Hybrid Ciphering System of Images based on Fractional Fourier Transform and Two Chaotic Maps

Noha Ramadan
Faculty of Electronic Engineering
Menofia University
Egypt

HossamEldin H. Ahmed
Fathi E. Abd El-Samie
Faculty of Electronic Engineering
Menofia University
Egypt

Said E. Elkhamy
Faculty of Engineering
Alexandria University
Egypt

ABSTRACT

This paper presents a new implementation of a hybrid ciphering system of images in Fourier domain based on two chaotic maps. The first map is the Bakermap,which is used to scramble the image pixels in three modes of operation (CBC, CFB and OFB). The second map is the logistic map,whose secret key depends on the plain text. In the key generation step of the logistic map, the chaotic stream is generated with plain text and hence the relation between the key and the plain text is established. We use Fractional Fourier Transform (FrFT) before the encryption to achieve a large degree of randomization. We examine the proposed algorithm and compare the results with the RC6 algorithm. The performance and security analysis prove that this hybrid ciphering system is efficient, reliable, and can effectively resist different attacks.

Keywords

Baker map, Fourier transform, Logistic map, Modes of operation, and Security analysis.

1. INTRODUCTION

Nowadays, transmission of digital images over networks has become a very important issue,such that the protection of images against illegal access is a must. Image encryption is used as a security manner over open channels. It has been found that the traditional encryption algorithms such as the Data Encryption Standards (DES) [1] and the Advanced Encryption Standard (AES) [2] are not effective for images,because of the bulky nature of images, high correlation between pixels and high redundancy, which complicate the operation and make it time consuming. Chaos-based image encryption algorithms have shown better performance than traditional encryption algorithms [3].Chaotic systems have several important properties, which agree withthe main encryption requirements such as diffusion and mixing [4]. These properties are the sensitivity dependence on initial conditions and the pseudo-randomness.

Recently, some chaos-based encryption algorithms with key stream depending only on the key were broken. Three schemes were presented in [5-7]. These schemes have the same encryption principle that is confusion and diffusion perform, alternatively. However, the authors in [8] analyzed this kind of scheme and found some problems such as weak sensitivity to the change of plain images or key stream. In these schemes, the same key streams were used to encrypt different plain images. The hacker can obtain the key from known plain text and chosen plain text attacks. To enhance the security and avoid the short periodicity of the chaotic key stream, the key stream should be related to the plain image.

The proposed hybrid ciphering system uses a combination between scrambling of positions and changing of the pixel values. Firstly, the Baker map is used to scramble the positions of the image pixels in three different modes of operation (CBC, CFB, and OFB) [9-11]. Secondly, the logistic map uses the plain image to generate the current chaotic number, and then takes the generated chaotic number as the next input of the chaotic iterations. This process is repeated and the last output value is used as the initial key. This key is used to encrypt the image. By doing so, the correlation between initialkey and the plain text is created [12].The FrFT is used before the encryption to achieve a large degree of randomization.

2. FRACTIONAL FOURIER TRANSFORM

The FrFT is the generalization of Fourier Transform (FT) [10]. The FrFT performs a rotation of the signal with a certain angle. We use the FrFT to change the statistical characteristics of the image after scrambling. The substitution and diffusion are performed in the FrFT domain, and this achieves a large degree of randomization when returning back to the spatial domain. The FrFT corresponds to a rotation of the FT with an arbitrary angle α = aπ / 2 with a ∊ R. The FrFT is defined by means of transform kernel as [13]:

$$K_\alpha(t,u)=\begin{cases}\sqrt{\frac{1-j\cot\alpha}{2\pi}}\cdot\exp(j\,\frac{t^2+u^2}{2}\cot\alpha-j\,\frac{tu}{\sin\alpha}) & if \quad \alpha\neq n\pi\\ \delta(u-t) & if \quad \alpha=2n\pi\\ \delta(u+t) & if \quad \alpha=(2n+1)\pi\end{cases}\tag{1}$$

The FrFT of a function *x*(*t*), with an angle α, is defined as,

$$X_\alpha(u)=\int_{-\infty}^{\infty}x(t)\,K_\alpha(t,u)dt \tag{2}$$

For a general function $f(x)$, we have

$$f_a(u) = F^a[f(x)]$$
$$= C_\alpha \int f(x) \exp[\, i\pi \frac{u^2 + x^2}{\tan\alpha} - 2i\pi \frac{ux}{\sin\alpha}]dx \qquad (3)$$

$$\text{where } \alpha = \frac{a\pi}{2}, \textit{and } C_\alpha = \frac{\exp[-i(\frac{\pi .sign(\sin(\alpha))}{4} - \frac{\alpha}{2})]}{|\sin\alpha|^{1/2}}$$

