Image Encryption Based on Fractional-Order Chaotic Generators

Ahmed G. Radwan[†‡], Salwa K. Abd-El-Hafiz[†] and Sherif H. AbdElHaleem[†]

† Engineering Mathematics Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt
‡ Nanoelectronics Integrated Systems Center (NISC), Nile University, Egypt
Email: agradwan@ieee.org, salwa@computer.org, sherifHamdyNet@hotmail.com

Abstract–This paper discusses a simple encryption system based on the fractional-order Lorenz and Rossler attractors. This system consists of a delay element, a multiplexer and the fractional-order generator. Four new parameters are added in the encryption key due to the fractional-implementation of the attractors. Those parameters are the three fractional-order parameters as well as a reset parameter, which decides the long-memory dependence. Encryption analyses of the proposed system, which include correlation coefficients, differential attack measures, histograms, NIST test suite and sensitivity analysis with respect to different key parameters, are evaluated for two different resolutions.

1. Introduction

Although the fractional calculus (non-integer derivatives and integrals) concept has been known for more than three centuries, huge research activities have been initiated in different fields during the last five decades due to the introduction of the rational approximations. The high impact of fractional calculus stems from its ability to interpret practical and complex phenomena better than integer-order calculus. Some of the advantages of the fractional order derivative in dynamical systems are that it gives extra degree(s) of freedom and it has long memory dependence unlike the integer calculus [1].

Many applications have been generalized in the fractional-order domain such as in tissue modeling [2], biomedical applications [3], and new charts have been patented as 3D Smith-chart [4]. The definition of Caputo fractional derivative is given by [1]:

$$D^{\alpha} f(t) = \frac{1}{\Gamma(1-\alpha)} \int_{0}^{t} \frac{f'(\tau)\, d\tau}{(t-\tau)^{\alpha}}\ , 0 < \ \alpha < 1. \qquad (1)$$

Pseudo Random Number Generators (PRNGs) are essential in recent applications to secure data and communication networks. Generally, most of the recently introduced PRNGs are based on chaotic systems whose behavior is sensitive to parameters and initial conditions. Lorenz and Rossler systems of ordinary differential equations are well-known chaotic generators. One of the recent applications, which uses these PRNGs, is image and video encryption systems that protect miscellaneous data ranging from personal data to military codes [5]. In addition, many recently proposed chaotic generators, which are based on analog and digital designs, are suitable for encryption applications (e.g., [6, 7]).

Although image encryption can be based on chaotic and non-chaotic generators [8], the encryption quality depends on many factors such as the size and sensitivity of the encryption key. Recently, fractional-order encryption based on Lorenz system was introduced [9] by the authors but the system was neither optimized nor simple. This paper introduces a simple encryption system based on one delay element and a simple multiplexer along with the fractional-order Lorenz or Rossler attractors. The encryption key can be controlled by the extra degrees of freedom as well as the reset parameter added in the proposed system.

2. Fractional-Order Lorenz System

Consider the following fractional-order system:

$$D_{*}^{\alpha}\, x(t) = f(x(t), t)\ , 0 < t < T, 0\ < \alpha < 1, \qquad (2)$$

where its solution can be expressed as

$$x(t) =\ x_0 + \frac{1}{\Gamma(\alpha)} \int_{0}^{t} (t-\tau)^{\alpha-1} f(x(t), \tau) d\tau. \qquad (3)$$

2.1 Adams-Bashforth predictor-corrector scheme

The steps for this numerical technique [12] is to evaluate

$$b_{j,n+1} = \frac{h^{\alpha}}{\alpha}((n-j+1)^{\alpha} - (n-j)^{\alpha}), \qquad 0 \leq j \leq n, \qquad (4)$$

where h and t_j are given by $h = \left(\frac{T}{N}\right)$, $t_j = jh$ and $j = 0, 1, \ldots, N$. Then, calculate the predictor x^p as

$$x^p(t_{n+1}) = x_0 + \frac{1}{\Gamma(\alpha)} \sum_{j=0}^{n} b_{j,n+1} f(x(t_j), t_j). \qquad (5)$$

Finally, calculate the new value $x(t_{n+1})$ by:

$$x(t_{n+1}) = x_0 + \frac{h^{\alpha}}{\Gamma(\alpha+2)} f(x^p(t_{n+1}), t_{n+1}) + \frac{h^{\alpha}}{\Gamma(\alpha+2)} \sum_{j=0}^{n} a_{j,n+1} f\big(x(t_j), t_j\big), \qquad (6a)$$

$$a_{j,n+1} = \begin{cases} n^{\alpha+1} - (n-\alpha)(n+1)^{\alpha} & j = 0 \\ (n-j+2)^{\alpha+1} + (n-j)^{\alpha+1} - 2(n-j+1)^{\alpha+1} & j \leq n^{\cdot} \end{cases} \qquad (6b)$$

2.2 Fractional-order Lorenz system

The fractional-order Lorenz system is defined as:

$$\frac{d^{\alpha}x}{dt^{\alpha}} = \ -10(y-x), \qquad (7a)$$

$$\frac{d^{\beta}y}{dt^{\beta}} = \ -xz + (24-16)x + 4y, \qquad (7b)$$

$$\frac{d^{\gamma}z}{dt^{\gamma}} = xy - \frac{8}{3}z, \qquad (7c)$$

and the fractional order Rossler system is defined by:

$$\frac{d^{\alpha}x}{dt^{\alpha}} = -y - z, \qquad (8a)$$

$$\frac{d^{\beta}y}{dt^{\beta}} = x + 0.43y, \qquad (8b)$$

$$\frac{d^{\gamma}z}{dt^{\gamma}} = 2 + z(x-4), \qquad (8c)$$

where α, β and $\gamma > 0$ determine the fractional-order of the equations. Therefore, the response of the fractional-order Lorenz and Rossler systems can be evaluated using equations (4) - (6).

2.3 Strange attractors

Figure 1 shows the Z output for two fractional-orders $\alpha = 0.8, 0.95$ and $\beta = \gamma = 1$. It is clear that the behavior of the fractional-order Lorenz system changes as the fractional-order changes but remains in the chaotic range [9].

3. The Simplest Fractional-Order Encryption System

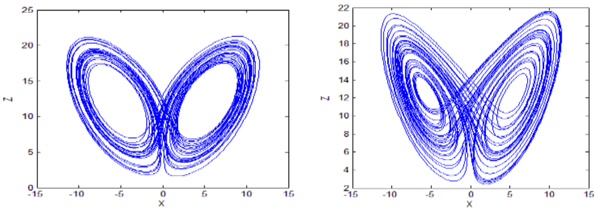
The block diagram of the proposed encryption process is given in Fig. 2, where a delay element and a multiplexer are used. The $X, Y,$ and Z outputs of the fractional-order system are calculated. Then, the least significant 8 bits from each of them are extracted because they have more chaotic responses [8, 9]. To enhance the encryption output, each encrypted pixel should depend on the previous values, which is realized here by the delay element.

Moreover, the nonlinear multiplexer is added to increase the complexity of the encryption system, where the least significant three bits of the previous encrypted pixel are the control parameters as shown in Table I. From (5) and (6), calculation of the new values of Lorenz or Rossler variables requires the previous n values, which need more storage and processing time.

To simplify this process, a reset parameter is added as shown in Fig. 2 for two reasons; to limit the long term dependency to a reasonable number and to increase the length of the encryption key. Therefore, the values of the RGB encrypted pixel depend on the previous encrypted values, under the multiplexer effect, as well as the output of the fractional-order chaotic system. Please note that the scanning of the input image is performed row-by-row until the whole image is encrypted.

3.1 Encryption key

Based on the previous discussion, the encryption key consists of seven components for both fractional-order Lorenz and Rossler systems, which are the fractional-order parameters, the initial values and the reset parameter as shown in Table II. The length of the proposed encryption key is 200 bits, which is long enough to resist brute-force attacks. It is to be noted that this encryption key can be increased by adding the three conventional parameters and in this case the key length will be 296 bits.



(a) (b)

Fig. 1. Strange attractor for the fractional-order Lorenz system with (a) α = 0.8 and (b) α = 0.95

