Optik 127 (2016) 315–319

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

The Effect of Fractional Fourier Transform Angle in Encryption Quality for Digital Images

Heba M. Elhoseny[a], Osama S. Faragallah[b,e,*], Hossam E.H. Ahmed[a], Hassan B. Kazemian[c], Hala S. El-sayed[d], Fathi E. Abd El-Samie[a]

[a] Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[b] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[c] Intelligent Systems Research Centre, Faculty of Computing, London Metropolitan University, London, UK
[d] Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-kom 32511, Egypt
[e] Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya, 21974, Kingdom of Saudi Arabia

ARTICLE INFO

Article history:
Received 21 August 2014
Accepted 24 August 2015

Keywords:
Cryptography
Image cryptosystem
Chaotic Baker map
FrFT
Security analysis

ABSTRACT

This paper investigates the effect of the angle of the Fractional Fourier transform (FrFT) on encryption quality in a chaotic image cryptosystem. The adopted approach for encryption is 2D chaotic Baker map. This map is applied to the transformed images using FrFT with different angles. We inspect its application to digital images and its exhaustive security investigation. The security investigation contains statistical tests like histogram and correlation coefficient, the maximum and the irregular deviation metrics, and the processing time. Experimental results prove that the rotation angle of the FrFT does not affect the encryption quality. This indicates a wide range of angles that can be used in this transform domain for encryption in addition to increasing the scheme sensitivity and making it hard for the attacker to exactly determine the right angle used in the transform domain.

1. Introduction

In modern cryptography, chaos theory has achieved a prominent role [1]. The charisma of utilizing chaos as the backbone for providing cryptosystems is fundamentally due to significant characteristics of chaos like random behavior, initial conditions sensitivity, and parameter tuning which satisfy the classic Shannon demands of permutation and substitution. The significant features of the chaotic systems are proper for secure communications, like ergodicity, sensitivity to control parameters and initial conditions, and pseudo-randomness [2–3]. Many of these attributes of chaotic systems correspond to their equivalent counterparts in conventional cryptosystems. So, chaotic cryptography has become efficient substantial origin for modern ciphers [4–8].

Applying chaotic systems in real number domain may cause speed restrictions and decadence in their random like nature that produce another problems like small cycle range, high-correlation and non-ideal distribution [9]. Also, permutation with spatial domain keeps the statistical features of the scrambled image after permutation. Performing permutation for image in spatial domain is not compact since the attacker may employ some features of permuted image to retrieve the original image.

The FrFT is a widely utilized tool in signal analysis [10]. If image encryption is carried in the FrFT domain, a larger degree of security is obtained. The FrFT angle is another factor that should be known by the attacker to break the encryption system. Furthermore, the complexity of the FrFT is acceptable as compared to the traditional Fourier transform [11].

In this paper, we study the effect of the angle of the FrFT on encryption quality in a chaotic image cryptosystem. The encryption algorithm applied is 2D chaotic Baker map. This map is applied to the transformed images using FrFT domain with different angles. Test results and evaluation metrics of the proposed scheme with different angles have been discussed.

The following sections of paper can be arranged as: Section 2 reviews the FrFT. Section 3 presents the chaotic Baker map. Section 4 introduces the proposed image cryptosystem with the chaotic Baker map. Section 5 explores security investigation and the obtained results. Finally, paper conclusion is presented in Section 6.

* Corresponding author at: Faculty of Electronic Engineering, Computer Science and Engineering, Elgamea, Menouf, Egypt. Tel.:+20 482239490..

http://dx.doi.org/10.1016/j.ijleo.2015.08.152
0030-4026/

2. Fractional Fourier transform

The Fourier Transform (FT) is a widely utilized tool in signal analysis. The FrFT is a generalization concept of the FT [10,12]. A kernel-based integral transformation of the FrFT has the following form [13]:

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

where, K_α is the form of the kernel-based integral transformation for defining the FrFT.