3. CHAOTICBAKER MAPSCRAMBLING.

The Baker map is a 2-D chaotic map, which converts a unit square into itself with scrambling. Its operation is cut in half, and the two halves are stacked on one another. The Baker map, B, can be described with the following formulas [14]:

$$B(x, y) = (2x, y/2) \text{ where } 0 \le x \le 1/2 \qquad (4)$$

$$B(x, y) = (2x - 1, y/2 + 1/2) \text{ where } 1/2 \le x \le 1 \qquad (5)$$

3.1 Generalized Baker Map

The Baker map can be generalized as follows:

1. An $N{\times}N$ square matrix is divided into k vertical rectangles of height N and with width n_i.

2. These vertical rectangles should be stretched horizontally.

3. Then, rectangles are stacked to have the left one in the bottom and the right one at the top.

3.2 Discretized Baker Map

It assigns a pixel value to another position in a bijective manner. The discretized Baker map is denoted by $B(n_1,n_2,\ldots\ldots,n_k)$, where $n_1,n_2,\ldots\ldots,n_k$ are integers, and Ni = $n_1 + \ldots.. + n_i$. The pixel at position (r,s), with $N_i \le r < Ni + n_i$ and $0 \le s < N$ is mapped to [15]:

$$B_{(n_1,\ldots,n_k)}(r,s) = \begin{bmatrix} \frac{N}{n_i}(r - N_i) + s \bmod \left(\frac{N}{n_i}\right), \\ \frac{n_i}{N}\left(s - s \bmod \left(\frac{N}{n_i}\right)\right) + N_i \end{bmatrix} \qquad (6)$$

This formula is based on the following:

1. An $N{\times}N$ square matrix is divided into k vertical rectangles of height N and with width n_i.

2. Each vertical rectangle is divided into n_i boxes, and each box contains N points.

3. Each of these boxes is mapped to a row of pixels.

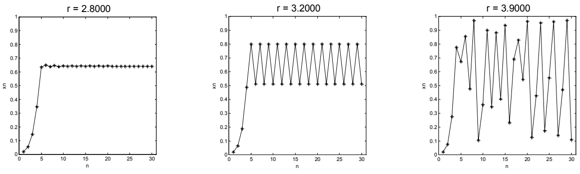
4. THE MODIFIED CHAOTIC LOGISTIC MAP

4-1 Chaotic Logistic Map

The logistic map is one of the simplest maps, where simple non-linear equations are used to produce such chaotic behaviors. Mathematically, a logistic map has the form:

$$x_{n=}rx_{n-1}(1 - x_{n-1}) \qquad (7)$$

Where x_n is a number between zero and one, n =1,2, … is the iteration index, $r$is a positive number and x_0 is the initial value. The value of r controls the output of the logistic map. It is found that when $r \subset [0, 3]$ and x_0= 0.02, as shown in Fig. 1(a), the x_n comes to the same value after several iterations without any chaotic behavior, When $r \in [3, 3.57]$, as shown in Fig. 1(b), the system appears periodicity. While $r \in]3.57, 4]$, the Logistic map exhibits chaotic behavior and depends crucially on the initial condition and this is an important characteristic of chaos [16].



(a)Iteration property when *r = 2.8*

(b)Iteration property when *r = 3.2*

(c)Iteration property when *r = 3.9*

Fig. 1 Analysis of Logistic map

4.2 Modified Chaotic Logistic Map

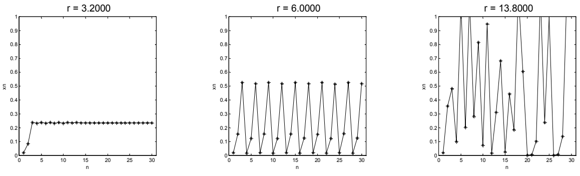
The modified chaotic Logistic map is developed to increase the range of r to be from *0 to 13.8*. The modified chaotic function is :

$$x_{n=}rx_{n-1}(1 - x_{n-1})(1 - x_{n-1})(1.2 - 2x_{n-1})\,(1.2 - 2x_{n-1}) \qquad (8)$$

The modified chaotic logistic map is applied under the following conditions:

- $x_n \in [0,1]$
- $r \in [0,13.8]$

Fig. 2 shows the iteration property of chaotic functions at different values of r to determine which value is suitable for encryption. It is found that the modified logistic map exhibits chaotic behavior when $r \in [6.1, 13.8]$, as shown in Fig. 2 (c), and hence increases the chaotic range of the parameter r.



