

# Data and image encryption through steganography inside an image (MKTEXT-7) and (MK-12,13,14,15)

Mohammed Abdul Hameed Jassim Al-Kufi<sup>a</sup>, Hussein Abbas Al-Salihi<sup>b,\*</sup>

<sup>a</sup>Department of Mathematics, Faculty of Basic Education, University of Kufa, Najaf, Iraq

<sup>b</sup>Directorate of Education, Najaf Governorate, Najaf, Iraq

(Communicated by Javad Vahidi)

---

## Abstract

We sometimes need to hide data such as texts or images of international paintings or important manuscripts of a high degree of confidentiality and confidentiality, and this is done through several tasks, including archiving or transferring the image of the painting or manuscript to another place. Of course, archiving and preservation are twofold: the first is archiving, documentation and preservation of paper. The second: archiving, documenting and electronic preservation, which is currently the widest due to the digital development in transactions in various fields. In our algorithms, we will hide texts or an image of a global painting located within the abstract art of the artist Dr Luqman Al-Mudhaffar within other images. This is done by hiding the numerical values of the text characters or the color values of the image matrix within the image matrix in which we will hide the text or the image of the global panel that we will call the warehouse image. So that when you look at the image, you see the image of the warehouse, and there is no reference to the text or the image of the global plate. This work, which is considered the secret of hiding the text or the image, will depend on two basic conditions (the first is that the image of the warehouse matches the image of the global board in terms of the number of rows and the number of columns. The second is the use of a secret key to hide and show that only authorized persons know). These two algorithms, which we will call (MKTEXT-7) & (MK-12), are considered a new method for encoding text and images, and it is one of the products of the great digital development in computer science. Masking and comparisons with readings of previous algorithms. We hope that the results will be at the required level so that we can develop them into more complex algorithms. We will also later combine this algorithm with previous algorithms to come up with a more complex algorithm that intruders cannot decipher.

Keywords: Universal plate, Abstract art, Encryption, Hide the image, Hide the text, Decode concealment, Repository image, Repository text  
2020 MSC: Primary 90C33; Secondary 26B25

---

## 1 Introduction

The art of concealment is a method followed in many areas of life according to human needs, and it is in several forms. We refer to some of them as [22, 17, 19, 15].

---

\*Corresponding author

Email addresses: [mohammeda.alkufi@uokufa.edu.iq](mailto:mohammeda.alkufi@uokufa.edu.iq) (Mohammed Abdul Hameed Jassim Al-Kufi), [author@institution.org](mailto:author@institution.org) (Hussein Abbas Al-Salihi)

We often need to hide certain text in order to protect it from intruders. Either for the purpose of archiving and storing it, or for the purpose of sending it to another party. It is done to you through encryption algorithms known by us and by hackers. Where the intruder has to know the encryption key for the purpose of decrypting and showing the text, and this makes the possibility of decrypting and knowing the text easy for intruders. For this reason, some researchers resort to designing and preparing new encryption algorithms for the purpose of increasing the complexity of decryption, and this is of course a good thing that makes intruders unable to break the encryption due to their ignorance of the special algorithm used by the researcher [2].

As a modern method of hiding and encrypting the text, some researchers have used the method of hiding the text inside an image. To increase the complexity, we send more than one image for the purpose of complicating the matter for intruders [18].

Among the algorithms in place to hide text inside an image is the algorithm referred to by the engineer (Hussein Ahmed Talib), which is as follows with its development [22]. We select the image that we want to use as a repository for the text that we want to hide and convert it to a black and white image and then convert its color values to the binary system, where the image matrix will be converted to dimensions [4].

$$((\text{Number of rows} \times \text{Number of columns}) \times 8)$$

Example:-

IMAGEGRY =

241 111 251 90  
 132 85 21 199  
 200 100 210 144

IMAGEBINERY =

11110001  
 10000100  
 11001000  
 01101111  
 01010101  
 01100100  
 11111011  
 00010101  
 11010010  
 01011010  
 11000111  
 10010000

The way to hide is shown in table (1). (See Appendix A)

|   |  |  |
|---|--|--|
| Decimal number                                  | 241                                    |  |
| The number is in binary                         | 1 1 1 1 0 0 0 1                        |  |
| The number that is hidden                       | Hide the number (1) in the last column | Hide the number (0) in the last column |
| The resulting number in binary after masking    | 1 1 1 1 0 0 0 <u>1</u>                 | 1 1 1 1 0 0 0 <u>0</u>                 |
| The resulting number is in decimal after hiding | 241                                    | 240                                    |

It is clear from this that the masking does not affect the image significantly, but only darkens the brightness of the color by 1 and this is not distinguishable through the eyes. We return to our example above and apply the work to hide text within an image as shown in Table (2).

(\*) To complete the above question. We answer it through the table below, which shows our need of pixels according to the length of the text we want to hide.

| the system            | Image  | Text   |
|-----------------------|--|--|
| