

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/358241751>

Image Encryption Through Rössler System, PRNG S-Box and Recamán's Sequence

Conference Paper · January 2022

DOI: 10.1109/CCWC54503.2022.9720905

CITATIONS

15

READS

211

5 authors, including:



[Mohamed khaled Elbeltagy](#)

The German University in Cairo

10 PUBLICATIONS 59 CITATIONS

[SEE PROFILE](#)



[Wassim Alexan](#)

The German University in Cairo

70 PUBLICATIONS 1,035 CITATIONS

[SEE PROFILE](#)



[Hisham H. Hussein](#)

Universities of Canada in Egypt

20 PUBLICATIONS 240 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Performance Analysis of Wireless Networks with Multiple DF Relay Nodes [View project](#)



Performance Analysis of Wireless Networks with Multiple AF Relay Nodes [View project](#)

Image Encryption Through Rössler System, PRNG S-Box and Recamán's Sequence

Mohamed ElBeltagy 
Wassim Alexan , SMIEEE
and Abdelrahman Elkharmy
Faculty of IET
The German University in Cairo
Cairo, Egypt
wassim.alexan@ieee.org
mohamed.elbeltagy@ieee.org

Mohamed Moustafa
Faculty of Informatics and Computer Science
Administrative Capital,
The German International University in Cairo
Cairo, Egypt
mohamed.dawood@student.giu-uni.de

Hisham H. Hussein
Faculty of Science and Innovation
Universities of Canada
Administrative Capital,
Cairo, Egypt
hisham.hussein@uofcanada.edu.eg

Abstract—This paper proposes a lightweight image encryption scheme that is based on 3 stages. The first stage incorporates the use of the Rössler attractor for the Rössler system, the second stage incorporates the use of a PRNG S-Box, while the third stage makes use of the Recamán's sequence. Performance of the proposed encryption scheme is evaluated using a number of metrics. The computed values of the metrics indicate a comparable performance to counterpart schemes from the literature, at a very low cost of processing time. Such a trait indicates that the proposed image encryption scheme possesses potential for real-time image security applications.

Keywords—Cryptography, image encryption, Rössler system, Recamán's sequence, S-Box.

I. INTRODUCTION

The tremendous evolution in digital image processing and network communications have created a great demand for real time secure image transmission over the Internet and through wireless networks [1]. Data security, through cryptography and steganography [2]–[7], has thus become a vital means to ensure safe and secure operation and usage of millions of online applications [8]. Cryptography, which plays a vital role in information security, has lured the attention of scientists and engineers, with contribution in its research and developments ascending in recent decades [9]–[11]. Global attempts focused lately on refining the security of image transmission, with novel cryptosystems proposed including cellular automata, DNA coding and chaos theory [12]–[14].

Chaos is characterized in pseudo-randomness, ergodicity and high sensitivity to initial conditions and parameters. Thus, it is extensively used in image encryption schemes. Results of such attempts have usually involved the usage of one or more PRNGs, as well as true RNGs. The literature on PRNGs incorporate examples pooling from chaos theory [15], [16], mathematical

sequences [17], electrical circuits [18], quantum physics [19], as well as many others.

The Rössler system is a third-order continuous-time system of differential equations with a single quadratic cross-term and depends on 3 parameters that were originally introduced by Otto Rössler in the 1970s [20]. These differential equations create a continuous time dynamical system that outcomes chaotic dynamics associated with the fractal properties of the attractor [21]. The calculated characteristics usually concern the generation of a single lobe chaotic attractor (spiral-type) following a period doubling cascade of a limit cycle, or a more complicate chaotic attractor (screw-type) due to the presence of homo-clinic orbits [22]. Some properties of the Rössler system can be concluded from linear methods such as eigenvectors, however the main features of the system require non-linear methods such as Poincaré maps and bifurcation diagrams. The original Rössler paper states the Rössler attractor was designed to operate likewise the Lorenz attractor, moreover it is also easier to analyze qualitatively [21].

