**Open Access** **Baghdad Science Journal** **P-ISSN: 2078-8665**
**Published Online First: July 2021** **2022, 19(1): 189-196** **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2022.19.1.0189

# Securing Text Messages Using Graph Theory and Steganography

***Samaher Adnan Abdul-Ghani*** ***Renna D.Abdul-Wahhab*** ***Enas Wahab Abood****

Department of Mathematics , Collage of Science, University of Basrah, Basrah Iraq.
*Corresponding author: samaheradnanmath@gmail.com, Renna_Dawood72@yahoo.com, enaswahab223@gmail.com*, enas.abood@uobasrah.edu.iq*
*ORCID ID: https://orcid.org/0000-0001-5125-3399 , http://orcid.org/0000-0003-0430-3044,https://orcid.org/0000-0002-8504-1463*

Received 28/3/2020, Accepted 2/11/2020, Published Online First 20/7/2021, Published 1/2/2022



## Abstract:

Data security is an important component of data communication and transmission systems. Its main role is to keep sensitive information safe and integrated from the sender to the receiver. The proposed system aims to secure text messages through two security principles encryption and steganography. The system produced a novel method for encryption using graph theory properties; it formed a graph from a password to generate an encryption key as a weight matrix of that graph and invested the Least Significant Bit (LSB) method for hiding the encrypted message in a colored image within a green component. Practical experiments of (perceptibility, capacity, and robustness) were calculated using similarity measures like PSNR, MSE, and SSIM. These measures had proved the efficiency of the system for image quality and hiding messages with PSNR ratio more than 85 dB, MSE ranged (4.537e-05 to 5.27546e-04) and SSIM=1.0 for using a cover file with size ranged from 256×300 to 1200×760 pixels and message ranged from 16 to 300 characters.

**Key words:** Data security, Graph theory, Text hiding, Encryption.

## Introduction:

Securing information is an essential requirement for any process which involves the exchange of information. This is especially important in the case of financial transactions such as credit card or bank accounts…etc. and also for military and governmental information. Many researchers through last years presented many methods and approaches to secure data of any kind like text, images, and sound waves. These methods vary in applications due to the kind of key, type of mathematical approach, the strength of the method, and its immunity against attack. There are two types of securing art, first is cryptography which is the art of changing plain data to be not understandable and unreadable only by the one who has the encryption key, while the second is the art of steganography which is used to secure data by including it in another innocent file like a cover [1,2,3]. Therefore, the main difference between encryption and steganography is that when information is encrypted, the snipers can know that there is a connection between two parties (two or more) and the information is encrypted, however in the case of steganography, the third party (sniper) isn't able to know about the connection between two behind the scenes because this connection was hidden completely in a medium[4,5].

Some studies used encryption to secure digital data and produced many types of methods like chaotic maps[6], the Triple Data Encryption Algorithm (TDES) that uses symmetric encryption, and The Advanced Encryption Standard (AES) which is symmetric encryption also that depends on the Rijndael algorithm. Whatever encryption developed methods had been used to secure information, the steganography still stands in hiding the secret information in digital cover files. Various steganography methods had been presented to secure data. Some of these methods in a spatial domain like Least Significant Bit (LSB) and others in the frequency domain as in DCT, FFT, and DWT transform. The type of data for secret and cover files also produced a way to differentiate the methods and domains[7].

This paper suggests a novel system to secure text messages by using graph theory; the graph is used to produce a key for encryption by generating a complete graph for the keyword and calculating an adjacency matrix of the graph, then applying it to text to obtain a cipher text. The cipher text is embedded in the green component of the cover image using the LBS (Least Significant Bit) technique that depends on hiding message bits within the LSB in cover file samples. The system permits the user to choose the keyword of n symbols (mixed letters, digits and special characters), also the system can encrypt many kinds of characters English, Arabic and special characters like ( +,-,*,>, etc.) using a table for transforming the characters to a number ranged from 0-100 prepared for this research. Statistical analysis like PSNR (Peak signal-to-noise ratio), MSE(mean squared error ) and SSIM(The Structural Similarity Index ) ratios are used to prove the efficiency of the system in securing text messages and produced very acceptable results.

