Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 26 (2023), No. 6, pp. 1089–1098
DOI : 10.47974/JIM-1608

Text encryption with singular values

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

Abstract

In this paper, we will talk about how text is encrypted. Generally, this is done through a number of processes that spread out the later values in a matrix, which is A through remittances are linear and the use of SVD enters, including one key where work will start on the application process. New matrices B1 and B2 of the original text matrix are generated in a compound, and the key is entered. The second step of the dispersion involves utilizing SVD on the final matrices and switching the S matrix between the two spectra for the new matrices C1 and C2, which signifies inserting the matrix of the encoded text as correlative F = [C1 C2]. To determine the accuracy of the work, we calculated the matrix of the absolute value of the difference between the matrix of numbers for the original text characters lettering before encryption and the matrix of numbers for text characters after decryption, which resulted in a zero matrix, as well as the calculation of the average values of this matrix which resulted in a zero matrix.

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

Keywords: *Text, Encryption text, SVD, M. K. Text Cipher 1.*

1. Introduction

The challenge of preserving database security and privacy (Database Security And Privacy) from key concerns in database applications via networks of various communications against spambots and unwanted

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

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

activity (Unauthorized Activity). The issue of maintaining the security and privacy of databases (Database Security And Privacy) from the important problems in database applications through networks of various communication against spambots activity of unauthorized (Unauthorized Activity). Access to the data or change it and the provision of a specific way to register all spambot activity while keeping total registrations of all the processes of updating the data that take place on a database away from the hands of the beneficiaries (Users) helps the Database Administrator to improve the security situation and the privacy of her future. It must include the programs used to work with databases, with a focus on security and privacy [1][2].

Offers the most recent applications, databases, and several methods of database protection, such as passwords and data encryption [3].

Passwords:

Every database application allows you to add passwords, and the beneficiary can offer programs to utilize passwords other than those provided by database applications [4]. Moreover, the following processes must be followed while selecting passwords:

Avoid using common passwords such as the person's name, date of birth, family name, work director's name, and so on[5]. (In cases when this strategy facilitates guessing).

Passwords are made up of a mix of letters, numbers, and special symbols that are provided by the operating system. For example, the number of letters, numbers, and special symbols that can be used to make a password is shown in the calculator below. [6] (Depending on what languages are available, only English).

The numbers = 11.

The number of characters = 52 (lower/upper case).

Special symbols provided by the keyboard =33.

Will be the total =95. letter, number, and unique code are added to all the shapes of the letters provided by any language except English to become a wide field choice.

The password should be at least 11 characters long (characters, numbers, or special symbols), and the following table (Table 1) displays the time necessary to guess the password:

Table 1

The number of encrypted characters, the number of attempts needed to crack the code, and the time required

Number of characters used	Number of the attempts	The time required
4	81450625	71.6464 hour
6	7.3509e+11	116.5481 year
8	6.6342e+15	631110 year
10	5.9874e+19	1898600000 year

The possibility of choosing multiple passwords for the important beneficiaries, for example, a database manager.

Choosing passwords is important because their validity is associated with the time of the day.

Data encryption:-

Procedures for data encryption include comprehensive encryption for data or partial encryption, where the data is encrypted so that hackers cannot be allowed through different computer networks. It is possible to know the nature of the data by withholding it, and the data structures used [7]. An example of this is the encryption of all the major and minor keys in tables of data structures used[14][15][16]. In the process of encryption using an encryption key, it is possible to use more than one key to encrypt the data according to its importance. The controls of selecting the key subject to the same controls for selecting the password follow-through regimes implemented in any institution after the transformation of the systems implemented on one computer (only one beneficiary) to Systems adopted the principle of (the server and the beneficiary) with retaining structures, programs, and data (Previous unchanged), poed the following security problems[8].

Each beneficiary within the network can review and update all system tables without notation of what he had done and what the nature of the beneficiary changed information (means that there is an opportunity to manipulate data without leaving a trace of it)[9][17].

You can use the one computer linked to the network to change all this data when the server is on[10].