The Recaman's sequence is an interesting sequence of integers that is very simple to define, but the resulting complexity exhibits how forceful it can be against cryptanalysis. The authors of [23] made use of Recaman's sequence image steganography for 2D images, where their proposed scheme led to excellent performance and resiliency against steganalysis.

In cryptography, an S-Box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext, thus ensuring Shannon's property of confusion. The first S-box used on symmetric key algorithms such

as Advanced Encryption Standard (AES) and the Data Encryption Standard (DES), but the main problem of such S-boxes is their statistic behavior. So, in order to produce a dynamic behavior, PRNG and chaotic systems are used to construct S-boxes, as in [24] and [25]. The authors of [26] introduced a novel approach to construct an S-box based on the Rössler system, where the effectiveness of the proposed S-box showed is well-exhibited in terms of being resistant against attacks. Another good example of a constructed S-box is that in proposed in [27]. The authors of [27] employ a novel transformation, modular inverse and permutation to construct their S-box. Performance evaluation and comparison against set benchmarks from the literature validate its cryptographic strength.

In this paper, we propose an image encryption scheme that is based on 3 stages. The first stage incorporates the use of Rössler system, while the second stage incorporates the use of S-Box and the third stage incorporates the use of Recamán's sequence. This paper is organized as follows. Section II briefly presents the Rössler system, followed by a PRNG S-Box and the Recamán's sequence used for the proposed image encryption scheme. Section III outlines the numerical results of the computations and testing and provides appropriate commentary on them. Section IV finally draws the conclusions of the paper and suggests a future work that can be further pursued.

II. THE PROPOSED IMAGE ENCRYPTION SCHEME

The proposed image encryption scheme is composed of three stages. The first stage makes use of the Rössler system, while second stages makes use of a PRNG S-Box, and in the third stage the Recaman's sequence was employed. The next few sections introduce each of those three concepts.

A. Rössler attractor

The Rössler system is an infamous prototype of a continuous dynamical system defined by the following set of 3 nonlinear differential equations:

$$\begin{aligned}\dot{x} &= (y + z) \\ \dot{y} &= x + ay \\ \dot{z} &= b + z(xc)\end{aligned}\quad (1)$$

where a , b and c are non-negative parameters. This well-known system approaches chaos through a period doubling bifurcation route. In the proposed encryption scheme, the employed parameter values are $a = 0.1$, $b = 0.01$ and $c = 14$ resulting in Fig. 1. Listing the computed x , y and z values in succession and plotting them against the iteration number yields a plot for the Rössler attractor points as shown in Fig. 2.

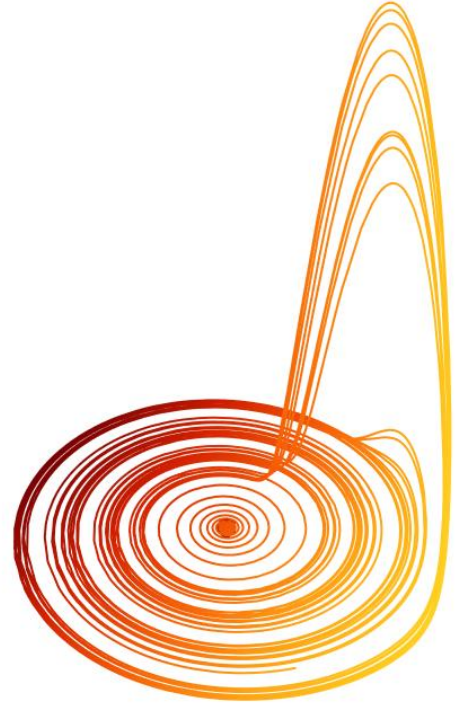


Fig. 1: Rössler attractor 3D graphical representation.