To summarize our contribution, we find it important to use new methods in mathematics to secure data sent over the Internet and to develop some of the methods that have been put forward in previous research. Moreover, the importance of the time consuming factor in securing and retrieving messages appears due to its impact on the consumption of network resources. Our research proposes the idea of securing messages with a short time and with high efficiency, reducing calculations and time to an acceptable minimum and investing modern math methods in that.

## Related Works

The securing mechanisms using cryptography and steganography have been studied by many researchers who sought to produce more immune schemes. Some of them used Chaotic systems to encrypt the data needed to be protected as well as decipher encrypted data like Deng Z. and Zhong S., they introduced an algorithm for digital image encryption based on the chaotic mapping, the authors analyzed the algorithm of chaotic and they ensured that it was simple and needed no prior knowledge of the orbital and the algorithm expanded the cryptographic space and reduced the number of iterations required in the mapping operation, and the image replacement method based on chaos that presented can resist the chosen-plaintext attacks[8]. Pareek NK. *et.al.* produced an algorithm for Block Cipher using chaotic maps of 1D and 2D to encrypt data and decrypt the cipher data to retrieve the plain data again[9]. Kwon OM *et.al.* and Cao Y. used the chaotic maps to secure communication signals and images such that the entropy generated by the chaotic map produces the required confusion and diffusion[10]. Al-Bahrani EA and Kadhum RNJ. proposed a hybrid model that used a chaos system and Feistel network structure with a secret key of n-characters to give a new Feistel cipher that related with the message size[11]. Sahib Ogla RA. presented a complex method to hide information based on a spiral search method. The proposed system converted the image color system from RGB to HSV and hid the secret message in H component after dividing the H component into blocks and quarters, then started hiding from the center and spread in all direction[12]. Other researchers used the Graph theory to produce new methods in encryption. Yamuna M. *et.al.* proposed a way to encrypt messages consisting of a binary string through a cipher chain blocking method. Musical notes of seven basic keys were used for encryption by taking the degree sequence of the graph constructed from that music note to form the key[13]. Akl SG. produced a model for securing the graph as a secret message itself, all the graph components as its vertices, its edges, and its edge weights need to be secured. The encryption algorithm depends on an alternative mapping, conjectured to be a one-way function, designed for securing graphs, and it requires a symmetrical key for both encryption and decryption[14]. Hraiz S and Etaiwi W. produced a new algorithm of a symmetric encryption using graph theory representation. Their algorithm encrypts text messages through converting them to a graph represented by adjacency matrix[15]. Etaiwi W. utilized graph theory properties to propose a symmetrical algorithm to encrypt and decrypt data securely. The algorithm used a cycle complete graph, and a minimum spanning tree to produce a cipher text .The author considered an undirected graph G(V,E) ,V represents vertices while E. is the edges between V. The algorithm represents data as vertices and each adjacent characters in the text represented as adjacent vertices in the graph, the vertices will keep adding until a cycle graph is formed. All alphabet characters are represented by a code in a special table. An adjacency matrix is created for the complete graph. Then the Minimum Spanning Tree (MST) is calculated from the complete graph and represented as adjacency-matrix that keeps data characters order in its diagonal. Adjacency-matrix of the complete graph is multiplied by the adjacency-matrix of MST. The resultant matrix is multiplied by the key matrix. The final matrix is the encryption data to be sent to the recipient for decryption a reverse multiplication is done with matrix inverse of the key and inverse of

the matrixes sent by the sender, but the pitfalls of this algorithm is the increasing in size of cipher text more than 20 times of the plain text[16]. Akhter F. proposed a secured Graphstega system for securing information based on hiding principle to avoid steganalytic attacks. it converts the text message to graph word by word with Huffman encoding instead of letter by letter[17]. Kumari M. and Kirubanad VB modified a cipher algorithm to encrypt the data. The authors plotted the encrypted data onto a graph. Then, the graph was transformed into an image. A desired symmetrical key is selected by the sender and receiver to encrypt and decrypt original data. This system is used to secure data storing it in the cloud as a secret message inserted in the graphical image cover file in a network environment , the key of encryption is about 2 digits and this means there is a possibility to find out by trying or analyzing[18].