So It rolls it is necessary that the focus is on the issue of the security of the data, documents and information and keep abreast of developments in this field[18], because weakness in this subject will make the country

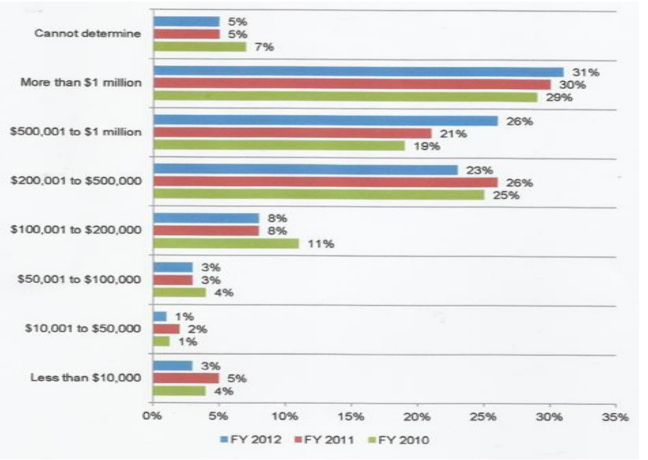

Figure 1

The economic impact of data breach incidents experienced over the three years(2010, 2011,2012)

unprotected and available to breakthrough and Information pirates, which would cause a loss of Informatics to lead to a negative impact on the economic side as shown by the histogram following (Figure 1) which shows the amount of the economic impact on one of the joints to work in a state where only the health aspect illustrated how important information security at present where all the nations of the world are subject to the effects of globalization and the development of modern scientific[11].

2. Methodology

2.1 *Encryption*

The entire algorithm for encrypting text in general:

Beginning, we define one key to be entered within the matrix of text encryption phases, which is real but not equal to zero.

Identify the numbers corresponding to the letters in the text you want to encrypt, including commas, the point of the bow, and everything else that fits into the numbers that make up the text and are stored in the computer's memory. Most of the time, you can use a special table to number the characters and signals used to write the text.

Employing the method of (DATA CUBE) we transform the numbers of text components into a three-dimensional matrix. Let this matrix A.

In this step, we will use the method of distracting the matrix numbers to create a matrix B1 and B2

B1=Key*A,B2=-Key*A

Aly SVD Distracting the numbers:

In this step, we will try (SVD Distracting the numbers) to conduct a spectral analysis of the matrices B1, B2 and for a switch between the singular values in the matrices analyses.

[UB1, SB1, VB1] = SVD(B1), [UB2, SB2,VB2]=SVD(B2)
C1 = UB1*SB2*VB1^T, C2 = UB2 * SB1 * VB2^T
F = [C1C2] (6)

Text Cipher= FThe full paper has to be submitted electronically via the website of the conference) Each abstract is issued a paper number (in the format XXX) when submitted through our OpenConf system. Authors are kindly asked to insert this paper number in the right areas in the header and footer before submitting the final version.

2.2 *Decryption*

Text decryption:

The full algorithm to decrypt the text.

Now, with phases of the decode matrix of text.

We have a matrix is encrypted M.K.Text Cipher1 = F

1. Divide the matrix F_{new} to restore matrices $C1_{new}$ and $C2_{new}$
2. Reflect the impact of (SVD Distracting the numbers) in step 5 of the encryption process to restore matrices $B1_{new}$ and $B2_{new}$.

   $[UC1_{new}, SC1_{new}, \_VC1_{new}] = SVD(C1_{new})$

   $[UC2_{new}, SC2_{new}, \_VC1_{new}] = SVD(C2_{new})$

   $B1_{new} = UC1_{new} * SC2_{new} * VC1_{new}^{T}$, $B2_{new} = UC2_{new} * SC1_{new} * VC2_{new}^{T}$
3. $A_{new} = \dfrac{B1_{new}}{key}$ (7)

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

$$45.456 \cong 45,\ 36.743 \cong 37 \ldots etc \tag{8}$$

Thus we construct a matrix of numerical values for encrypted text characters that is equal to the original matrix and error-free. We recover the letters and symbols matching the numerical values of the last matrix to display the same original text without mistakes.

