering phase begins firstly by employing a Fourier transform on the original source plainimage. Then the Fourier transformed resulted image are shuffled with the aid of applying a 2D-CCM and finally employing an inverse Fourier transform to get the final encrypted image. The deciphering phase applies inverse steps of the ciphering phase.The deciphering phase begins firstly by also employing a Fourier transform on the encrypted image. Then the Fourier transformed resulted image are subjected inversely shuffling with the aid of applying an inverse 2D-CCM and finally employing an inverse Fourier transform to get the final original image. Figs. 2-3depicts encryption/decryptionphases of the proposed DFT based 2D-CCM image cryptosystem, respectively.

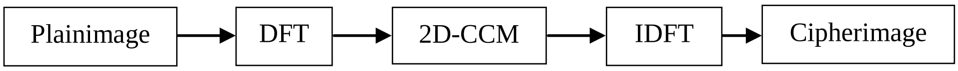


Fig. 2: Ciphering phase of the proposed DFT based 2D-CCM image cryptosystem.

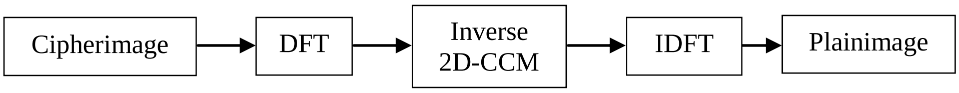
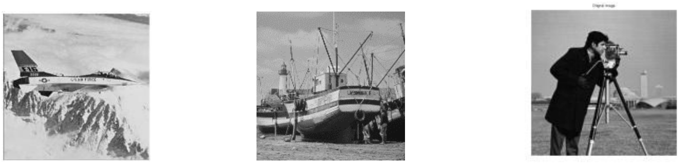


Fig. 3: Deciphering phase of the proposed DFT based 2D-CCM image cryptosystem.

4. Security Study

This section is dedicated for testing the security of the proposed DFT based 2D-CCM image cryptosystem visually and with a group of encryption testing.The proposed DFT based 2D-CCM image cryptosystem is examined through a set of encryption tests to inspect the security of the proposed DFT based 2D-CCM image cryptosystem. These examination experiments have been performed with a group of testing image. The tested images may involve the Airplane, Boat and Cameraman images as illustrated in Fig. 4.



a) Airplane b) Boat Cameraman

Fig. 4: Different samples of original images

4.1. Visual Testing

The proposed DFT based 2D-CCM image cryptosystem is visually inspected using a group of testing images like Airplane, Boat and Cameraman images. The encryption results for such images is appeared in Fig. 5. The visually testing results demonstrated the efficiency of the proposed DFT based 2D-CCM image cryptosystem in hiding all areas of the testing images. Such visually examined testing results proved and confirmed the significance of the proposed DFT based 2D-CCM image cryptosystem.

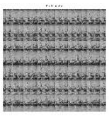
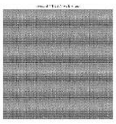
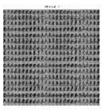
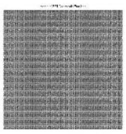
Image	Encrypted image usingthe CCM and the proposed DFT based 2D-CCM image cryptosystem	
	2D-CCM	DFT based 2D-CCM image cryptosystem
Airplane		
Boat		
Cameraman		

Fig. 5: Encryption outcomes of the 2D-CCM and the proposedDFT based 2D-CCM image cryptosystem

4.2. Statistical Testing

4.2.1 Histogram Testing

The histogram testing results of the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystem for the tested plainimages/cipherimages are illustrated in Fig. 6.The histogram testing results of the proposed DFT based 2D-CCM image cryptosystem for the encrypted images are almostdistinct from their respected original images histogram testing results. Also, it may be shown that thehistogram testing results of the 2D-CCM for encrypted images cipher are the same as the histogram testing results of their respected original images. This is expected since the 2D-CLM just changes the location of pixels.