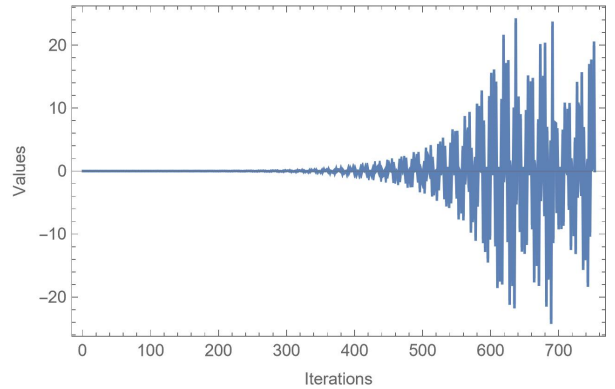


Fig. 2: Rössler attractor 2D graphical representation.

B. S-Box

A substitution-box is a pivotal constituent of modern-day block ciphers that helps in the generation of a muddled ciphertext for the specified plaintext. Through the incorporation of S-box, a nonlinear mapping among the input and output data is established to create confusion [28]. The security of data relies on the substitution process. Substitution is a nonlinear transformation which performs confusion of bits. It provides the cryptosystem with the confusion property described by Shannon [29]. In

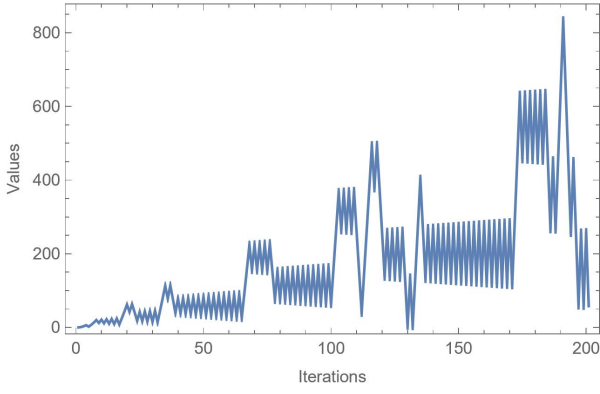


Fig. 3: The 2D shape of Recamán's sequence.

general, an S-box takes m input bits and transforms them into n output bits. This is called an mn S-box and is often implemented as a lookup table. These S-boxes are carefully selected to resist and obstruct linear and differential cryptanalysis. Through the incorporation of an S-box, a nonlinear mapping among the input and output data is established to create confusion [30], [31].

For the proposed encryption scheme, we randomly generate an S-box of dimensions 16×16 utilizing Wolfram Mathematica[®]. Table IV displays its values.

C. Recamán's Sequence

In order to generate the Recaman's sequence, one can let $a_1 = 1$ and follow the mathematical expression shown in (2) to generate its elements a_n .

$$a_n = \begin{cases} a_{n-1} - n, & \text{if } a_{n-1} - n > 0 \\ a_{n-1} + n, & \text{otherwise,} \end{cases} \quad (2)$$

where n is the position of the element in the sequence. This delivers the first few elements as 1, 3, 6, 2, 7, 13, 20, 12, 21, 11, 22, 10, 23, 9, ...

Fig. 3 is the 2D graphical representation for the first 200 iterations which are used in our proposed encryption scheme to generate a key of randoms bits.

D. Image Encryption and Decryption Processes

The proposed image encryption scheme is implemented as follows.

First, an image of appropriate dimensions is chosen, and then the image's pixels are converted into a 1D stream of bytes. Lastly, these bytes are converted into a bit stream d .

Second, the mean intensity of the image pixels is calculated. The resulting value is a rather small number, which we multiply by a magnifying factor f_M .

resulting value of the multiplication shall be denoted by μ .

Next, we cyclically shift d to the right by μ places and the resulting bit stream, now denoted d_μ , is then XORed with k_{CA} . k_{CA} is the first key, a bit stream of the same length as d and d_μ , that is made up of a repetition of the first N_{CA} bits resulting from the binary representation of the first 250 Rössler numbers in Rössler attractor. Let us denote the resulting bit stream as C_1 . This concludes the first step of encryption.

