Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 26 (2023), No. 6, pp. 1319–1327
DOI : 10.47974/JIM-1630

Text encryption by image encryption key with based on Generalized Singular Value Decomposition (GSVD)

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

Abstract

This paper we will address the encryption process text is generally through a number of processes of dispersion of the later values in a matrix is A through remittances linear in addition to the use of GSVD enters, including one key which is gray image or to be possible colored but to be converted to a grayscale image, where work will begin the application process distracting initial. In a compound to generate new matrices B1 and B2 of the original text matrix and which enters the mean of the matrix of images key.The second phase of the dispersion is using GSVD on the last matrices with the matrix of the key and switch C matrix among the two spectral for the new matrices B1 with key and B2 with key to generation new matrices B11,B22, which represents putting as correlative F = [B11;B22] who represents the matrix of the initial of the encoded text. For purpose of ascertaining the accuracy of the work we calculated the matrix of absolute value of the difference between the matrix of numbers for original text characters lettering before encryption and matrix of numbers for text characters after decryption to show us zero matrix, as well as the calculation of the average values of this matrix was zero.

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

Keywords: *Text, Encryption text, Image, GSVD.*

1. Introduction

Every day, the demand for effective network security grows tremendously. Businesses are required to safeguard sensitive information against loss or theft. Not only must organisations address their security

E-mail: mohammeda.alkufi@uokufa.edu.iq

requirements, but they must also be aware of where the computer is susceptible and how to defend it. Currently, a user must be connected in any way, anywhere, and at any time[1,2].

The word cryptography is derived from the Greek words kryptos, meaning concealed, and graphein, meaning writing. It has always been necessary to exchange information in secret. There are several examples in the history of individuals attempting to conceal information from rivals. Cryptography, the study of encrypting and decrypting data, may be dated back to Egypt around the year 2000 BC[3,4].

It was initially employed in Egypt to communicate surreptitiously with the assistance of regular hieroglyphics. Julius Caesar (100-44 BC) created a basic substitution cypher that is still in use today. During the first and second world wars, the necessity for secrecy expanded tremendously, resulting in the development of several novel cryptographic systems[5-7].

As civilization has progressed, so has the demand for more complex measures of data protection. As the globe gets more connected, the need for information and electronic services rises, and with it, so does reliance on electronic systems. It is normal practise to exchange sensitive information such as credit card details via the Internet. Cryptography is one of the most important technologies for privacy, trust, access control, electronic payments, corporate security, authentication, and many more applications in todays information society. Cryptography is not just for governments and highly experienced specialists; it is available to everyone[8-10].

Since ancient times, cryptography or encryption has been employed in the military domain[11]. He asserted that the Pharaohs were the first to use encryption for multicasting between military sectors[12]. It was also said that the Arabs have a long history of endeavours in the realm of encryption. The Chinese used a number of cryptography and encryption technologies to convey messages during the battle[13,14]. It was their objective, through the use of encryption, to conceal the real shape of the communications so that if they fell into the hands of the adversary, they would be impossible to read. Julius Kaiser, one of the Roman Emperors, employed the best approach in the past[15,16]. The employment of this science, encryption, and connection to the globe networked via open networks has become an important requirement in the modern day[17]. And where these networks are utilised to electronically communicate information, both among private individuals and between private and public institutions, whether military or civilian[18]. Methods must be reserved to ensure information secrecy. It has made significant efforts from across the world to create best solutions for them to communicate data without the possibility of leaking this info.

Because of the rapid development of computers and the enormous growth of networks, particularly the World Wide Web of the Internet, work and study in the subject of cryptography is still ongoing[19-25].

3. Methodology

The application of the algorithm labeled on the Selection of text to clarification the steps:

3.1 *First / text encryption*

The full algorithm to encrypt the text in general:

1. Beginning we define one gray image key to entered within the matrix of text encryption phases.
2. Identify the numbers that correspond to the letters in the text you want to encrypt, including commas, the point of the bow, and anything else that fits within the numbers that make up the text and are stored in the computers memory. Most of the time, you can choose a special table that shows how the characters and signals used to write the text are numbered.
3. Using the method of (DATA CUBE) we transform the numbers of text components to a three-dimensional matrix. Let this matrix A.
4. In this step, we will use the method of distracting the matrix numbers to create a matrix B1 and B2

   Key1=double(key), key2=mean(key1)

   And if key2=0 then we can assume key2 is equal 1 because it is the key to not characterized by high secrecy.

   we reply to the dimensions of the matrix key1 to new dimensions to conform the dimensions of A

   Let the dimensions of A is n,m.

   Key1=imresize(key1,[n m])

   $$B1 = Key2 * A, B2 = Key1. * A$$

   Regarding to calculate (B2), the multiplication operation between (key1) and (A) are a multiple each element in (key1) with the corresponding element in (A).