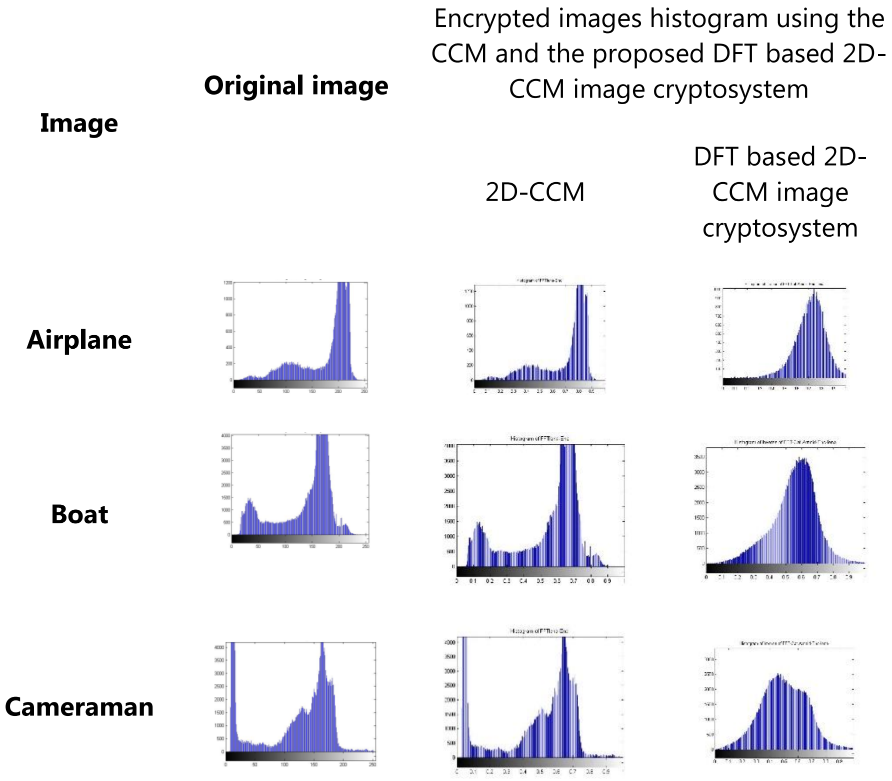


Fig. 6: Histogram testing results of the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystem

4.2.2 Correlation Coefficients Testing

The correlation coefficients are computed between the encrypted and original images as [23]:

$$C_r = \frac{\operatorname{cov}(P,C)}{\sqrt{D(P)}\sqrt{D(C)}}, \tag{4}$$

Low correlation coefficients values ensure efficient encryption quality. The correlation coefficients testing results of the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystems for the tested plainimages/cipherimages are given in Table 1. The testing outcomes demonstrate that the correlation coefficients between pairs of plainimage/cipherimage are near the ideal zero value which in turn verified and ensured good encryption efficiency.

Table 1: Correlation coefficient testing of the CCM and the proposed DFT based 2D-CCM image cryptosystems

Image	**Entropy values with 2D-CLM and the proposed 2D-CLM based SVD image cryptosystems**	
	2D-CCM	**DFT based 2D-CCM**
Airplane	0.0053	0.0072
Boat	5.2289e-004	-0.0056
Cameraman	0.0031	5.9118e-004

4.3. EntropyTesting

The entropy testing examines the information amount in the outcome encrypted image that resulted using the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystem The entropy may be computed using [24]:

$$E = -\sum_{i=1}^{n} P_r(x_i)\log P_r(x_i) \tag{5}$$

Where x_i representsthe ithpixelgray value. High estimations for entropy demonstrate good encryption efficiency. The entropy testing outcomes of the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystems are shown inTable 2. The entropy testing outcomes demonstrated that encrypted images entropy for the 2D-CCM are larger with respect to their respective results of the proposed DFT based 2D-CCM image cryptosystem.

Table 2: Entropy outcomes of the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystems

Image	**Encrypted images Entropy using the CCM and the proposed DFT based 2D-CCM image cryptosystems**	
	2D-CCM	**DFT based 2D-CCM**
Airplane	**6.7071**	6.9314
Boat	**7.1238**	7.1528
Camerama n	**7.0097**	7.4039

4.4. Differential Testing

The Differential testing is conducted to examine the impact of employed for testing the effect of just one-pixel alternation in the original image on the constructed encrypted image using cipherimage using the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystem. The differential testing involve the Numberof Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) testing. The NPCR is estimated by [25-27]:

$$NPCR(Enc_1, Enc_2) = \frac{\sum_{i,j} D(x_i, y_j)}{M \times N} \times 100\%, \tag{6}$$

$$D(x_i, y_j) = \begin{cases} 1 & if \quad Enc_1(x_i, y_j) = Enc_2(x_i, y_j) \\ 0 & \quad \text{Otherwise} \end{cases} \tag{7}$$

where M, N are both the height and width of Enc$_1$ and Enc$_2$images.

The UACI is estimated by [25-27]:

$$UACI(Enc_1, Enc_2) = \frac{1}{M \times N}\left[\Sigma_{x_i y_j} \frac{Enc_1(x_i, y_j) - Enc_1(x_i, y_j)}{255}\right] \times 100\%, \quad (8)$$

The NPCR and UACI testing outcomes of the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystems are shown in Table 3. The entropy testing outcomes demonstrated that encrypted images entropy for the 2D-CCM are larger with respect to their respective results of the proposed DFT based 2D-CCM image cryptosystem.

The NPCR and UACI testing outcomes ensured and provedthe high sensibility of both the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystems with respect very small alternations which also good encryption for both the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystems.

Table 3: The **NPCR and UACI** testing outcomes of the 2D-CCM and the proposed DFT based 2D-CCM image cryptosystems

Image		**Encrypted images NPCR and UACI using the CCM and the proposed DFT based 2D-CCM image cryptosystems**	
		2D-CCM	**DFT based 2D-CCM**
Airplane	**NCPR**	**100**	**100**
	UACI	**0**	**0**
Boat	**NCPR**	**100**	**100**
	UACI	**0**	**0**
Cameraman	**NCPR**	**100**	**100**
	UACI	**0**	**0**

5. Conclusion

The paper proposed a secure DFT based 2D-CCM image cryptosystem. The proposed DFT based 2D-CCM image cryptosystem is tested and examined and investigated with a group of different encrypting metrics like visual inspection, histogram, entropy, encryption quality and differential examinations.The experimental testsoutcomes confirmedthe efficiencyand the significance ofthe proposed DFT based 2D-CCM image cryptosystem.

References

1. Majid Khan, and Tariq Shah," A Literature Review on Image Encryption Techniques", 3D Res, vol. 29(5), 2014.

2. Fuwen Liu, Hartmut Koenig ,"A Survey of Video Encryption Algorithms," Journal of Computers & Security, Vol. 19, No. 1, 2010, pp. 3-15.

3. Zhengan Huang, Shengli Liu, Xianping Mao, Kefei Chen and Jin Li "Insight of the Protection for Data Security under Selective Opening Attacks," journal of Information Sciences, Vol. 412-413, 2017, pp. 223-241.

4. Esam Elsheh and Ben Hamza "Secret Sharing Approaches for 3D Object Encryption," journal of Expert Systems with Applications, Vol. 38 , No. 11, 2011, pp. 13906-13911.

5. Hossam. Ahmed, Hamdy M. Kalash and Osama S. Farag Allah "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption", Proceedings of Informatica, Vol. 31, No 1, Mar 2007, pp. 121-129.

6. S. Lian, J. Sun and Z. Wang. "Security analysis of a chaos-based image encryption algorithm," Physica A: Statistical and Theoretical Physics, vol. 351, Issues 2-4, 15 June 2005, pp. 645-661.

7. Fuyan Sun, Shutang Liu, Zhongqin Li, and Zongwang Lü, "A novel image encryption algorithm based on spatial chaos map," Chaos,Solitons and Fractals vol. 38, pp. 631-640, 2008.

8. Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes", Proceedings of International Journal of Video & Image Processing and Network Security, Vol. 12, No. 04, 2012, pp. 18-31.

9. Heba M. Elhoseny, Osama S. Faragallah, Hossam E.H. Ahmed, Hassan B. Kazemian, Hala S. El-sayed, Fathi E. Abd El-Samie, "The Effect of Fractional Fourier Transform in Encryption Quality for Digital Images," Optik-International Journal for Light and Electron Optics, vol. 127(1), pp. 315-319, 2016.

10. Heba M. Elhoseny, Hossam E. H. Ahmed, Alaa M. Abbas, Hassan B. Kazemian, Osama S. Faragallah, Sayed M. El-Rabaie, Fathi E. Abd El-Samie, "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," Signal, Image and Video Processing Journal, vol. 9(3), pp. 611-622, 2015.

11. Z.Yun-Peng, L.Wei, C. Shui-Ping, Z. Zheng-Jun, N. Xuan, and D.Wei-Di, "Digital Image Encryption Algorithm Based on Chaos and Improved DES",IEEE International Conference on Systems, Man and Cybernetics, pp. 474-479, 2009.

12. W. Stallings., "Cryptography and Network Security: Principles and Practice," Prentice Hall, New Jersey, 1999.

13. Bruce Schneier, "Applied Cryptography Protocols, algorithms, and source code in C,"John Wiley & Sons, Inc., New York, second edition, 1996.

14. R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, "The RC6TM Block Cipher", M. I. T laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, USA, 1998.

15. X. Zhang, X. Fan, J. Wang, and Z. Zhao, "A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution," Multimedia Tools and Applications, vol. 75, no. 4, pp. 1745–1763, 2016.

16. Shujun Li, Guanrong Chen and Xuan Zheng, "Chaos-based encryption for digital images and videos," chapter 4 in Multimedia Security Handbook, February 2004.

17. S. Lian, G. Sun, and Z. Wang, "A block cipher based on a suitable use of chaotic Standard map," Chaos, Solutions and Fractals, vol. 26, pp. 117-129, 2005.

18. S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," Phys. Lett. A 351, pp. 645-661, 2005.

19. 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, pp. 749-61, 2004.

20. G. Peterson, "Arnold's Cat map," Math Linear Algebra, 1997.

21. Katherine Struss, "A Chaotic Image Encryption," Mathematics Senior Seminar, 4901, Spring 2009.

22. Stuti Goel, Arun Rana, Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography," IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), vol. 6(1), pp. 41-48, 2013.

23. X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," Applied Soft Computing, vol. 37, pp. 24–39, 2015.

24. Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas , S. El-Rabaie, Fathi E. Abd El-Samie, "Homomorphic image encryption," Journal of Electronic Imaging 18(3), 033002, 2009.

25. Li Y, Zhang F, Li Y, Tao R., "Asymmetric multiple-image encryption based on the cascaded fractional Fourier transform," Opt. Lasers Eng., vol. 72, pp. 18-25, 2015.

26. Ensherah A. Naeem, Mustafa M. AbdElnaby, Hala S. El-sayed, Fathi E. Abd El-Samie, and Osama S. Faragallah, "Wavelet Fusion for Encrypting Images with a Few Details," Computers and Electrical Engineering, vol. 54, pp. 450-470, 2016.

27. Chen L, Zhao D., "Image encryption with fractional wavelet packet method," Optik, vol. 119, pp.286-291, 2008.