## Proposed System:

The proposed system consists of two steps of securing techniques, encryption and steganography. The encryption algorithm is a symmetrical key system based on graph theory properties like edges, weight matrix and path while steganography is worked on spreading encrypted text bits randomly in the green component of a colored image as a cover file using replacement operation with Least Significant Bit (LSB) of Green-component

## Encryption Algorithm:

The message is about a series of characters (English, Arabic, and special symbols) that need to be secured by an encryption algorithm with a key. The key is a text also but processed by graph theory then used for the encryption process. Firstly a table of codes designed for this algorithm is used to substitute the text characters with its corresponding code number. The special codes are illustrated in Table 1.

The algorithm of encryption is consisting of several steps as below:

## Key Generation Steps:

1. Let P be a password of length N, Construct P to a simple graph.
2. Each character is represented by a vertex, every edge in the graph connecting two vertices sequentially while form a path graph.
3. Weight each edge using character table by counting the distance between each connected two Vertices from the character table.
4. Construct a complete graph and compute the adjacency matrix K as encryption Key.
5. End.

**Table 1. symbols of keyboard.**

| Symbol | Code | Symbol | Code | Symbol | Code | Symbol | Code |
|---|---|---|---|---|---|---|---|
| ! | 1 | E | 26 | \ | 51 | ك | 76 |
| @ | 2 | R | 27 | Z | 52 | م | 77 |
| # | 3 | T | 28 | X | 53 | ن | 78 |
| $ | 4 | Y | 29 | C | 54 | ئ | 79 |
| % | 5 | U | 30 | V | 55 | ا | 80 |
| ^ | 6 | I | 31 | B | 56 | أ | 81 |
| & | 7 | O | 32 | N | 57 | ل | 82 |
| * | 8 | P | 33 | M | 58 | ب | 83 |
| ( | 9 | { | 34 | , | 59 | ي | 84 |
| ) | 10 | } | 35 | . | 60 | س | 85 |
| _ | 11 | [ | 36 | ? | 61 | ش | 86 |
| + | 12 | ] | 37 | ظ | 62 | د | 87 |
| + | 13 | ; | 38 | ز | 63 | ج | 88 |
| 0 | 14 | " | 39 | و | 64 | ح | 89 |
| 1 | 15 | : | 40 | ة | 65 | خ | 90 |
| 2 | 16 | / | 41 | ى | 66 | ه | 91 |
| 3 | 17 | L | 42 | لا | 67 | ع | 92 |
| 4 | 18 | K | 43 | آ | 68 | غ | 93 |
| 5 | 19 | J | 44 | لآ | 69 | ف | 94 |
| 6 | 20 | H | 45 | ر | 70 | ق | 95 |
| 7 | 21 | G | 46 | ؤ | 71 | ث | 96 |
| 8 | 22 | F | 47 | ء | 72 | ص | 97 |
| 9 | 23 | D | 48 | ئ | 73 | ض | 98 |
| Q | 24 | S | 49 | ذ | 74 | inter | 99 |
| W | 25 | A | 50 | ط | 75 | Space | 100 |
| | | | | | | Ctrl | 0 |

## Encryption Step:

Let M be a message to be encrypted.

1. Convert each letter of the message to its code value using the Table (1).
2. Put the plaintext codes in the matrix (m x n), in which the number of columns equals to the number of key elements..
3. Multiply matrices of plaintext by the generated key K (mod(101)) to get the cipher text.
4. Convert the values from step 3 of cipher matrix to obtain the encrypted message.
5. End

At the receiver side, the decryption process depends on the key generation algorithm and codes table. The encryption process takes two steps also:

**Decryption Key Generation Step:**

To create the decryption key we need to perform the encryption key generation steps then take the inverse of generated key to use it for decryption.