(a)Iteration property when r = 3.2.

(b)Iteration property when r = 6.

(c)Iteration property when r = 13.8.

Fig. 2 Analysis of modified logistic map.

5. KEY RELATEDTO PLAIN TEXT

In this part, the encryption process is discussed, and the decryption is a reverse process. For a gray-scale image of size M×N, we use a 1-D lexicographically-ordered vector im = { im_1 , im_2 , … , im_L }, where L= $M{\times}N$. Given the initial value x_0 =0.02, the system parameter r=10, and the iteration index n=1,2,... The encryption can be described as follows:

5.1 The Encryption Process

Step 1:For $n = 1$, iterate the modified logistic map by using equation (8) once to get x_1.

Step 2 :Modify x_1 according to the following formula [17]

$$x_1 = mod\,(x_1 + (im_1 + 1)/255,1) \quad (9)$$

Step 3:For $n = n+1$, return to step 1 until $n=L$ to get x_L

Let the new initial value of the logistic map be $(x_0+x_L)/2$

Step 4: Iterate the modified logistic map using Eq. (8) for L times with the new initial value. So, we obtain the sequence

$$X = \{x_{L+1}, x_{L+2}, \dots, x_{2L}\} \quad (10)$$

Step 5:To get sequence $K=\{k_1,k_2,\dots,k_L\}$:

$$k_n = mod(floor(x_{L+n} \times 10^5), 256) \quad (11)$$

where n = 1, 2, ... L

Now, we obtain a set of secret keys $S_K=\{x_0, r, x_L, c\}$, where c is a constant and $c\in[1, 255]$, x_L contains $\{x_0, r, im\}$. As a result, S_K includes three independent variables $\{x_0, r, c\}$ and is related to the plain image.

Step 6:Let n=1.

Step 7:Compute the first cipher pixel by using the value of im_1, the constant c and the first key k_1.

$$c_1 = k_1 \oplus mod(im_1 + c, 256) \quad (12)$$

Step 8:Let $n=n+1$.

Step 9:Compute the n^{th} pixel of the cipher image using the following formula, in which the cipher output feedback is introduced

$$c_n = k_n \oplus mod(im_n + im_{n-1}, 256) \quad (13)$$

Step 10:Repeat steps 8 and 9 until n reaches L, and hence the cipher image $C=\{c_1,c_2,\dots,c_n\}$ is obtained.

6. THE PROPOSED HYBRID CIPHERINGSYSTEM

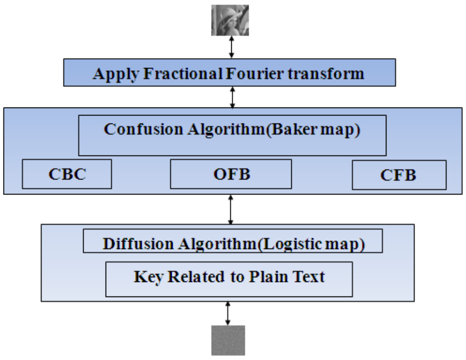
The proposed hybrid ciphering system is divided into two parts. The first part is applying the FrFT to the original image. The second part combines the confusion with diffusion. The confusion algorithm is performed using 2-D chaotic Baker map scrambling in three different modes of operation; Cipher Block Chain (CBC), Cipher Feedback (CFB), and Output Feedback (OFB) in which the Initialization Vector (IV) works as the main key. The diffusion algorithm is performed by applying the key related to plain text algorithm in Fig. 3.

The proposed hybrid ciphering system steps are described as follows:

1. The FrFT is applied to the original image.
2. The transformed image is encrypted using the chaotic Baker map in one of the three different modes of operation for confusion.
3. The shuffled transformed image is applied to the second stage of chaotic encryption for diffusion (the key related to plain text algorithm). Hence, we obtain the encrypted image.