The FrFT of a function x, with an angle α, can be represented with $R^\alpha = X^\alpha$,

$$X_\alpha(u)=\int_{-\infty}^{\infty}x(t)k_\alpha(t,u)\mathrm{d}t \tag{2}$$

Using the formulations in Eqs. (1) and (2), we can get [13]:

$$\begin{aligned}f_a(u)&=F^a[f(x)]\\&=C_\alpha\int f(x)\exp\left[i\pi\frac{u^2+x^2}{\tan\alpha}-2i\pi\frac{ux}{\sin\alpha}\right]\mathrm{d}x\end{aligned} \tag{3}$$

where $\alpha=\frac{a\pi}{2}$ and $C_\alpha=\frac{\exp-\left[i\left(\frac{\pi\sin(\sin(\alpha))}{4}-\frac{\alpha}{2}\right)\right]}{|\sin\alpha|^{1/2}}$

F^a defines the transform from coordinates (t, w) counterclockwise to coordinates (u, v) with angle α in time-frequency plane as illustrated in Fig. 1. From [14], we can see that F^0 means zero rotation.

$F^{\pi/2}$: FT operator
F^{π}: time reverse operator
$F^{3\pi/2}$: inverse FT operator
$F^{2\pi}$: I: 2^π rotation
$F^\beta F^\alpha = F^{\beta+\alpha}$ additives.

3. Chaotic Baker map

3.1. The two-dimensional Baker map

The chaotic Baker map, *CBM* is defined as [15]:

$$\begin{aligned}CMB(x,y)&=(2x,y/2)\quad \text{when}\quad 0\le x<1/2\\ CMB(x,y)&=(2x-1,y/2+1/2)\quad \text{when}\quad 1/2\le x\le 1\end{aligned} \tag{4}$$

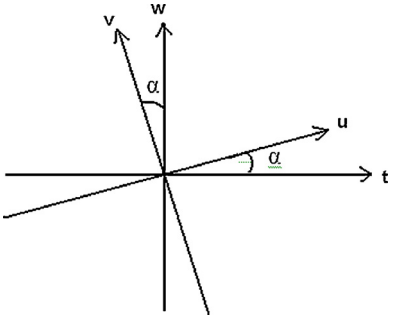

Fig. 1. The original coordinates (t, w) rotate to coordinates (u, v) with angle α in time-frequency plane.

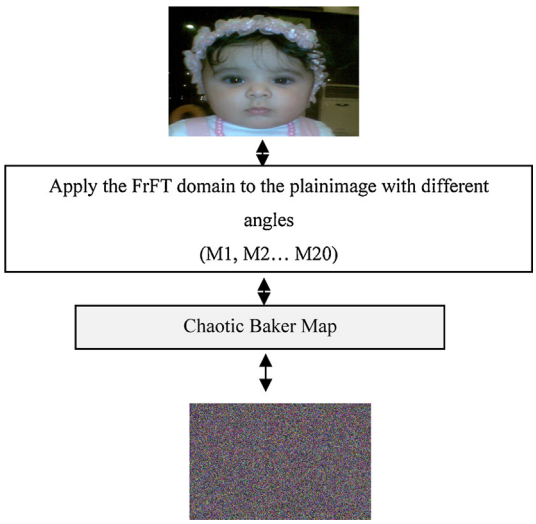

Fig. 2. Block diagram for the proposed image cryptosystem.

3.2. Generalized Baker map

The generalized Baker map is obtained by splitting the square into t vertical rectangles $[H_{j-1}, H_j]\times[0,1]$, $j=1,\ldots,t$, $H_j=p_1+\ldots+p_j$, $H_0=0$ such that $p_0+\ldots+p_t=1$. The lower right corner of the j-th rectangle is placed at $H_{ji}=p_1+\ldots+p_j$. The generalized Baker map stretches each rectangle horizontally by the factor of $1/p_j$. At the same time, the rectangle is contracted vertically by the factor of p_j. Finally, all rectangles are accumulated on top of each other as described by the following equation:

$$CMB(x,y)=\left(\frac{1}{p_j}(x-H_j),p_jy+H_j\right),\quad \text{for}\quad (x,y)\in[H_j,H_j+P_j]\times[0,1]. \tag{5}$$

3.3. Discretized Baker map

The discretized generalized Baker map will be denoted $CBM(n_1,\ldots,n_t)$, where the sequence of t integers, $n_1,\ldots,n_t$ is selected such that each integer n_j divides N, and $n_1+\ldots+n_t=N$. Denoting $N_j=n_1+\ldots+n_j$, the pixel (r, s), with $N_j\le r<N_j+n_j$, and $0\le s<N$ is mapped.

$$CMB_{(n_1,\ldots,n_t)}(r,s)=\left[\frac{N}{n_i}(r-N_j)+s\mod\left(\frac{N}{n_j}\right),\frac{n_j}{N}\left(s-s\mod\left(\frac{N}{n_j}\right)\right)+N_j\right] \tag{6}$$

An $N\times N$ square is divided into vertical rectangles of height N and width n_i [15].