5. Apply GSVD distracting the numbers:

   In this step, we will apply (GSVD Distracting the numbers) to conduct a spectral analysis of the matrices B1,B2 with the key1 and for the purpose of a switch between the c1 and c2 in the matrices analyzes.

$$[UB1, VB1, XB1, CB1, SB1] = GSVD(B1, key1), \quad (8)$$
$$[UB2, VB2, XB2, CB2, SB2] = GSVD(B2, key1)$$
$$B11 = UB1 * CB2 * XB1^{T},$$
$$B22 = UB2 * CB1 * XB2^{T}$$
$$F = [B11; B22]$$

   F is the matrix of the text code.

3.2 *Second / Text decryption:*

The full algorithm to decrypt of the text.
Now, with phases of decode matrix of text.

We have matrix is encrypted = F

1. Determine the dimensions of the matrix F (only rows and columns) that it equal (2n,m)
2. Divide the matrix F to restore matrices $B11_{new} = F(1:n, 1:m)$ and $B22_{new} = F(n+1:2n, 1:m)$.
3. define the same image key that we used in the encryption and perform the same mathematical processors that as follows:-

   Key1=double(key), key2=mean(key1)

   And if key2=0 then we can assume key2 is equal 1 because it is the key to not characterized by high secrecy.

   Key1=imresize(key1,[n m])
4. Reflect the impact of (GSVD) that is in step 5 of the encryption process to restore matrices $B1_{new}$ and $B2_{new}$.

$$[UB11_{new}, VB11_{new}, XB11_{new}, CB11_{new}, SB11_{new}] \ (9) = GSVD(B11_{new}, key1)$$
$$[UB22_{new}, VB22_{new}, XB22_{new}, CB22_{new}, SB22_{new}] = GSVD(B22_{new}, key1)$$

5. $$B1_{new} = UB11_{new} * CB22_{new} * XB11_{new}^{T},$$
   $$B2_{new} = UB22_{new} * CB11_{new} * XB22_{new}^{T}$$

6. $A_{new}\frac{B1_{new}}{key2}$

The last matrix A_{new} represent the numerical values of the letters of the cipher text after decryption they include the error increase or decrease of less than 0.5 which cannot represents the numerical values for letters. So, we approximate each value to the nearest integer, as below:

$$45.456 \cong 45, 36.743 \cong 37 \ldots etc$$

Bringing we produces matrix of numerical values for letters of cipher text identical to the original matrix and without any error.

From the last matrix, we get back the letters and symbols that match its numerical values so that the original text is shown without any mistakes.

4. The Results

Below the text that we will encrypt it and the key used and will be followed by results

1. The text, which we will encrypt it:

   [This paper we will address the encryption process text is generally through a number of processes of dispersion of the later values in a matrix is A through remittances linear in addition to the use of GSVD enters, including one key which is text or a gray Image or to be possible colored but to be converted to a grayscale image]

2. Image Key:

Figure

The key image

The text after decryption of all encryption keys:-

> This paper we will address the encryption process text is generally through a number of processes of dispersion of the later values in a matrix is A through remittances linear in addition to the use of GSVD enters, including one key which is text or a gray Image or to be possible colored but to be converted to a grayscale image

Average the absolute value of the difference between the elements of Matrix of the numbers after decoding and its treatment mathematically to approximated to the nearest integer and matrix of The numbers before the encryption is equal =0.

4.1 *Encryption and decryption time:*

Encryption time = 0.0160 second.
Decryption time= 0.0620 second

5. Discussion

1. The algorithm uses technology (GSVD) as a basis to encrypt text in any language.
2. This algorithm is based on any grayscale image as an encryption key.
3. Is it possible to use a color image as the key through more than one way in which to deal either convert to grayscale image or taking one of the bands of the color image as the key.
4. This is the first algorithm in its stride and used the analysis of the matrix and nature encryption keys.
5. The resulting text after decryption is identical to the original text and the error rate is zero.
6. The rate of encryption time is equal (0.0235second).
7. The rate of decryption time is equal (0.0625second).
8. The time of encryption and decryption calculated according on the speed by processors of personal computer that least of the times of encryption and decryption known.
9. The program adopted in the implementation of this algorithm is a program called MATLAB.
10. Can be developed this algorithm to encrypt any fingerprint or an object after converting it to a digital matrix and is available for use any other object convertible to a digital matrix as an encryption key

algorithm gives more complexity and strength of the traditional methods of encryption.