Next, the randomly generated S-Box is used for substituting the decimal representation for each 8 bits from the bitstream acquired after the first step as in Table IV. The randomly generated S-box is mainly used to provide 256 as total from 16 rows 16 columns randomly distributed numbers starting from 0 to 255, RandomSample function from Wolfram Mathematica[®] was used in order to satisfy this condition. Next, we change those resulted Decimal representations to a bitstream C_2 . At this point, we take the x and y coordinates of each of the points of the Recamán's sequence equations and flatten them into a single 1D array. Next, we list plot those values into 2D, as shown in Fig. 3.

Examining the plot in Fig. 3, we change those integer values to bits. This newly obtained bitstream of length N_L would make up the seed of our Recamán's sequence based key. We repeat those N_L bits until they are of the same length as d and C_1 , thus forming the second key. Let us denote it k_L .

Next, we XOR k_L with C_2 obtaining C_3 . This concludes the third step of encryption.

Finally, C_3 is reshaped back into an image of the same dimensions as those of the plain image, obtaining the encrypted image.

The decryption process is implemented in a reverse manner as to that of the encryption process.

III. NUMERICAL RESULTS AND PERFORMANCE EVALUATION

This section outlines the numerical results of the proposed image encryption scheme. Performance is evaluated and compared to counterpart algorithms found in the literature. The proposed scheme is implemented using the computer algebra system Wolfram Mathematica[®] on a machine running Windows 10 Enterprise. The PC is equipped with a 2.3 GHz 8-Core Intel[®] Core[™] i7 processor and 32 GB of 2400 MHz DDR4 of memory. The utilized keys are assigned the following values: $N_{CA} = 250$, $N_L = 200$ and $f_M = 10^6$. Four images that are commonly used in image processing applications/experimentation are utilized in this section.

These are Lena, Mandrill, Peppers and House, all of dimensions 256×256 .

The graphical representation denoted by Table II is a histogram representing the pixels distributions characteristics of sample images. As observable, the plain images (prior to encryption) and decrypted images' pixels are non-uniformly distributed on the histogram. In contrast to the histogram pixels distribution for the encrypted image which show a uniform pattern all along with the histogram. Noting that statistical analyses, attempts of breach and attacks do not yield any cryptanalytic results in comparison to those carried out on images of non-uniform distribution. Thus, this observation yields to that no information could be distinguished or determined from any of the characteristics of the encrypted images.

Fig. 4 shows the correlation coefficient diagrams of the plain and encrypted Lena image. It is clearly seen that the horizontal, vertical and diagonal correlation coefficients of the adjacent pixels for the plain image are linear. However, on inspecting the plots generated from the encrypted image, it is clear that the plots are uniform and have a scatter-like distribution. This signifies a resistance of the proposed scheme to statistical analyses or attacks.

A time-size complexity metric is utilized to assess the efficiency of the proposed image encryption scheme in order to identify whether the scheme is adequate for real-time applications. Table I displays the processing time required for encryption, decryption, and their summation for certain different standardized square image dimensions such as $\{128, 256, 512, 1024, 2048\}$. Furthermore, Table I shows that for an image dimensions of 128×128 , a decryption time of less than a single second is enough to successfully decrypt the image. In turn, this means that the proposed image encryption scheme is appropriate for real-time image exchange among handheld devices. This also translates into better resource management and optimization concerning the power consumed during image processing on the devices. Moreover, Table I shows that the amount of time required for the encryption-decryption process increases with increases in the dimensions of the image. This behavior is exhibited with a certain rate that starts to converge into a slower rate beyond an image dimensions of 1024×1024 .

Table III lists the computed values of MSE and PSNR of our proposed scheme, as well as those of 2 of its counterparts from the literature, specifically [32] and [33]. A larger value of the MSE signifies an improved level of security. Our proposed scheme is shown to outperform the MSE values of [33], while it achieves a lower performance than that achieved in [32]. Since the PSNR as a metric is inversely proportional to the

TABLE I: Processing time for various dimensions of the Lena image.