4. The proposed encryption algorithm

Fig. 2 illustrates a block diagram for the proposed image cryptosystem.

5. Test results and evaluation metrics

To study the effect of angle of the FrFT, we apply the encryption/decryption process of chaotic Baker map several times with

Table 1
Different angles of FrFT.

Angles	**M1**	**M2**	**M3**	**M4**	**M5**
(*x*,*y*)	(30,20)	(30,30)	(40,50)	(40,40)	(43,64)
Angles	**M6**	**M7**	**M8**	**M9**	**M10**
(*x*,*y*)	(20,31)	(22,37)	(78,83)	(45,45)	(0,10)
Angles	**M11**	**M12**	**M13**	**M14**	**M15**
(*x*,*y*)	(0,22)	(0,35)	(0,40)	(0,73)	(0,95)
Angles	**M16**	**M17**	**M18**	**M19**	**M20**
(*x*,*y*)	(20,0)	(34,0)	(46,0)	(60,0)	(82,0)

different angles and apply the encryption quality metrics again to judge the effect of them. Twenty different angles have been used as shown in Table 1.

5.1. Histogram test

A histogram test illustrates pixels distribution in the image. This is achieved by sketching pixels number for each gray-level value appeared in the image [16].

Fig. 3 shows encrypted image histogram utilizing chaotic Baker map with different angles of FrFT. It appears identical to original image histogram as this map depends only on scrambling that maintains most of the image characteristics. Here the difference of angles does not affect the histogram analysis of the encrypted images.

5.2. Correlation coefficient test

Correlation coefficient CC is employed to determine the relation between the original image and its corresponding encrypted one [17]. Strong encryption implies small values for the CC. The CC is calculated using the following equation:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{7}$$

$$D(x) = \frac{1}{L}\sum_{l=1}^{L}(x_l - E(x))^2, \quad cov(x,y)$$
$$= \frac{1}{L}\sum_{l=1}^{L}(x_l - E(x))(y_l - E(y)), \quad E(x) = \frac{1}{L}\sum_{l=1}^{L}x_l \tag{8}$$

where, x and y represent gray-scale pixel values of the source and ciphered images.

5.3. Maximum deviation test

This measure investigates the encipherment power in a way that estimates how much it enlarges the variance between the source and the ciphered images. The MD is estimated using the following equation [17]:

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=0}^{255} h_i \tag{9}$$

where, h_i represents the absolute difference curve amplitude at value i. High value of the MD implies that the encrypted image is more different compared with the source image.

5.4. Irregular deviation test

The Irregular Deviation relies on how much the divergence resulted from the encipherment process becomes infrequent [45].