We have implemented the chaotic Baker map with five different values of block size W, where the Initialization Vector (IV) is a section of the encrypted Cameraman image as follows:

1. W_1 is 128×128 pixels.
2. W_2 is 64×64 pixels.
3. W_3 is 32×32 pixels.
4. W_4 is 16×16 pixels.


Apply Fractional Fourier transform
Confusion Algorithm(Baker map)
CBC
OFB
CFB
Diffusion Algorithm(Logistic map)
Key Related to Plain Text

5. W_5 is 8×8 pixels.

Fig. 3 Block diagram of the hybrid ciphering system.

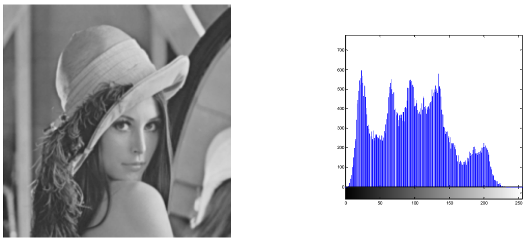
7. PERFORMANCE ANALYSIS

7.1 Statistical Analysis

To examine the quality of the hybrid ciphering system and the stability via statistical attacks, the histogram is calculated for all images and also all the performance metrics.

7.1.1 Histogram

The histogram clarifies how the pixel values of the image are distributed. The original image (Lena.bmp) with the size 512×512 pixels is shown in Fig.4(a) and the histogram of the original image is shown in Fig. 4(b). Fig. 5 illustrates the histogram of the encrypted images with the hybrid system. As we can see, the histograms of the encrypted image with the proposed algorithm in different modes of operation with different block sizes are fairly uniform and are significantly different from that of the original image due to the diffusion caused by the effect of modes of operation in addition to working in the FrFT domain.



(a) The original image.

(b) The histogram of the original image.

Fig. 4 The histogram of the original image.

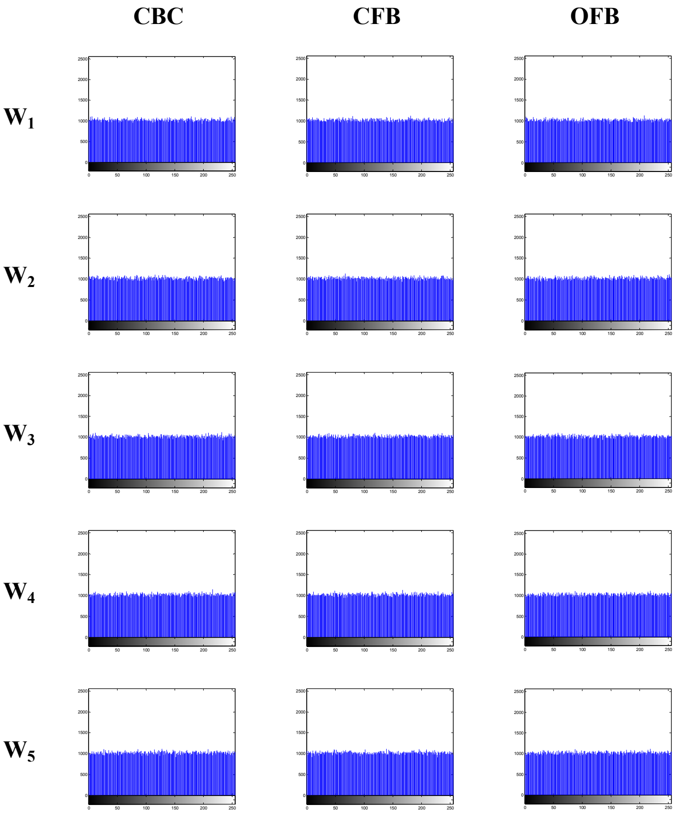


Fig. 5 Histograms of the encrypted image with chaotic Baker map in different modes of operation with different block sizes ($W_1, \ldots, W_5$).

7.1.2 Correlation Coefficient Analysis.

The correlation coefficient equals one ifthe encrypted image is the same as the original image and the encryption process fails in hiding the details of the original image. If the correlation coefficient equals zero, then the original and encrypted imagesare completely different. From Table 1, we see very promising results.

Table 1 Correlation coefficient between the original image and encrypted images using the proposed algorithm in three modes of operation, CBC, CFB, OFB with different block sizes.