Image dimensions	Time [s]		
	Encryption	Decryption	Total
128×128	5.39173	0.268098	5.659828
256×256	6.41808	1.336811	7.754891
512×512	7.70297	3.989731	11.692701
1024×1024	17.86431	15.879460	33.74377
2048×2048	52.73229	63.00331	115.7356

MSE, the comparison among those 3 schemes in terms of PSNR still holds the same significance as aforementioned.

Information entropy is employed to measure the randomness of the distribution of gray pixel values of an encrypted image. Theoretically, the entropy value of a randomly encrypted image is 8 because a gray scale image has 256 symbols and the data of the pixel has 2^8 possible combinations. The entropy values of various encrypted images are shown in Table V. As can be seen, each of the values is a little over 7.999 which reveals that the proposed encryption scheme randomizes the distribution of the pixels of the plain image, making it impossible for an attacker to gain any information about the plain image. Moreover, Table V provides a comparison among the achieved information entropy values with those achieved by counterpart schemes from the literature [32]–[34].

Any PRNG can be easily tested for randomness using the test devised by the National Institute of Standards and Technology (NIST). A good PRNG should satisfy its randomness criteria by a number of tests that comprise the NIST analysis suite. Specifically, the probability, or p -value of each of the tests should be greater than 0.1 for any bitstream to be regarded as random. Table VI shows the results of the NIST analysis as run on an encrypted Lena image. It is clear that the values for all the tests are indeed larger than 0.1, deeming the success of our proposed image encryption scheme at passing the NIST analysis.

IV. CONCLUSIONS AND FUTURE WORKS

In this paper, we proposed an image encryption scheme that is based on 3 stages. The first stage incorporated the use of the Rössler System, while the second stage incorporated the use of a PRNG S-Box and the final stage incorporated the use of the Recamán's sequence. Performance evaluation of the proposed scheme was carried out utilizing a number of appropriate metrics and analyses. Those included visual inspection of both plain and encrypted images, a histogram analysis, a cross-correlation analysis, entropy values, MSE and

TABLE II: Numerical results of the achieved values for various metrics.

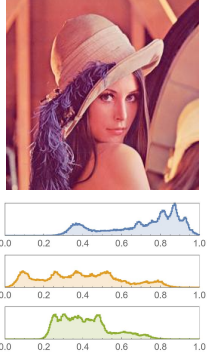
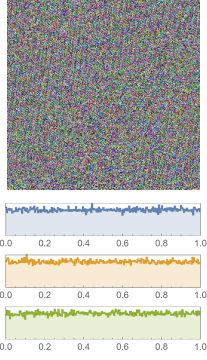

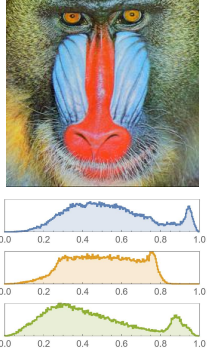
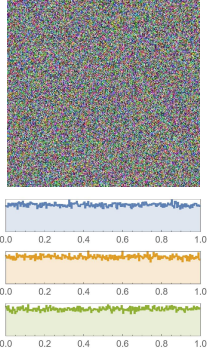
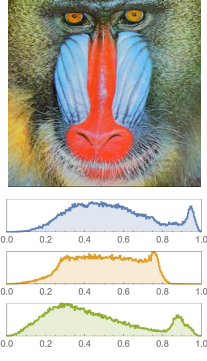
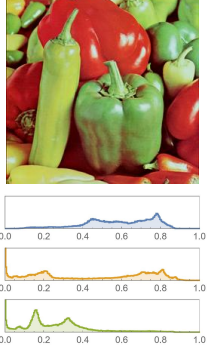
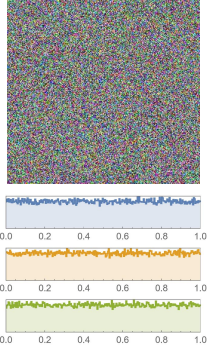
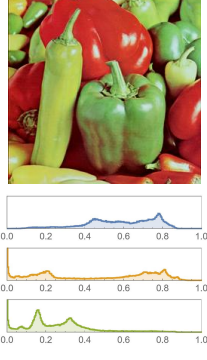
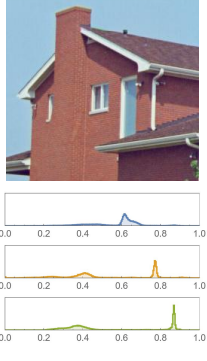
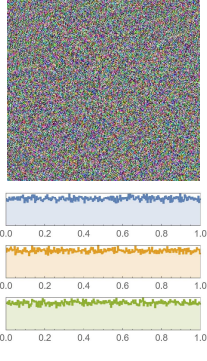
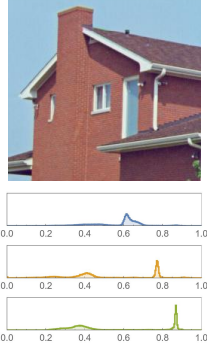
Image data	Plain image/histogram	Encrypted image/histogram	Decrypted image/histogram
Lena $d = 256 \times 256$			
Mandrill $d = 256 \times 256$			
Peppers $d = 256 \times 256$			
House $d = 256 \times 256$			