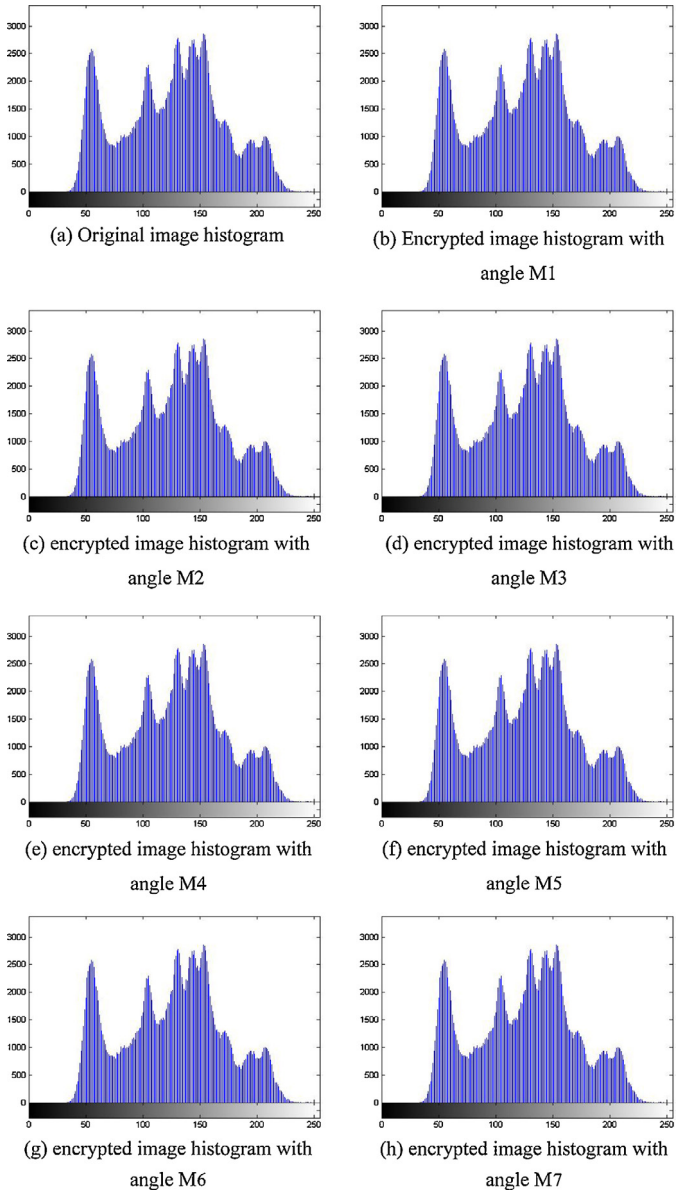

Fig. 3. Histogram of the encrypted image using chaotic Baker map using various angles of FrFT.

It yields indication about the resulted divergence at each pixel of the source image. [17]:

$$D = |I - J| \tag{10}$$

where I, J are source and ciphered images, respectively.

$$\mathrm{DC} = \frac{1}{255}\sum_{i=0}^{255} h_i \tag{11}$$

where, h_i defines the absolute difference histogram amplitude at value i.

$$\mathrm{AC}(I) = |H(i) - \mathrm{DC}| \tag{12}$$

$$\mathrm{ID} = \sum_{i=0}^{255} \mathrm{AC}(i) \tag{13}$$

Low ID values indicate a powerful cipher.

Table 2
Encryption quality results.

Angles of FrFT domain	CC	MD	ID	T (in s)
M1	0.0057	56,029	253,262	4.127
M2	0.0092	56,029	253,260	4.246
M3	0	56,029	251,510	4.063
M4	0.005	56,029	253,298	4.118
M5	0	413,420	186,646	4.031
M6	0.0092	405,310	186,922	4.456
M7	0.0096	405,310	186,916	4.251
M8	0.0096	405,310	186,916	4.162
M9	0.00003	393,440	187,566	4.381
M10	0	56,029	251,510	5.12
M11	0	56,029	251,510	5.128
M12	0.0092	405,310	186,922	4.243
M13	0.0052	56,029	253,298	4.80
M14	0.0092	405,310	186,922	4.26
M15	0	56,029	251,510	4.969
M16	0.0050	56,029	253,298	4.77
M17	0.0057	56,029	253,262	4.77
M18	0.0057	56,029	253,262	4.38
M19	0.0057	56,029	253,298	4.26
M20	0	413,420	186,648	4.49

Table 2 illustrates the encryption quality results for the encrypted images using different angles of the FrFT, where M_1,. . ., M_{20} indicates the angles used in the FrFT, CC indicates the correlation coefficient, MD indicates the maximum deviation metric, ID indicates the irregular deviation metric, and T(s) indicates the processing time for the encryption process. From obtained results in Table 2, we can see that the correlation coefficients with different angles have lower values indicating a good correlation. Also the difference of angles does not affect the correlation. The maximum deviation values of all encrypted images with different angles have high. The irregular deviation values are almost low and close indicating that the difference of angles does not affect the encryption quality. Finally, the processing times of the encryption process with all angles are very close.

5.5. Sensitivity test

To examine sensitivity of the proposed scheme to the difference of rotation angles, we encrypt the transformed image using FrFT with angle (20,30) and apply decryption algorithm with the same angle and angle (21,30). Fig. 4 shows the obtained results.

Table 3 shows the correlation coefficient between source and ciphered images with two different angles (20,30), (21,30). Fig. 4 and Table 3 prove the sensitivity of the proposed scheme to tiny changes in angle, so it is very hard to detect the right angle used in the transform.

The experimental results verify and prove that the angle of rotation of the FrFT does not affect the quality of image encryption. This is considered as a good property for the FrFT as it allows a wide range of angles without restrictions. So, it is very hard to any attacker to exactly expect the angle used in the domain. This increases the sensitivity of the transform. Simulation results has proved that the FrFT has the following advantages:

a. The encrypted image A with angle (20,30) b. The decrypted image B with angle (20,30) c. The decrypted image C with angle (21,30)

Fig. 4. Encryption and decryption with different angles

Table 3
Sensitivity test.

