Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 26 (2023), No. 6, pp. 1311–1318
DOI : 10.47974/JIM-1629

Image encryption with General Singular Values Decomposition via logistic function by encryption key only real number (method-2)

Mohammed Abdul-Hameed
Department of Mathematics
College of Basic Education
Kufa University
Najaf
Iraq

Abstract

In this algorithm the development of a previous algorithm was a master's thesis by researcher Maher AL-Bashkani. Where he used a technique (gsvd) with Logistic function to encrypt the image through a composite key which is two keys. The first is a real number and the second is a picture. In this algorithm we will call it (MK-11) we will dispense with the second key (picture) and with only the first key (real number). We will generate a 3D matrix that represents another key we create through the work of our algorithm. This is a new method that has not been used by previous algorithms. We know nothing about this triple matrix we create by implementing the algorithm. Therefore, this algorithm is considered very excellent and possesses high immunity against hackers who try to break the encryption.

The work of this algorithm focuses on three steps: The first is to create an array with the same dimensions as the image we want to encode depending on the numerical components of the image matrix as we will see later. The second step is the first distraction of the image matrix by adopting the first encryption key (real number) and logistic function. Step 3 We apply GSVD between the resulting image matrix after the first encoding contained in the second step above and the matrix that was created in the first step above to perform a second encryption step, the final encryption is two steps of encryption which adds complexity to the image encryption makes it difficult to penetrate by hackers. The results we obtained by implementing this algorithm were excellent and compete readings for modern algorithms. It is superior to accuracy and quality. Therefore, this algorithm can be adopted in information security.

Subject Classification: *94A60, 68P25, 81P94.*

Keywords: *Image encryption, GSVD, Logistic function.*

E-mail: **mohammeda.alkufi@uokufa.edu.iq**
http://orcid.org/0000-0001-7080-3181

1. Introduction

Information security has been a concern of nations throughout history many specialists and researchers have worked in this field starting from the Roman state BC passing through a large number of countries and civilizations including the civilization of Mesopotamia and the civilization of the Nile Valley and the Persian state Chinese, Indians and even spread this important science in all nations and countries of the world because of its importance in the management of military, financial, commercial and other affairs of the country[1][2]. Throughout the march of this science and its development in the great current era it is a field of applied mathematics fields there is not any Problem in it. Because of the adoption of various mathematical methods in the dispersion of data after conversion to numerical values (Vectors or matrices) and encrypted so that it does not make it possible to penetrate[3][4]. This science suffered many problems, including the lack of acceptance of some supervisors on the theses of master and doctoral any development of old algorithms and their total reliance on old methods and classical concepts the ballet algorithms obsolete and ended up at the time[5][6].

The second problem suffered by this science, specifically in modern times is dominated by specialists in the field of computers and the marginalization of the role of mathematics altogether on the other hand, the mathematicians did not object to this marginalization[7]. You see that all the algorithms are within the encryption field in particular and the image processing field in general computer specialists rely on algebraic, topological, or other mathematical techniques, but they do not point to the virtue of this science (mathematics) on information security field[8]. Specialists are mathematics who develop algorithms and improve according to the development of daily science and give it to computer specialists who deny mathematicians this privilege. My words are specific to what is happening in my country because the spirit of selfishness beat the specialists of the computer because they believe themselves the finest level of mathematics[9]. Where we often find committees that discuss master and doctoral theses in the image processing field without a specialist in mathematics and this represents a fatal scientific error[10].

In my recent research, I've talked about the order in which I made my algorithms in the field of image coding. The last algorithm we made was called "MK-10". This algorithm, which we will call "MK-11. That algorithm used the same basic idea with two encryption keys (real number

and image).Here, in our algorithm, we dispensed with the picture and the key became a real number.

We will adopt all the algorithms in our last search (MK-10) to compare the results and readings[11]. We will get we will also use abbreviations in the same search for globally adopted standards, coding time and decoding time. I would like to point out at the end of the introduction that I will adopt two images in the application of the algorithm They are my personal image (I think it will be funny) and the image of the baboon monkey[12].

1.1 *Encryption*

Let k is real number (key)

$$\text{cod} = A > 127.5$$

for example

if
$$A = \begin{bmatrix} 127.4 & 130 & 111 \\ 95 & 127.8 & 127.9 \\ 120 & 128 & 145 \end{bmatrix}$$

then
$$\text{cod} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$Y = (k * A) * (255 - A)$$

$$AA_1 = k * A$$

$$AA_2 = -k * A$$

$$[u_1, v_1, x_1, c_1, s_1] = \text{gsvd}(AA_1, \text{cod})$$

$$[u_2, v_2, x_2, c_2, s_2] = \text{gsvd}(AA_2, \text{cod})$$

$$AAA_1 = u_1 * c_2 * x_1^T$$

$$AAA_2 = u_2 * c_1 * x_2^T$$

$$F = \begin{bmatrix} -AAA_1 \\ AAA_2 \end{bmatrix}$$

1.2 *Decryption*

Let F be an encryption image.