6. Conclusion

1. This algorithm is multi-functional, where encrypted text by used the encrypted key (image) as desired by the user with GSVD.
2. The encryption algorithm is a composition of 2 dispersal operations and substituted one confidential key above which makes it impossible strongly disassemble code the means and decoding programs currently available.
3. Brought together the algorithm between three scientific fields within two specialists are: the competence of two fields in mathematics that matrix algebra and numerical analysis in addition to the competence of computers and programming language MATLAB.
4. The level of encryption algorithm is characterized by high precision and so under standards of accuracy results used the mean of error.
5. Was characterized this algorithm their implementation quickly by computer compared to other encryption algorithms concerning the text.
6. Alone in this algorithm is the introduction the technique of GSVD.

7. Acknowledgements

I am very thankful to everyone who helped me in preparing and working, in particular, my daughters, Maryam Mohammed Abdul Hameed, and Mrs. Iman Abdul Sajjad Abdul Zahra.

References

[1] Aleksey Gorodilov,Vladimir Morozenko, Genetic Algorithms for finding the keys length and crypto analysis of the permutation cipher, *International Journal Information-Theories and Applications,* Vol. 15 (2008).

[2] Bethany Delman,Genetic Algorithms in Cryptography published in web; July (2004).

[3] Darrell Whitley, A Genetic Algorithm Tutorial, Computer Science Department, Colorado State University, Fort Collins, CO 80523.

[4] Introduction to Cryptography- Ranjan Bose- Tata Mc-Grew- hill Publisher ltd, (2001).

[5] N. Koblitz,A course in number theory and Cryptography, Springer-Verlag, New York, INc, (1994).

[6] Nalani N, G. Raghavendra Rao, Cryptanalysis of Simplified Data Encryption Standard via Optimisation Heuristics; *International Journal of Computer Science and Network Security*, Vol.6 No.1B (January 2006).

[7] Sean Simmons,Algebric Cryptoanalysis of Simplified AES, 33, 4; Proquest Science Journals Pg. 305 (October 2009).

[8] Sujith Ravi, Kevin Knight,Attacking Letter Substitution Ciphers with Integer Programming, Oct, 33, 4; Proquest Science Journals Pg. 321O (2009).

[9] A K Verma, Mauyank Dave and R.C Joshi,Genetic Algorithm and Tabu Search Attack on the Mono Alphabetic Subsitution Cipher in Adhoc Networks; *Journal of Computer Science,* 3(3): 134-137 (2007).

[10] William Stallings, Cryptography and Network Security: Principles and Practice, 2/3e Prentice hall (1999).

[11] R. Venkateswaran- Research Scholar- Ph.D- Karpagam Academy of Higher Education- Karpagam University- Coimbatore, Tamilnadu, India. & Dr. V. Sundaram- Director- Computer Applications- Karpagam College of Engineering-(Affiliated to Anna University)- Coimbatore, Tamilnadu, India./ Information Security: Text ncryption and Decryption with Poly Substitution Method and Combining the Features of Cryptography /*International Journal of Computer Applications,* (0975- 8887) Volume 3, No. 7, 28 June (2010).

[12] W. M. Farmer, Overview of Cryptography. 07-cryptography overview. pdf.(2003).

[13] Kirk Job-Sluder, Cryptography: A guide to protecting your files for consultants, educators and researchers. Indiana University. IST_ Conf_2002_sluder.pdf. (2002).

[14] Scott Wilson, An Introduction to Cryptography. Intro To Crypto.pdf. (2004).

[15] Claire Topping. General Cryptographic Knowledge. White Paper general_cryptographic_knowledge3.pdf. (2003).

[16] Cisco, Cisco IOS Software Feature: Network-Layer Encryption. White Paper encrp_wp.pdf. (2000).

[17] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. chap1.pdf. (2000).

[18] Erkay Savas, Data Security & Cryptography. Oregon State University & Trust Technologies. L1.pdf. (2002).

[19] Tal Malkin, Introduction to Cryptography. Summary 1 What is Cryptography 2 Modern Cryptography.pdf. (2003).

[20] Tom St Denis, Cryptanalysis in Society. Cryptanalysis in Society.pdf. (2004).

[21] C.F. Van Loan, Generalized the singular value decomposition, *SIAM Journal on Numerical Analysis*, 13 : 76-83 (1976).

[22] V.G.R. Bhatta, H. Panackal, P. Poojary, S.K. Pandey. Algebraic construction of near-bent function with application to cryptography. *Journal of Discrete Mathematical Sciences and Cryptography.* 24(2), 527-540 (2021). https://doi.org/10.1080/09720529.2021.1897214.

[23] 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.

[24] 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), 1121-1137 (2020). https://doi.org/10.1080/09720529.2020.1818448.

[25] 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), 1139-1156 (2020). https://doi.org/10.1080/09720529.2020.1822040.