**Decryption Algorithm:**

1- Put the cipher text in the matrix (m× n), where the number of columns equals the number of inverse key elements.
2- Convert the value for each letter of the cipher text using the Table (1).

3- Compute plaintext by multiplying [cipher matrix with inverse key mod (101)].
4- Convert the value of any number we obtained the original text.
5- End.

**Example:** Let M be a message to be encrypted:
M= "GOOD LUCK" , the Key is="فصبر جميل" .
Solution:
1- Construct plaintext matrix as: [G, O, O ,D ,space, L,U,C,K].
2- Convert the value for each character using table(1) as:

$$PlainText = [\ 46\ \ 32\ \ 32\ \ 48\ \ 100\ \ 42\ \ 30\ \ 54\ \ 43\ ]$$

3- Encryption key as: key= " فصبر جميل ".

$$Key = [\ 94\ \ 97\ \ 83\ \ 70\ \ 100\ \ 88\ \ 77\ \ 84\ \ 82\ ]$$

4- Construct a simple graph (Fig.1)


**Figure 1. Graph of kind path for keyword**

5- Compute weight matrix $wij = |cod(i) - cod(j)|$ .
6- Construct a complete graph, ( Fig. 2) :

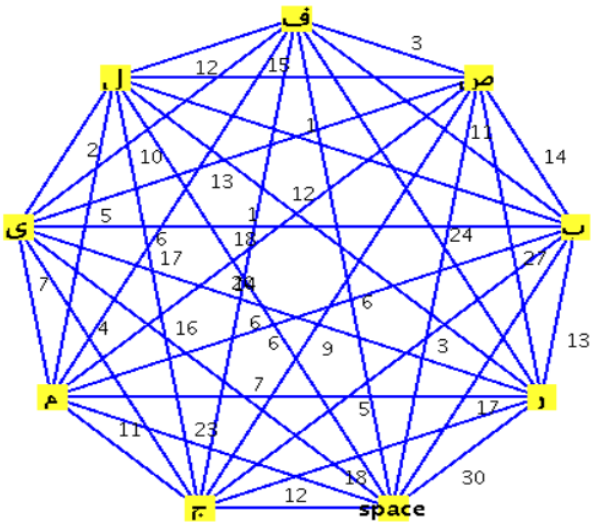



**Figure 2. complete graph of the key**

Then compute adjacency matrix K as a final Encryption Key:

$$K = \begin{bmatrix} 0 & 3 & 11 & 24 & 6 & 6 & 17 & 10 & 12 \\ 3 & 0 & 14 & 27 & 3 & 9 & 20 & 13 & 15 \\ 11 & 14 & 0 & 13 & 17 & 5 & 6 & 1 & 1 \\ 24 & 27 & 13 & 0 & 30 & 18 & 7 & 14 & 12 \\ 6 & 3 & 17 & 30 & 0 & 12 & 23 & 16 & 18 \\ 6 & 9 & 5 & 18 & 12 & 0 & 11 & 4 & 6 \\ 17 & 20 & 6 & 7 & 23 & 11 & 0 & 7 & 5 \\ 10 & 13 & 1 & 14 & 16 & 4 & 7 & 0 & 2 \\ 12 & 15 & 1 & 12 & 18 & 6 & 5 & 2 & 0 \end{bmatrix}$$

7- Compute the cipher text codes :

$$Cipher = (K \times PlainText)\ mod 101$$

$$Cipher = [\ 79\ \ 63\ \ 28\ \ 47\ \ 37\ \ 57\ \ 53\ \ 8\ \ 11\ ]$$

Cipher text is: [ت ج X ء ظ ل ن * – ]
8- End.

Then, the cipher code (*Cipher*) is hidden in a colored image as a cover and transformed via any communication media reaching to receiver side.