TABLE III: A comparison of MSE and PSNR values among the proposed scheme and its counterparts from the literature.

Image	Proposed Scheme		[32]		[33]	
	MSE	PSNR [dB]	MSE	PSNR [dB]	MSE	PSNR [dB]
Lena	8893.04	8.6403	10869.73	7.7677	4859.03	11.3
Mandrill	8286.99	8.94683	10930.33	7.7447	7274.44	9.55
Peppers	10064.2	8.10303	N/A	N/A	6399.05	10.10
House	8361.94	8.90773	N/A	N/A	N/A	N/A

TABLE IV: S-Box values generated from Wolfram Mathematica®.

102	216	26	199	187	45	252	245	204	154	125	19	238	215	208	43
6	198	195	11	67	223	20	255	7	1	211	162	14	236	145	9
107	170	147	246	196	232	109	133	33	34	179	212	234	197	27	190
82	206	99	18	75	172	12	63	167	203	160	122	78	94	79	51
184	235	37	243	150	143	40	244	10	137	50	186	247	68	185	100
210	169	61	123	253	76	180	16	159	142	21	88	38	237	81	129
71	230	175	217	35	65	202	90	29	136	177	121	80	115	95	140
127	85	110	93	153	225	124	62	209	231	224	54	146	4	157	161
58	86	72	138	250	201	222	116	104	165	47	5	2	39	249	84
170	83	0	174	87	58	172	189	29	135	86	105	223	156	143	132
48	200	112	23	105	164	148	181	0	73	32	56	44	131	178	36
60	92	218	113	254	103	241	108	98	52	117	101	28	220	25	46
242	151	13	168	219	59	213	17	87	158	182	192	171	126	155	227
134	141	42	41	193	106	83	31	166	128	91	176	111	114	74	248
132	144	69	228	57	240	119	207	77	139	174	70	221	189	97	214
226	251	188	53	30	183	15	55	229	22	89	49	156	120	149	194

TABLE V: Entropy values for encrypted images.

Image	Proposed	[32]	[34]	[33]
Lena	7.9991	7.9990	7.9978	7.9968
Mandrill	7.9990	7.9991	7.9993	N/A
Peppers	7.9991	N/A	N/A	N/A
House	7.9989	N/A	N/A	N/A

TABLE VI: NIST analysis on an encrypted image of Lena.

Test name	p-value	Remarks
Frequency	0.521667	Success
Block Frequency	0.779001	Success
Run ($m = 50162$)	0.455298	Success
Long runs of ones	0.011365	Success
Rank	0.177465	Success
Spectral FFT	0.683215	Success
No overlapping	0.332454	Success
Overlapping	0.412563	Success
Universal	0.987111	Success
Linear complexity	0.566321	Success
Serial	0.089741	Success
Approx. Entropy	0.521547	Success
Cumulative sum forward	0.987411	Success
Cumulative sum reverse	0.321577	Success

PSNR values. A comparison with counterpart schemes from the literature was carried out and the proposed scheme exhibited comparable security performance.