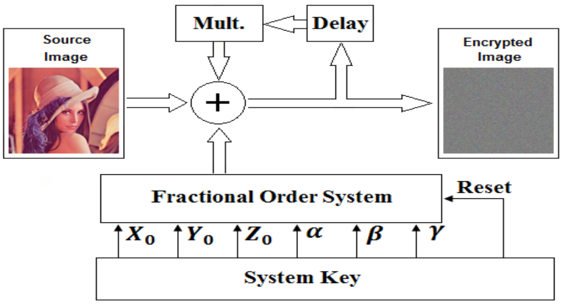


Fig. 2. The proposed simplest fractional-order image encryption system

Table I: Multiplexing table

Selection bits			R_{out}	G_{out}	B_{out}	Selection bits			R_{out}	G_{out}	B_{out}
R_{LSB}	G_{LSB}	B_{LSB}				R_{LSB}	G_{LSB}	B_{LSB}			
0	0	0	B	R	G	1	0	0	G	B	R
0	0	1	G	B	R	1	0	1	R	B	G
0	1	0	R	G	B	1	1	0	B	G	R
0	1	1	B	R	G	1	1	1	G	R	B

Table II: The proposed encryption key

	α	β	γ	X_0	Y_0	Z_0	Reset
# of bits	32	32	32	32	32	32	8
Lorenz	0.9399	0.9899	0.9899	4.6379	7.1289	5.8229	200
Rossler	1.0349	1.0349	1.0349	0.0999	0.1999	0.2999	200

4. Encryption Results and Analysis

The proposed encryption system is tested using the colored version of Lena with two different resolutions and the following analyses are evaluated to measure the quality of the encrypted images.

4.1 Histogram analysis

Figure 3 shows the histogram results of the original and encrypted RGB image components, which illustrate the disappearance of peaks and the uniform distribution of all colors after the encryption process.

4.2 Pixel correlation analysis

Conventional image pixels are highly correlated in horizontal, vertical and diagonal directions. Hence, one of the main objectives of any good encryption system is to eliminate these dependencies [10]. Figure 4 shows these correlations before and after the encryption process. The averages of the correlation coefficients drop down from approximately 0.938, 0.965 and 0.92 in case of Lena 256×256 for horizontal, vertical and diagonal directions, respectively, to the order of 10^{-3} for Lorenz and Rossler fractional-order systems as shown in Table III for different resolutions.

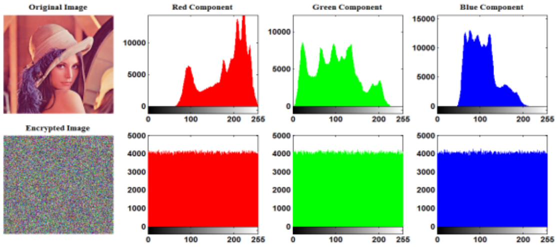


Fig. 3. The histogram RGB components of the original and encrypted Lena 1024 × 1024 images.

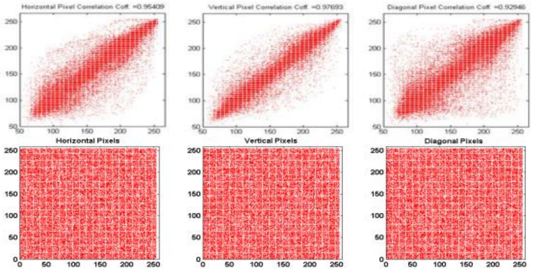


Fig. 4. Horizontal, vertical and diagonal pixel correlations for the original and encrypted Lena 256 × 256 images

4.3 Differential attack measures

Differential attack measures (MAE, NPCR, UACI) indicate the effect of one pixel change in the original image on the encrypted image as per their definitions in [11]. Table III shows the average of 20 random cases of pixel changes of these measures for two different resolutions of colored Lena image. It is clear from these values that better encryption is obtained for the high resolution case where the MAE, NPCR and UACI values approach their optimum values without the use of permutation techniques.

4.4 NIST test suite

The NIST statistical test suite 800-22 is a standard measure of the encrypted image randomness [12]. Table IV shows the results of the 15 NIST tests for the fractional-order Lorenz and Rossler generators where the encrypted images passed all the tests and, hence, the randomness of the encrypted image is inferred.

4.5 Sensitivity Analysis

One of the critical measures for a good encryption system is the sensitivity of its key, which can be tested by changing the value of any bit and inspecting the wrong decrypted image. Evaluation of the wrong decrypted images can be performed using the Mean Square Error (MSE) and entropy. The wrong decrypted images for three different cases with two different resolutions for the two generators are discussed as shown in Table V. These cases depend on changing the least significant bit of the parameters α, X_0 and Reset, respectively. It is clear that the output of the proposed system is very sensitive to each component in the encryption key.

Table VI shows the calculations of the MSE and entropy for the three different wrong decrypted images. From this Table, the MSE values indicate how far the wrong decrypted image is from the correct one and the entropy values approach their maximum value of 8, which reflect the randomness.