At the receiver side, the keyword is transformed to a code as in Table (1) then extracting the weight matrix as in encryption phase. An inverse key is built:

$$k^{-1} = \begin{bmatrix} 25 & 17 & 0 & 0 & 0 & 59 & 0 & 0 & 0 \\ 17 & 67 & 0 & 0 & 17 & 0 & 0 & 0 & 0 \\ 0 & 0 & 100 & 0 & 0 & 0 & 0 & 51 & 51 \\ 0 & 0 & 0 & 68 & 32 & 0 & 65 & 0 & 0 \\ 0 & 17 & 0 & 32 & 15 & 0 & 0 & 0 & 0 \\ 59 & 0 & 0 & 0 & 0 & 4 & 0 & 38 & 0 \\ 0 & 0 & 0 & 65 & 0 & 0 & 46 & 0 & 91 \\ 0 & 0 & 51 & 0 & 0 & 38 & 0 & 12 & 0 \\ 0 & 0 & 51 & 0 & 0 & 0 & 91 & 0 & 60 \end{bmatrix}$$

The key inverse used for reconstructing a plain message as in relation:

$$PlainCode = Cipher \times k^{-1}\ mod(101)$$

$$PlainCode = [\ 46\ \ 32\ \ 32\ \ 48\ \ 100\ \ 42\ \ 30\ \ 54\ \ 43\ ]$$

A replacement operation is implemented for codes of plain code with Table (1) to get the real message.

$$PlainText = [\ G, O, O, D, SPACE, L, U, C, K]$$

**Steganography Algorithm:**

The second step or proposed algorithm is steganography that hides the encrypted message in a cover file, the cover file is chosen as a colored image in RGB format and using the LSB method for hiding the secret message. The hiding algorithm steps are done as follows:

- The encrypted text message is delivered from encryption algorithm as a series of numbers, these numbers are transformed to ASCII code that is 7-bits to represent each number.

[34 4 2 56 57 3 12 ]→ ['100010' '000100' '000010' …]

- The image is separated into its color components ( RED - GREEN-BLUE) ,The GREEN component is transformed to ASCII code too.
- Each bits of the text message bits is embedded in the cover image replaced with LSB of GREEN component.
- The length of the secret message is embedded in the BLUE component by the same mechanism in

the first two pixels that make us able to hide a message with $2^{16}$ characters.
- Reconstruct the R-G-B components to form the image again.
- Send the image to the receiver.
- End.

Figure 3 shows the image before and after hiding a message "GOOD LUCK".


**Figure 3. the cover image (256×300) pixels**

At the receiver side the cover image is manipulated reversely to retrieve the encrypted text, as bellow:
- The image is separated into its color components (RED-GREEN-BLUE), the BLUE component is transformed to ASCII code.
- Taking the 16 bits of the LSB of the first 16 pixels to calculate the length L of the hidden message.
- Each bit of the LSB in the green component of the cover image is taken to build the ASCII code of the hidden message characters with the length L.
- After the cipher message is built depending on the Table (1), the decryption algorithm is used to expose the plain message.
- End.

## Experimental Results Analysis:

Different lengths of secret messages were encrypted and hidden in different RGB images with the proposed system. The system proves its efficiency in securing text messages with less time in the range between (0.03-0.07) seconds for encrypting messages in lengths between (9-300) characters and(0.035-0.1) seconds for hiding algorithm.