And we have the real number k is a key.

Well we have a matrix guide to choose the correct roots (cod)

$$AA_1 = -F\left(\left[1 : \frac{\text{end}}{2}\right], :\right)$$

$$AA_2 = -F\left(\left[\frac{end}{2}+1:end\right],:\right)$$
$$[u_1, v_1, x_1, c_1, s_1] = gsvd(AA_1, cod)$$
$$[u_2, v_2, x_2, c_2, s_2] = gsvd(AA_2, cod)$$
$$A = u_1 * c_2 * x_1^T$$
$$A = \frac{A}{k}$$
$$k*x^2 - 255*k*x + A = 0$$

Of the elements of the matrix A are born a new matrix whose components are second-order equations on the following formula

$$k*x^2 - 255*k*x + A = 0$$

2. Application for the proposed algorithm

We also mention that we utilised the MATLAB software to implement the method, and I wrote the program myself to assure the work's safety and correctness.

Experiment Result in Table 1 & Table 2.

Table 1

Name of Image	Encryption time/s	Decryption time/s	Mean error	MSE	PSNR
Baboon	1.3470	13.9530	3.4856e-12	2.3282e-22	156.2957
MK-image	1.2790	14.1790	3.7564e-12	2.5930e-22	156.0618

Table 2

Readings for the global standards accuracy before encryption and after decryption for (Baboon, MK-image, Lena, Child, Suspension bridge, and Floating bridge) images.

Name of Image	Baboon	MK-image	Lena	Child	Suspension bridge	Floating bridge
						
EBE	0.0030	0	0.1416	0.0741	1.6775e-04	0.0074

Contd...

EAD	0.0030	0	0.1416	0.0741	1.6775e-04	0.0074
EEI	0	0	0.1585	0	0	0.0037
SDBE	56.1909	69.3053	63.8309	67.8032	46.7713	55.4479
SDAD	56.1909	69.3053	63.8309	67.8032	46.7713	55.4479
SDEI	8.5072e+06	7.2548e+07	7.2565e+13	2.0737e+07	1.1000e+09	3.1444e+11
CCOAD	1	1	1	1	1	1
CCOE	0.1233	0.4295	-0.2431	-0.1404	0.4917	-0.0390
NPCR	100	100	100	100	100	100
UACI	1.2841e+07	3.6473e+07	6.1623e+13	2.0499e+07	1.4230e+09	3.8840e+11
Encryption time/s	1.3470	1.2790	1.349	0.9680	0.8360	0.6910
Decryption time/s	13.9530	14.1790	14.0740	13.7530	11.3280	11.1270
Mean error	3.4856e-12	3.7564e-12	1.0312e-12	1.8097e-12	1.3721e-12	1.2464e-12
MSE	2.3282e-22	2.5930e-22	2.9489e-23	6.4074e-23	3.6006e-23	2.7508e-23
PSNR	156.2957	156.0618	160.7825	159.0974	160.3490	160.9335
Key	50	100	122112	67	543	8907

3. Conclusion

We infer from all of those Figures and tables that this algorithm (image Encryption using (General Singular Values Decomposition) via logistic function by Encryption key just real number (method-2)) has the following strengths and disadvantages for scientific honesty: -

- We adopted an initial encryption key, is a real number to do the program, which represents the algorithm to create another encryption key, is a three-dimensional matrix we do not know it although we have encrypted. This means, it is a secret encryption key even on the workers on encryption. This gives the algorithm strength and immunity against hackers.
- The possibility of applying the algorithm on medical and military images and so on and all extensions.
- The algorithm can be used to encrypt text in all languages.
- Encryption time is acceptable and falls within common levels, but it is not very ideal because the encryption process enters into very complex stages.
- The decryption time is very large and is unacceptable in the cases of normal encryption but came because of the very complex operations

that we perform for decryption, which we have shown through the search above on the sidelines of table (1) above, an unprecedented case. This means that our algorithm is unique in this way in complex encryption and decryption and was not preceded by another. It is for this reason that this algorithm applies only in sensitive cases and special highly.

- The relationship between the original image and the image after decryption at its highest value is equal to (1) which indicates to be no loss of data during encryption and decryption.