Finally, the processing time was computed and was shown to be rather low, showcasing the appropriateness of the proposed scheme for secure image exchange between handheld devices. A future work that could be further pursued would be the construction of a secure S-box, instead of relying on a PRNG S-box generated via Wolfram Mathematica®.

REFERENCES

- [1] A. El Mahdy and W. Alexan, "A threshold-free ltr-based scheme to minimize the ber for decode-and-forward relaying," *Wireless Personal Communications*, vol. 100, no. 3, pp. 787–801, 2018.
- [2] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Lightweight image encryption: Cellular automata and the lorenz system," in *2021 International Conference on Microelectronics (ICM)*. IEEE, 2021, pp. 34–39.
- [3] S. Yasser, A. Hesham, M. Hassan, and W. Alexan, "Aes-secured bit-cycling steganography in sliced 3d images," in *2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE)*. IEEE, 2020, pp. 227–231.
- [4] A. Samir, W. Alexan, R. T. ElDin, and A. El-Rafei, "3d steganography by random shuffling of image contents using residue model," in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2020, pp. 912–918.
- [5] M. I. Mihailescu and S. L. Nita, "Big data cryptography," in *Pro Cryptography and Cryptanalysis*. Springer, 2021, pp. 379–400.
- [6] W. Alexan, E. Mamdouh, A. Elkhateeb, F. Al-Seba'ey, Z. Amr, and H. Khalil, "Securing sensitive data through corner filters, chaotic maps and lsb embedding," in *2021 3rd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, 2021, pp. 359–364.
- [7] W. Alexan, M. El Beheiry, and O. Gamal-Eldin, "A comparative study among different mathematical sequences in 3d image steganography," *International Journal of Computing and Digital Systems*, vol. 9, no. 4, pp. 545–552, 2020.

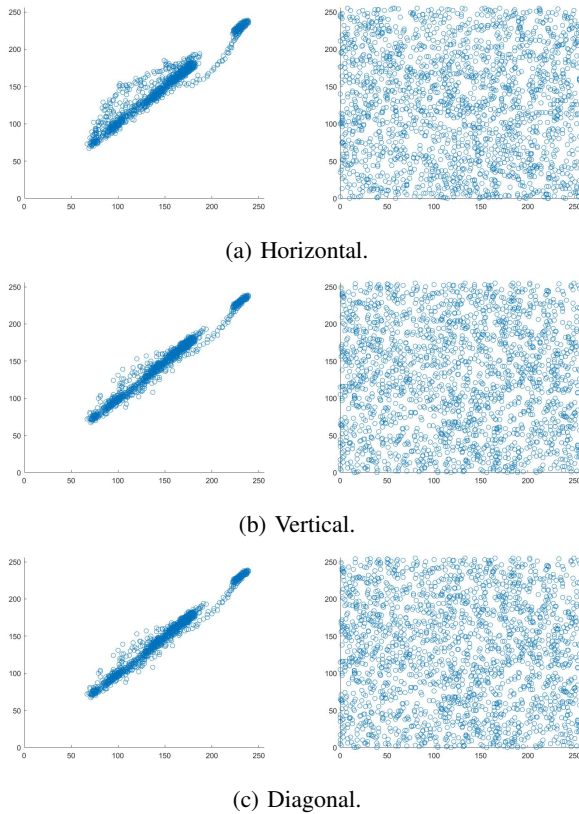


Fig. 4: Adjacent pixels cross-correlation for the Lena image, in 3 directions. In each of the subfigures, the left one is for the plain image, while the right one is for the encrypted image.

[8] W. El-Shafai, I. M. Almomani, and A. Alkhayer, "Optical bit-plane-based 3d-jst cryptography algorithm with cascaded 2d-frft encryption for efficient and secure hevc communication," *IEEE Access*, vol. 9, pp. 35 004–35 026, 2021.

[9] I. Verbaauwhede, "The cost of cryptography: Is low budget possible?" in *2011 IEEE 17th International On-Line Testing Symposium*, 2011, pp. 133–133.