5. Conclusions and Future Work

The fractional-order domain gives extra degrees of freedom per system dimension and this helps in securing the key generation. Also, it increases the range of system parameters in which the system can be chaotic. The proposed system has three extra degrees of freedom more than the conventional Lorenz or Rossler cases. Moreover, strong sensitivity to system parameters makes chaotic generators more practical for use in image encryption. The sensitivity of the fractional-order parameters has been tested by changing the lease significant bits and the results were very satisfactory. Future work includes enhancing the encryption algorithm by adding a permutation stage for image pixels. Our current implementation uses stream encryption, which works on each pixel separately. This work can be extended to block-based encryption, which will be more secure.

References

[1] K. Diethelm, “An Algorithm for The Numerical Solution of Differential Equations of Fractional Order,” Elec. Transact. Numer. Anal. 5, 1-6, 1997.

[2] R.L. Magin, Fractional Calculus in Bioengineering. Redding, CT: Begell House, 2006.

[3] K. Moaddy, A.G. Radwan, K.N. Salama, S. Momani, I. Hashim, “The Fractional-Order Modeling and Synchronization of Electrically Coupled Neurons System,” Computers and Mathematics with Applications, 64, 3329-3339, 2012

[4] A.G. Radwan, A. Shamim, K.N. Salama, “Fractional Order Element Based Impedance Matching", US 2012/0123750 Patent, 2012.

[5] N. Ferguson, B. Schneier and T. Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing, 2010.

[6] A.G. Radwan, A.M. Soliman, and A.-L. EL-sedeek, "MOS realization of the modified Lorenz chaotic system," Chaos, Solitons & Fractals, (21), 553-561, 2004.

[7] A.G. Radwan, A.M. Soliman, and A.S. Elwakil, "1-D digitally-controlled multi-scroll chaos generator," Int. J. Bifurcation & Chaos, 17, 1, 227-242, 2007

[8] A.G. Radwan, S.H. AbdElHaleem, S.K. Abd-El-Hafiz “Symmetric Encryption Algorithms Using Chaotic and Non-Chaotic Generators: A Review,” Journal of Advanced Research, DOI:10.1016/j.jare.2015.07.002.

[9] A.G. Radwan, S.K. Abd-El-Hafiz, S.H. Abd-El-Haleem, "Image Encryption in the Fractional-Order Domain," International Conference on Engineering and Technology (ICET 2012), 1-6, 2012.

[10] E.B. Corrochano, Y. Mao, G. Chen, "Chaos-based image encryption: Handbook of Geometric Computing," Springer, 231-265, 2005.

[11] Y. Wu, J.P. Noonan, S. Agaian, "NPCR and UACI randomness tests for image encryption," J. Selected Areas in Telecommun., 31-38, 2011.

[12] A. Rukhin, et al., "A Statistical test suite for random and pseudorandom number generators for cryptographic applications" NIST Special Publication 800-22, 2001.

Table III: The correlation coefficients and differential attack measures for two different resolutions of Lena image

	Lorenz (Lena 256 × 256)			Lorenz (Lena 1024×1024)			Rossler (Lena 1024×1024)		
	H	**V**	**D**	**H**	**V**	**D**	**H**	**V**	**D**
Red	-0.0028	-0.0027	0.0052	0.0004	-0.0009	-0.0003	-0.0008	0.0001	-0.0002
Green	-0.0016	-0.0066	-0.0036	-0.0029	-0.0006	0.0007	-0.0003	0.0003	-0.0009
Blue	-0.0073	0.0042	0.0027	-0.0004	-0.0017	0.0010	-0.0024	0.0004	0.0004
Average	0.0039	0.0045	0.0038	0.0012	0.0011	0.0007	0.0012	0.0003	0.0005
	MAE	**NPCR %**	**UACI %**	**MAE**	**NPCR %**	**UACI %**	**MAE**	**NPCR %**	**UACI %**
Red	84.4256	46.8452	15.7267	84.2355	86.4153	29.0217	84.2197	86.4147	29.0349
Green	77.8605	46.8586	15.7428	77.9644	86.4193	29.0447	78.1030	86.4178	29.0351
Blue	70.4003	46.8485	15.7253	70.3602	86.4169	29.0328	70.3823	86.4184	29.0283
Average.	77.5621	46.8508	15.7316	77.5200	86.4171	29.0331	77.5683	86.4170	29.0328