CC between original image and B	1
CC between original image and C	0.0542

(A). Using FrFT domain to analyze signal is simple and the computational complexity of the FrFT is acceptable.
(B). It does not affect image or cause any distortion, as correlation between the reconstructed image and the original image is equal to one.
(C). It provides a high level of security, as a small change in angels used for decryption causes a great distortion in the reconstructed image.
(D). We can use FrFT for super resolution and encryption.
(E). Filtering in FrFT domain allows decreasing the mean square error in estimating distorted and noisy signals.

For these reasons, the FrFT has a superior performance in encryption applications.

6. Conclusion

This paper presented an algorithm for encryption that depends on applying 2D chaotic Baker map in the FrFT domain with various angles. Various angles have been utilized to determine the effect rotation in FrFT domain. Experimental results and discussion demonstrated that the rotation angle of the FrFT does not affect the encryption quality. This implies that a wide range of angles can be used in this transform domain for encryption. So, it is so hard for the attacker to reconstruct the original image, because he needs initially to guess the exact rotation angle and then break the chaotic encryption algorithm.

References

[1] S. Li, Q. Li, W. Li, X. Mou, Y. Cai, Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding, IMA Int. Conf. Crypt Coding 2260 (2001) 205–221.
[2] F. Dachselt, W.S. Chwarz, Chaos and cryptography, IEEE Trans. Circuits Syst. Part I: Fundam. Theory Appl. 48 (12 (Dec.)) (2001) 1498–1508.
[3] K. Kelber, W. Schwarz, General design rules for chaos-based encryption systems, in: International Symposium on Nonlinear, Theory and its Applications (NOLTA2005), Bruges, Belgium, 18–21 October, 2005, pp. 465–468.
[4] J.C. Yen, J.I. Guo, A new hierarchical chaotic image encryption algorithm and its hardware architecture, Proceedings of the 9th VLSI Design/CAD Symposium, Taiwan, 1998, pp. 358–362.
[5] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurc. Chaos 8 (6) (1998) 1259–1284.
[6] W. Xiao, J. Zhang, W. Wu, A watermarking algorithm based on chaotic encryption, Proc. IEEE Tencon (2002) 545–548.
[7] S. Li, X. Zheng, On the security of an image encryption method, Proc. IEEE Int. Conf. Image Process. (ICIP) 2 (2002) 925–928.
[8] M. Ashtiyani, P.M. Birgani, H.M. Hosseini, Chaos-based medical image encryption using symmetric cryptography, Proceedings of the 3rd International Conference on Information and Communication Technologies from Theory to Applications (ICTTA), 7–11 April 2008, pp. 1–5.
[9] G. Jakimoski, L. Kocarev, Chaos and cryptography block encryption ciphers based on chaotic maps, IEEE Trans. Circuits Syst. Part I: Fundamental Theory Appl. 48 (2 (February)) (2001) 163–169.
[10] A.C. McBride, F.H. Kerr, On Namias' Fractional Fourier transforms, IMA J. Appl. Math. 39 (1987) 159–175.
[11] A. Bultheel, H. Martinez, A shattered survey of the Fractional Fourier Transform, December 2003, pp. 38–45.
[12] H.M. Ozaktas, Fractional Fourier domains, Signal Process. 46 (1995) 119–124.
[13] H.M. Ozaktas, Z. Zalevsky, M.A. Kutay, The Fractional Fourier transform, Wiley, Chichester, 2001.

[14] H.M. Elhosany, H.E. Hossin, A.M. Abbas, H.B. Kazemian, O.S. Faragallah, S.M. El-Rabaie, F.E. Abd El-Samie, Chaotic encryption of images in the Fractional Fourier transform domain using different modes of operation, Signal, Image Video Process. 7 (3 (May)) (2013) (ISSN 1863-1703).
[15] Y. Mao, G. Chen, S. Lian, A novel fast image encryption scheme based on 3D chaotic Baker maps, Int. J. Bifurc. Chaos 14 (10) (2003) 3613–3624 (June).
[16] I.F. Elashry, O.S. Farag Allah, A.M. Abbas, S. El-Rabaie, F.E. Abd El-Samie, Homomorphic image encryption, J. Electron. Imaging 18 (3) (2009), 033002(1-14).
[17] Nawal El-Fishawy, M. Osama, A. Zaid, Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms, Int. J. Netw. Secur. 5 (3 (Nov)) (2007) 241–251.