[10] G. De Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*. IEEE, 2008, pp. 580–585.

[11] H. Rifa-Pous and J. Herrera-Joancomartí, "Computational and energy costs of cryptographic algorithms on handheld devices," *Future internet*, vol. 3, no. 1, pp. 31–48, 2011.

[12] A. G. Mohamed, N. O. Korany, and S. E. El-Khamy, "New dna coded fuzzy based (dnafz) s-boxes: Application to robust image encryption using hyper chaotic maps," *IEEE Access*, vol. 9, pp. 14 284–14 305, 2021.

[13] Y. Wang, X.-W. Li, and Q.-H. Wang, "Integral imaging based optical image encryption using ca-dna algorithm," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–12, 2021.

[14] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "Dna and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159 732–159 744, 2020.

[15] K. M. Hosny, *Multimedia security using chaotic maps: principles and methodologies*. Springer Nature, 2020, vol. 884.

[16] M. T. Elkandoz and W. Alexan, "Logistic tan map based audio steganography," in *2019 international conference on electrical and*

computing technologies and applications (ICECTA). IEEE, 2019, pp. 1–5.

[17] S. Wolfram, *A new kind of science*. Wolfram media Champaign, IL, 2002, vol. 5.

[18] C. Wen, X. Li, T. Zanotti, F. M. Puglisi, Y. Shi, F. Saiz, A. Antidormi, S. Roche, W. Zheng, X. Liang *et al.*, "Advanced data encryption using 2d materials," *Advanced Materials*, p. 2100185, 2021.

[19] Y. Zhang, H.-P. Lo, A. Mink, T. Ikuta, T. Honjo, H. Takesue, and W. J. Munro, "A simple low-latency real-time certifiable quantum random number generator," *Nature communications*, vol. 12, no. 1, pp. 1–8, 2021.

[20] O. Rossler, "An equation for hyperchaos," *Physics Letters A*, vol. 71, no. 2-3, pp. 155–157, 1979.

[21] O. E. Rössler, "An equation for continuous chaos," *Physics Letters A*, vol. 57, no. 5, pp. 397–398, 1976.

[22] R. Genesio, G. Innocenti, and F. Gualdani, "A global qualitative view of bifurcations and dynamics in the rössler system," *Physics Letters A*, vol. 372, no. 11, pp. 1799–1809, 2008.

[23] S. Farrag and W. Alexan, "Secure 2d image steganography using recaman's sequence," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 2019, pp. 1–6.

[24] G. Wang, "Chaos synchronization of discrete-time dynamic systems with a limited capacity communication channel," *Nonlinear Dynamics*, vol. 63, no. 1, pp. 277–283, 2011.

[25] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a discrete chaotic cryptosystem using external key," *Physics Letters A*, vol. 319, no. 3-4, pp. 334–339, 2003.

[26] A. Belazi, R. Rhouma, and S. Belghith, "A novel approach to construct s-box based on rossler system," in *2015 international wireless communications and mobile computing conference (IWCMC)*. IEEE, 2015, pp. 611–615.

[27] A. H. Zahid, E. Al-Solami, and M. Ahmad, "A novel modular approach based substitution-box design for image encryption," *IEEE Access*, vol. 8, pp. 150 326–150 340, 2020.

[28] M. Ahmad, H. Chugh, A. Goel, and P. Singla, "A chaos based method for efficient cryptographic s-box design," in *International Symposium on Security in Computing and Communication*. Springer, 2013, pp. 130–137.

[29] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[30] E. Tanyildizi and F. Özkaynak, "A new chaotic s-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117 829–117 838, 2019.

[31] M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf, "Bijective s-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110 397–110 411, 2020.

[32] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26 203–26 222, 2019.

[33] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, 2018.

[34] H. Liu, B. Zhao, and L. Huang, "Quantum image encryption scheme using arnold transform and s-box scrambling," *Entropy*, vol. 21, no. 4, p. 343, 2019.