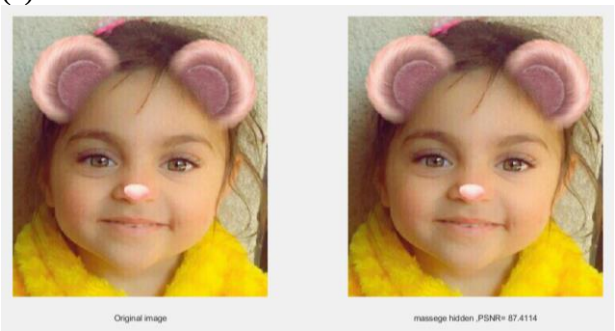
In this paper, the PSNR was calculated for the cover image before and after hiding. PSNR is a common analysis mostly used for comparing noise ratio between two matrixes (two images in case of image processing field). Typical values for the PSNR in lossy image are in range (30-50) dB, for the 8 bits images, where higher is better[19,20]. It is based on mean squared error (MSE) between them. MSE and PSNR (in dB) are defined as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I1(i,j) - I2(i,j)\right)^2$$

$$PSNR = 10 * log_{10} * \frac{255}{\sqrt[2]{MSE}}$$

Here I1 is the original cover image and I2 is the cover image after the message was hidden, the PSNR ratios for all experimental images before and after hiding were very high and MSE were low that means there is less noise for the cover image after and before hiding process for different sizes of messages and image resolution, Fig. 4. Also SSIM is calculated to check the imperceptibility requirement of the proposed system; the results are shown in Table 2.


(a)




(b)

**Figure 4. shows the differences among PSNR ratios for hiding a different lengths of text messages as in (a) (b) a message with (16,32) characters in 256×300 pixels**

**Table 2. Statistical analysis of the hiding technique**

| Message size (character) | Cover size (pixels) | PSNR ratio | MSE | SSIM |
|---|---|---|---|---|
| 16 | 256×300 | 91.5689 | 4.537e-05 | 1.0 |
| 32 | 256×300 | 87.4114 | 1.1801e-04 | 1.0 |
| 128 | 1200×760 | 97.4984 | 2.199074e-04 | 1.0 |
| 300 | 1200×760 | 85.9081 | 5.27546e-04 | 1.0 |

As shown in Table 2, the PSNR scores more than 85 dB for images before and after hiding process that means it is much better in securing and hiding

information with less noise ratio. And that was proved also with the values of MSE as well as SSIM comparing this methods with DMWT and DWT system in (4) that ranged from (30-51) dB for the images (256×256) pixels.

The most common attacks on stegosystem is traffic analysis. In it the intruder monitors the network traffic between sender and receiver and tries to capture any unusual communication pattern of information[17]. When something seems suspicious to the intruder means there are secret information. The steganography stage in this paper served the immunity of the system against traffic analysis, thus the innocent appearance of the cover letter concealing the secret message from attackers.

Statistical analysis, on the other hand, is used to analyze the content of the message to uncover a secret message[21]. The intruder can transform the message to ASCII code to check some pattern of numbers or counts the characters frequency… etc... So, the encryption process comes to distort the data before being covered, using a graph properties in generating the key matrix makes it hard to be found out and the encryption process encodes the message block by block with advantage of graph properties and this blocking encoding makes the system strong against common attacks that works on letter by letter analysis attacks.

comparing the proposed method of encryption with others like in (15) shows the advantages of proposed algorithm in many aspects like the size of cipher text regarding to plain text, Table(3) shows that the number of characters generated with (15) for n characters of plain text is $n^2$ character while proposed algorithm produced n cipher characters. Also time consumption in this algorithm was less than in (15) as shown in Fig. 5.

**Table 3. Relationship between plain text and cipher text size.**

| Character of plaintext | Cipher of (14) | Cipher of proposed method |
|---|---|---|
| 50 | 2500 | 50 |
| 100 | 10000 | 100 |
| 150 | 22500 | 150 |
| 200 | 40000 | 200 |
| 250 | 62500 | 250 |
| 300 | 90000 | 300 |