Mode of operation	Block size				
	W_1	W_2	W_3	W_4	W_5
CBC	0	0	0	0	0.0022
CFB	0	0.002	0.0013	0	0
OFB	0	0	0.0039	0.0018	0.0013

7.1.3 Maximum Deviation Analysis

Thequality of the encryption algorithm lies in maximizing the deviation between the original and the encrypted image. In this test, the OFB mode with W_2 achieves better resultsthan CBC mode with W_4, which achieves the worst results as shown Table 2. The maximum deviation of the RC6 algorithm is 186907.

Table 2 Maximum deviation results.

Mode of operation	Block size				
	W_1	W_2	W_3	W_4	W_5
CBC	186110	186660	186522	185694	186450
CFB	186729	187312	186153	186325	186802
OFB	186640	187270	187060	186660	186680

7.1.4 Irregular Deviation Analysis

Irregular deviation is based on how much the deviation caused by encryptionis irregular. The lower the irregular deviation value, the better the encryption algorithm. In this test, the CFB mode with W_1achieves the best result and the CBCmode with W_5achieves the worst resultas shown in Table 3. The Irregular deviation of the RC6 algorithm is 184910.

Table 3 Irregular deviation results.

Mode of operation	Block size				
	W_1	W_2	W_3	W_4	W_5
CBC	184742	184724	184948	184684	185322
CFB	184596	184878	184644	185024	184654
OFB	184698	184654	184938	184910	185138

7.1.5 NPCR and UACI Analysis.

To evaluate the variations between the original image and the encrypted images, there are two additional tests; NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity). In this test, the OFB mode with W_2achieves the best UACI and the CFB mode with W_4achieves the best NPCR as shown in Tables 4 and 5. The UACI and NPCR of the RC6 algorithm are equal to 28.2307 and 99.6174, receptivity.

Table 4 The UACI results.

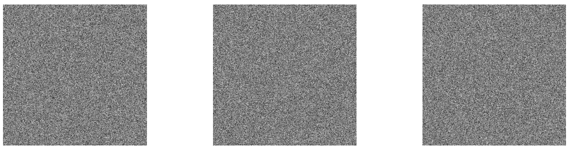
Mode of operation	Block size				
	W_1	W_2	W_3	W_4	W_5
CBC	28.2176	28.2692	28.2614	28.2166	28.1823
CFB	28.2525	28.2311	28.1933	28.221	28.2707
OFB	28.2528	28.2892	28.1876	28.2089	28.2231

Table 5 The NPCR results.

Mode of operation	Block size				
	W_1	W_2	W_3	W_4	W_5
CBC	99.6044	99.6094	99.6143	99.6201	99.6128
CFB	99.6159	99.6189	99.6113	99.6262	99.5987
OFB	99.6155	99.6105	99.6094	99.622	99.5972

7.2 Key Sensitivity Test

Large key sensitivity is required in secure image encryption, which means that the cipher image cannot be decrypted correctly if there is only a slight difference between encryption and decryption keys. For our hybrid system, we test the sensitivity of the key by making small changes in one parameter of the key such as x_0 and compare the resulting encrypted images. In this test, it is not easy to compare the encrypted images by simply observing themin Fig. 6. Thus, for comparison, we can calculate the correlation coefficients between the original image and the three encrypted images. The lower the correlation coefficient, the higher the key sensitivity as shown Table 6.



Encrypted image A with x_0= *0.02*

Encrypted image A' with x_0 = *$0.02+10^{-4}$*

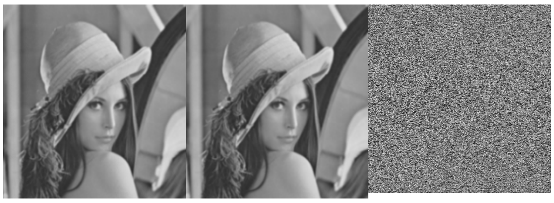
Encrypted image A" with x_0 = *$0.02+10^{-15}$*

Fig. 6 Results of the proposed algorithm with different keys.

Table 6 Correlation coefficient values between the three encrypted images A, B, and C.

Image 1	Image 2	C.C
Encrypted image A	Original image	0.000095166
Encrypted image A'	Original image	0.00098368
Encrypted image A"	Original image	0

Another method for sensitivity test can be performed by making small changes in the constant *r* by a factor 10^{-10}. In the case of no change of the constant *r*, it is clear that the decrypted image appears as original image as shown in Fig. 7(a) and (b). If we changed the constant *r* by a factor 10^{-10}, the decrypted image is completely different from the original image as shown in Fig. 7 (c).



a) The original image

b) decrypted image at *r=10*

c) decrypted image at *$r=10+10^{-10}$*

Fig. 7 Results of the proposed algorithm with changes in *r*.