4. Discussion

- This the algorithm (General Singular Values Decomposition via logistic function by Encryption key only real number (method-2)) came she develop for the algorithm previous that we accomplished with a master student where the previous algorithm depends on two encryption keys (real number and image). Here, we only used the real number.
- The algorithm is very complex with evidence of decryption time but can be complex more by combining it with other algorithms as we have pointed out in our previous research.
- The readings that appeared to the international accuracy standards confirm the quality of the algorithm and is modern algorithm that has privacy from the rest of the algorithms.
- Through the MATLAB program, we have been able to apply this algorithm to all types of images and all fields of scientific and practical.

5. Acknowledgement

sanctification and veneration for the souls of the martyrs who were killed in the October Uprising. I thank them for their great virtue, because without their pure holy blood we could not eliminate administrative corruption in our country.

References

[1] A.H. Lotfy, A.A. El-Abbas-History of Mathematics-Cairo-General Authority for Amiri Press Affairs-1959.

[2] A.AL-Rammahi, M. Al-kufi; Image cryptography via svd modular numbers; *European Journal of Scientific Research*-Volume 138 No 2 (February, 2016).

[3] A.G. Radwan, genuine article some generalized discrete logistic maps, Engineering Mathematics Department, Faculty of Engineering, Cairo University, 12613, Egypt.

[4] (https://ui.adsabs.harvard.edu/abs/1981JSP....26..173G). doi:10.1007/BF01106792 (https://doi.org/10.1007% 2FBF01106792).

[5] Amira B. S., Zahraa M. T. Ahmed S. N. 2010. An Investigation for Steganography using Different Color System. *AL-Rafidain Journal of Computer Sciences and Mathematics* for the year. Proceedings of the Third Scientific Conference on Technology of information. 29-30 / Nov. / 2010, Faculty of Computer Science and Mathematics-University of Mosul. 474-492: http://computerscience.uomosul.edu.iq/files/pages/page_4034788.pdf.

[6] Deepak A., Sandeep K., Anantdeep A. An Efficient Watermarking Algorithm to Improve Payload and Robustness without Affecting Image Perceptual Quality, *Journal of Computing*. 2(4). 105-109 (2010).

[7] Grassberger, P. On the Hausdorff dimension of fractal attractors. *Journal of Statistical Physics*. 26 (1): 173-179 (1981). Bibcode:1981JSP....26..173G.

[8] Grassberger, P.; Procaccia, I. Measuring the strangeness of strange attractors. *Physica D: Nonlinear Phenomena* 9 (1-2): 189-208 ((1983)). Bibcode:1983PhyD....9..189G (https://ui.adsabs.harvard.edu/abs/1983PhyD....9..189G). doi:10.1016/0167-2789(83)90298-1 (https://doi.org/10.1016%2F0167-2789%2883%2990298-1).

[9] Hansen, P.C. Regularization, GSVD and truncated GSVD. BIT Numer. Math. 29, 491-504 (1989).

[10] H. Abdi, Singular Value Decomposition (SVD) and Generalized Singular Value Decomposition (GSVD), Encyclopedia of Measurement and Statistics, 2007.

[11] M.J. Burjus. AL-Bashkani-Image Cryptography using General Singular Values Decomposition-Thesis of master degree-Faculty of Computer Science & Mathematics \ the University of Kufa-January / 2019.

[12] MATLAB Version 7.12.0.635 (R2011a) 32 bit (win 32) march 18,2011 License Number 161052.

[13] W. Gao, M.R. Farahani. The hyper-Zagreb index for an infinite family of nanostar dendrimer. *Journal of Discrete Mathematical Sciences and Cryptography,* 20(2), 515-523 (2017). https://doi.org/10.1080/09720529.2016.1220088.

[14] A.J.M. Khalaf, A.Q. Baig, M.R. Azhar, M. Imran, M.R. Farahani. The Eccentric Based Zagreb Indices of Carbon Graphite *Journal of Discrete Mathematical Sciences, Cryptography.* 23(6), (2020), 1121-1137. https://doi.org/10.1080/09720529.2020.1818448.

[15] A.J.M. Khalaf, M.F. Hanif, M.K. Siddiqui, M.R. Farahani. On degree based topological indices of bridge graphs. *Journal of Discrete Mathematical Sciences, Cryptography.* 23(6), (2020), 1139-1156. https://doi.org/10.1080/09720529.2020.1822040.

[16] M. Alaeiyan, F. Afzal, M.R. Farahani, M.A. Rostami. An exact formulas for the Wiener polarity index of nanostar dendrimers, *Journal of Information and Optimization Sciences*, 41(4), 933-939 (2020). https://doi.org/10.1080/02522667.2020.1748274.