3. The Results

3.1 *The text before encryption*

This study will examine the encryption process text, generally accomplished by various dispersion methods of the later values in a matrix. In addition to the usage of SVD, A through remittances linear enters, including three keys consecutively, where work will begin the application process distracting initially we termed (MK-Distracting the numbers method1). In a compound to generate new matrices A1 and A2 of the original text matrix and which enters the first key (Key1) and then use the second key (Key2) for a linear transform matrices A1 and A2 second phase in dispersing Numbers Matrices (MK-Distracting the numbers method2) to get the new matrices B1 and B2. The third step of the dispersion involves utilizing SVD on the final matrices and switching the S matrix between the two spectra for the new matrices C1 and C2, which signifies inserting the matrix of the encoded text as correlative F = [C1 C2]. Then conducting, the process of chromaticity values in the last matrix composite F, which will be values of real non-specific range, that is to say, including what is less than zero, including what is bigger than the one to be ultimately values of later within the closed set [0,1] while retaining the largest value and the smallest value... In the matrix, FF within the last matrix ensures the possibility of return versa in the decryption phase in a way that we call (MK press numbers). The final matrix resulting matrix is the final encrypted text that we call (M.K. Text Cipher1).

Key=9

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

3.2 *The text after decryption*

In this paper, we will talk about how text is encrypted. This is usually done through several processes that spread the later values across a matrix. We will also talk about how to use svd enters, including how to use three keys in order. alication process of distracting initially we called (MK-Distracting the numbers method1)In a compound to generate new matrices A1 and A2 of the original text matrix and which enters the first key (Key1) and then using the second key (Key2) for a linear transform matrices A1 and A2 second phase in dispersing Numbers Matrices (MK-Distracting the numbers method2) to get the new matrices B1 and B2. The third step of the dispersion is to use SVD on the last matrices and switch S.	Matrix among the two spectra for the new matrices C1 and C2 indicates setting the matrix of the encoded text's start as correlated F = [C1 C2]. Then conducting, the process of chromaticity values in the last matrix composite F, which will be values of real non-specific range, that is to say, including what is less than zero, include in g what is bigger than the one to be ultimately values of later within the closed set [0,1] while retaining the largest value and the smallest value... In the matrix, FF within the last matrix ensures the possibility of return versa in the decryption phase in a way that we call (MK press numbers). The final matrix resulting matrix is the final encrypted text that we call (M.K. Text Cipher1).

4.5

Encryption time = 0.003 seconds.
Decryption time = 0.006 second.

5. Conclusion

1. The encryption algorithm is composed of two dispersal operations and substituted one confidential key, making it impossible to disassemble code the means and decoding programs currently available.
2. The level of the encryption algorithm is characterized by high precision and so under standards of accuracy; results used the mean of error.
3. Enters the algorithm with one key to enter within the matrix of text encryption phases, which is a real number but not equal to zero.
4. Characterized this algorithm's implementation quickly by a computer compared to other encryption algorithms concerning the text.

5. Alone in this algorithm is the introduction of the technique of SVD within the two stages of dispersion.
6. Brought together, the algorithm between three scientific fields within two specialists is the competence of two fields in mathematics, matrix algebra, and numerical analysis, in addition to the competence of computers and the programming language MATLAB.

6. Acknowledgement

After this research, I cannot help but extend my thanks and gratitude to the Department of Mathematics for the moral, administrative, and scientific assistance it provided me. And I also extend my thanks and appreciation to my supporter and my first assistant in my work; she is my wife, Mrs. Balqis Shrrad Hussain.

References

[1] Alnehrinclaih University Journal of Science - Volume 55 version (4) December, . 53-58 / Provide sober protection for the privacy and security of information databases Imad Abdul Rasul Abdul-Sahib _ University of Technology, Baghdad, Iraq - Imad_sahib@Yahoo.com. (2012).

[2] Ahmed M.A. Al thneibat1, Bahaa Eldin M. Hasan2, Abd El Fatah. A. Hegazy3, Nermine Hamza4, Secure Outsourced Database Architecture, *IJCSNS International Journal of Computer Science and Network Security*, Vol. 10, 246-253 (2010).