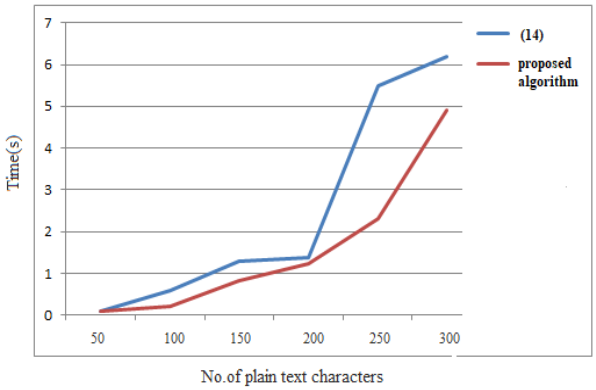



**Figure 5. The time consumption between proposed method of encryption and method of Hraiz S, Etaiwi W. in(15)**

## Conclusion:

Securing data of any type like text, images, sound, etc. became an essential matter to take care of many researchers and web users. Many researchers produced systems of the enormous variety in this scoop to support web and data manipulators with more and more securing approaches, at the opposite side the snipers and eavesdroppers develop methods for breaking security. This paper proposed an algorithm programmed by MAPLE and MATLAB. The algorithm is combined of two methods, encryption using the graph theory and steganography by LSB technique for securing text messages in a cover file of RGB image. The experimental tests using PSNR, MSE and SSIM proved the efficiency of the algorithm via testing many types and sizes of secret messages and cover image with the condition the cover is always bigger than the secret. The time consumption for a total process (encryption and hiding) was low.

Many enhancements can be added in future to strengthen the encryption and hiding algorithms by studying and investing more graph properties and types for encryption, like directed and complete and trivial graphs. Also, development can be directed towards securing different types of data such as images, video and audio, which reduces coding time, and improves the performance of the algorithm by investing more mathematical optimization methods.

## Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Besides, the Figures and images, which are not ours, have been given the permission for re-publication attached with the manuscript.

- Ethical Clearance: The project was approved by the local ethical committee in University of Basrah.

## Authors' contributions statement:

•Samaher Adnan role was in Graph theory principles and analysis for making data encryption.

•Renna D. Abdul-Wahhab was responsible for revision and proofreading of the manuscript.

•Enas Wahab works on steganography and algorithm programming

## References:

1. Liang R, Qin Y, Zhang C, Lai J, Liu M, Chen M. An Improved Arnold Image Scrambling Algorithm. IOP Conf Ser Mater Sci Eng. 2019;677(4).
2. Almuhammadi S, AL-Shaaby AA. A Survey on Recent Approaches Combining Cryptography and Steganography. In: ICIT 2017. 2017 .
3. Ali H, Abood E, Khudhair W. Using LSB Method For Hiding Hill Encrypted Grayscale And RGB Images In RGB Image. J Garmian Univ. 2019;6(SCAPAS Conferance):46–53 .
4. Iman M.G.Alwan. Image Steganography by Using Multiwavelet Transform. Baghdad Sci J. 2014;11(2):275–283 .
5. Hashim MM, Mohd Rahim MS, Alwan AA. A review and open issues of multifarious image steganography techniques in spatial domain. J Theor Appl Inf Technol. 2018;96(4):956–77 .
6. Cao Y. A new hybrid chaotic map and its application on image encryption and hiding. Math Probl Eng. 2013;2013 .
7. Sattar B. Sadkhan- SMIEEE, Abbas A. Mahdi and Rana S. Mohammed. Recent Audio Steganography Trails and its Quality Measures. 2019 International Conference of Computer and Applied Sciences (CAS2019),IEEE.2019:238-243.
8. Deng Z, Zhong S. A digital image encryption algorithm based on chaotic mapping. J Algorithm Comput Technol. 2019;13:174830261985347 .
9. Pareek NK, Patidar V, Sud KK. Block Cipher Using 1D and 2D Chaotic Maps. Int J Inf Commun Techol [Internet]. 2010 Apr;2(3):244–259. Available from: https://doi.org/10.1504/IJICT.2010.032412
10. Kwon OM, Park JH, Lee SM. Secure communication based on chaotic synchronization via interval time-varying delay feedback control. Nonlinear Dyn [Internet]. 2011;63(1):239–52. Available from: https://doi.org/10.1007/s11071-010-9800-9
11. Al-Bahrani EA, Kadhum RNJ. A new cipher based on Feistel structure and chaotic maps. Baghdad Sci J. 2019;16(1):270–80 .
12. Sahib Ogla RA. Symmetric- Based steganography technique using spiral-searching method for HSV color images. Baghdad Sci J. 2019;16(4):948–58 .
13. Yamuna M, Sankar A, Ravichandran S, Harish V. Encryption of a binary string using music notes and graph theory. Int J Eng Technol. 2013;5(3):2920–5 .
14. Akl SG. How to encrypt a graph. Int J Parallel Emergent Distrib Syst [Internet]. 2020;35(6):1–14. Available from: https://doi.org/10.1080/17445760.2018.1550771
15. Hraiz S, Etaiwi W. Symmetric encryption algorithm using graph representation. In: 2017 8th International Conference on Information Technology (ICIT). 2017. p. 501–6 .
16. Etaiwi W. Encryption Algorithm Using Graph Theory. J Sci Res Reports. 2014;3:2519–27 .
17. Akhter F. A secured word by word Graph Steganography using Huffman encoding. In: 2016 International Conference on Computer Communication and Informatics (ICCCI). 2016. p. 1–4 .
18. Kumari M, Kirubanad VB. Data encryption and decryption using graph plotting. Int J Civ Eng Technol. 2018;9(2):36–46 .
19. Abood EW. Combining a Hill Encryption Algorithm and LSB Technique With Dispersed Way for Securing Arabic and English Text Messages Hidden in Cover Image. Ibn AL-Haitham Journal For Pure and Applied Science. 2017 Sep 25;30(2):214-23.
20. Welstead, Stephen T. .Fractal and wavelet image compression techniques. SPIE Publication. 1999: 155–156.
21. Desoky A, Younis M. Graphstega: graph steganography methodology. Journal of Digital Forensic Practice.2008; 2(1): 27-36.