8. CONCLUSION

In this paper, we introduced an efficient hybrid ciphering system of images based on two chaotic maps. The confusion is achieved withthe first chaotic Baker map in one of three modes of operation; CBC, CFB, or OFB. We examined the effect of the block size of the Baker map in each mode. The diffusion is performed by a proposed key related to plaintext algorithm using a modified chaotic logistic map, which has a wide range of a chaotic parameter *r* to be more robust to attacks. The key of the diffusion algorithm depends on the initial key and the plain image.Thus, the proposed algorithm can resist the known plain text and chosen plain text attacks. All of these procedures for encryption are used in the FrFT domain. Security and sensitivity analysis have been carried out in detail and they demonstrate that this hybrid ciphering system is secure and fast, so it is suitable for real time applications. Our future work is to examine the proposed algorithm over wireless noisy and fading channels and its robustness against the errors due to noise and multipath propagation.

9. REFERENCES

[1] National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication 46, U.S. Government Printing Office, Washington, DC, 1977.

[2] Announcing the ADVANCED ENCRYPTION STANDARD (AES).Federal Information Processing Standards Publication 197.United States National Institute of Standards and Technology (NIST). November 26, 2001.

[3] Patidar, V., Pareek, N. K., Sud, K. K., A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Commun. Nonlinear Sci. Numer.Simulat., 2009, 14: 3056-3075.

[4] Zhang LH, Liao XF, Wang XB, "An image encryption approach based on chaotic maps," Chaos, Solitons& Fractals, Vol. 24, 2005; pp. 759–765.

[5] Y. Mao, G. Chen, and S. Lian, “A novel fast image encryption scheme based on 3D chaotic baker maps,” International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3613–3624, 2004.

[6] J. Shen, X. Jin, and C. Zhou, “A color image encryption algorithm based on magic cube transformation and modular arithmetic operation,” in Advances in Multimedia Information Processing, vol. 3768 of Lecture Notes in Computer Science, pp. 270–280, Springer, 2005.

[7] X. He, Q. Zhu, and P. Gu, “A new chaos-based encryption method for color image,” in Rough Sets and Knowledge Technology, vol. 4062 of Lecture Notes in Computer Science, pp. 671–678, Springer, 2006.

[8] C. Li and G. Chen, “On the security of a class of image encryption schemes,” in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS ’08), pp. 3290–3293, Seattle, Wash, USA, May 2008.

[9] Swiss encryption technology, "Medi Crypt, Modes of operation", pp. 1-4,http: //www.mediacrypt.com/ pdf/MC modes 1204pdf.

[10] Cliford Bergman, Encryption modes, Lecture 16, Feb. 2005, pp. 1-18,

[11] Nawal El-Fishawy, Osama M. Abu Zaid Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms. International Journal of Network Security, 5(3) : 241–251, Nov. 2007.

[12] Cao Guanghui, Hu Kai, Zhang Yizhi, Zhou Jun, and Zhang Xing, " Chaotic Image Encryption Based on Running-Key Related to Plaintext" Hindawi Publishing Corporation the Scientific World Journal Volume 2014, Article ID 490179, 9 pages

[13] L. B. Almeida, "The fractional Fourier transform and time-frequency representations," IEEE Trans. Signal Process., vol. 42, no. 11, pp.3084–3091, Nov. 1996.

[14] Hossam M. Kasem; Mohamed E. Nasr; Elsayed A. Sallamand F. E. Abd El-Samie "Efficient transmission of 1D and 2D chaotic map encrypted images with orthogonal frequency division multiplexing", Proc. SPIE 8285, International Conference on Graphic and Image Processing (ICGIP 2011), 82850D (September 30, 2011)

[15] Jiri Fridrich.." Symmetric Ciphers Based on Two-Dimensional Chaotic Maps." International Journal of Bifurcation and Chaos, Vol. 8, No. 6 , 1259-1284 1998.

[16] S. Li, ―Analyses and new designs of digital chaotic ciphers, Ph.D. dissertation, Info. And Comm. Eng., Xi'an Jiaotong Univ., China, 2007.

[17] C. Zhu and K. Sun, "Chaotic image encryption algorithm by correlating keys with plaintext," China Communications, vol. 9, no. 1, pp. 73–79, 2012.