[3] Liu, S., Kuhn, R., Data Loss Prevention, IT Professional, Volume 11, 10-13 (2010).

[4] Lv Guangjuan, Xu Ruzhi, Zu Xiangrong, Information Security Monitoring System Based on Data Mining International, 2009 *Fifth International Conference on Information Assurance and Security, IEEE*, Volume 1, 472-475 (2009).

[5] Sharma, A., Ojha, V., Belwal, R.C., Agarwal, G., Password-based authentication: Philosophical survey, 2010 *International Conference on Intelligent Computing and Intelligent Systems, IEEE*, Volume 3, 619-622, (2010).

[6] Yang Jian, An Improved Scheme of Single Sign-On Protocol Based on Dynamic Double Password, 2009 *International Conference on*

Environmental Science and Information Alication Technology, IEEE, Volume 3, 572-574 (2009).

[7] Zhao Yong-Xia, The Technology of Database Encryption, Second *International Conference on Multimedia and Information Technology, IEEE*, Volume 2, 268-270 (2010).

[8] F. Vancea,C. Vancea, Protecting data integrity with chained rows and public key cryptography, *Journal of Computer Science and Control Systems*, Volume 1, 114-117 (2008).

[9] Navleen Kaur, Dr. Amardeep Singh, Sarabpreet Singh; Enhancement of Network Security Techniques using Quantum Cryptography; *International Journal on Computer Science and Engineering,* Volume 3, 1960-1964 (2011).

[10] *Alnehrinclaih University Journal of Science* - Volume 55 version (4) December, . 53-58 / Provide sober protection for the privacy and security of information databases Imad Abdul Rasul Abdul-Sahib _ University of Technology, Baghdad, Iraq - Imad_sahib@Yahoo.com (2012).

[11] Third Annual Benchmark Study on Patient Privacy & Data Security-Ponemon Institute© Research Report-Sponsored by ID Experts-Independently conducted by Ponemon Institute LLC- Publication Date: December 2012- Ponemon Institute: Private & Confidential Report 1- Third Annual Benchmark Study on Patient Privacy & Data Security- Presented by Ponemon Institute, December (2012).

[12] Kolman B. Introductory Linear Algebra with Alications- Ninth Edition Bernard Kolman/ Drexel University-David R.Hill/ Temple University- Macmillan (1984).

[13] Nidhal K. El Abbadi / Department of Computer Science_University of Kufa, Najaf_Iraq, Adil Mohamad and Mohammed Abdul-Hameed/ Department of Mathematical_ University of Kufa_Najaf, Iraq __ Image Encryption Based on singular Value Decomposition- *Journal of Computer Science* 10 (7): 1222-1230, 2014-ISSN: 1549-3636-© 2014 Science Publications-doi:10.3844/jcssp.2014.1222.1230 Published Online 10 (7) (2014). (http://www.thescipub.com/jcs.toc).

[14] Algebraic construction of near-bent function with alication to cryptography- Vadiraja G. R. Bhatta, Harikrishnan Panackal, Prasanna Poojary & Shashi Kant Pandey- https://doi.org/10.1080/09720529.2021.1897214- *Journal of Discrete Mathematical Sciences and Cryptography.* 24(2), 527-540 (2021).

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] A. Alsinai, B. Basavanagoud, M. Sayyed, M.R. Farahani, Sombor index of some nanostructures, *Journal of Prime Research in Mathematics*, 17(2), 123-133 (2021).

[20] A. Hasan, M.H.A. Qasmi, A. Alsinai, M.Alaeiyan, M. R. Farahani, M.Cancan, Distance and Degree Based Topological Polynomial and Indices of X-Level Wheel Graph. *Journal of Prime Research in Mathematics,* 17(2), 39-50 (2021).

[21] A. Alsinai, H.M.U. Rehman, Y. Manzoor, M. Cancan, Z. Taş, M.R. Farahani, Sharp upper bounds on forgotten and SK indices of cactus graph, *Journal of Discrete Mathematical Sciences and Cryptography*, 1-22 (2022). https://doi.org/10.1080/09720529.2022.2027605.