Table IV: The results of NIST test suite for Lena image with resolution 1024 × 1024

Test	**Lorenz**				**Rossler**			
	P-VALUE		**PROPORTION**		**P-VALUE**		**PROPORTION**	
Frequency	0.048716	✓	0.958	✓	0.534146	✓	1.000	✓
Block Frequency	0.002971	✓	1.000	✓	0.066882	✓	1.000	✓
Cumulative Sums	0.425214	✓	0.958	✓	0.208684	✓	1.000	✓
Runs	0.350485	✓	0.958	✓	0.213309	✓	1.000	✓
Longest Run	0.012650	✓	1.000	✓	0.350485	✓	1.000	✓
Rank	0.739918	✓	0.958	✓	0.162606	✓	1.000	✓
FFT	0.534146	✓	1.000	✓	0.534146	✓	1.000	✓
Non Overlapping Template	0.375234	✓	0.993	✓	0.339083	✓	0.989	✓
Overlapping Template	0.006196	✓	1.000	✓	0.437274	✓	1.000	✓
Universal	0.048716	✓	1.000	✓	0.162606	✓	1.000	✓
Approximate Entropy	0.122325	✓	1.000	✓	0.437274	✓	1.000	✓
Random Excursions	0.233453	✓	0.992	✓	0.112370	✓	1.000	✓
Random Excursions Variant	0.165844	✓	0.996	✓	0.088830	✓	1.000	✓
Serial	0.404928	✓	1.000	✓	0.281897	✓	0.979	✓
Linear Complexity	0.213309	✓	1.000	✓	0.275709	✓	1.000	✓

Table V: The encrypted, correct decrypted and three wrong decrypted images of Lena for different resolutions

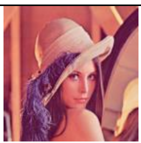
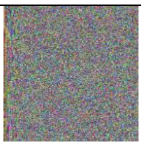
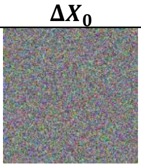
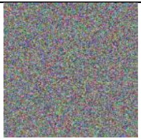
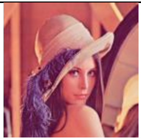
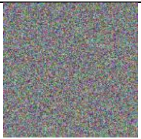
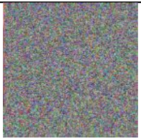
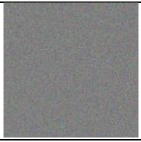
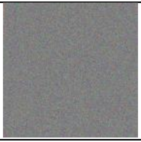
		Encrypted Image	**Decrypted Image**	**Wrong Decrypted $\Delta\alpha$**	**Wrong Decrypted ΔX_0**	**Wrong Decrypted ΔReset**
Rossler	**Lena (256 × 256)**					
Lorenz	**Lena (256 × 256)**					
	Lena (1024 × 1024)					

Table VI: MSE and entropy results of different correct and wrong decrypted images with different resolutions

	Image	**Case**	**MSE**			**Entropy**		
			R	G	B	R	G	B
Rossler	**Lena 256 × 256**	Exact	0.00	0.00	0.00	7.2353	7.5683	6.9176
		Wrong Decrypted $\Delta\alpha$	10502.33	9000.80	6862.06	7.9971	7.9976	7.9972
		Wrong Decrypted ΔX_0	10577.68	8950.17	7078.34	7.9967	7.9972	7.9972
		Wrong Decrypted ΔReset	10589.88	9007.03	7060.99	7.9971	7.9972	7.9970
Lorenz	**Lena 256 × 256**	**Wrong Decrypted $\Delta\alpha$**	10545.14	9019.71	7060.10	7.9968	7.9972	7.9969
		Wrong Decrypted ΔX_0	10616.61	9028.90	7099.40	7.9972	7.9972	7.9972
		Wrong Decrypted ΔReset	10585.58	8914.07	7047.67	7.9971	7.9971	7.9971
	Lena 1024 × 1024	Exact	0.00	0.00	0.00	7.2516	7.5919	6.9491
		Wrong Decrypted $\Delta\alpha$	10626.49	9049.56	7107.42	7.9998	7.9998	7.9998
		Wrong Decrypted ΔX_0	10629.66	9053.20	7109.69	7.9998	7.9998	7.9998
		Wrong Decrypted ΔReset	10633.12	9053.49	7084.28	7.9998	7.9998	7.9998