**Open Access** **Baghdad Science Journal** **P-ISSN: 2078-8665**
**Published Online First: July 2021** **2022, 19(1): 189-196** **E-ISSN: 2411-7986**

# تأمين الرسائل النصية باستخدام نظرية البيانات و إخفاء المعلومات

**سماهر عدنان عبدالغني** **رنا داود عبدالوهاب** **ايناس وهاب عبود**

قسم الرياضيات، كلية العلوم، جامعة البصرة، البصرة، العراق.

**الخلاصة:**

تامين البيانات يعتبر كعنصر مهم في انظمة لاتصالات وتناقل البيانات. ويكمن دوره الرئيسي في الحفاظ على المعلومات الحساسة بأمان وبشكل متكامل من المرسل إلى المتلقي ، وهناك نوعان من مبادئ الامنية هما التشفير وإخفاء المعلومات ، الأول يعمل على تغيير مظهر المعلومات ويغير من هيئتها في حين أن الثاني يخفيها من الدخلاء. النظام المصمم يقترح طريقة جديدة للتشفير باستخدام خصائص نظرية البيانات ؛ يعطي مفتاحًا تم إنشاؤه بتحويل كلمة السر الى مخطط (graph) من نوع متكامل complete ثم نستخرج مصفوفة التجاور adjacency matrix للمخطط ونستخدمها كمفتاح نهائي لتشفير النص وذلك باستخدام عملية الضرب (ضرب المصفوفات) للحصول على النص المشفر بعدها يتم استخدام طريقة البت الاقل اهمية Least Significant Bit LSB لإخفاء الرسالة المشفرة في صورة ملونة في المكون الاخضر G من مكوناتها. وكذلك تم توظيف معادلة تحليل PSNR والتي اثبتت كفاءة النظام في اخفاء الرسالة باقل تشويش ممكن بحوالي (85-97) dB لصورة الغلاف قبل وبعد عملية الاخفاء و MSE تتراوح بين (4.537e-05 -5.27546e-04) و SSIM=1.0 .

**الكلمات المفتاحية:** أمن البيانات ، نظرية الرسم البياني ، إخفاء وتشفير النصوص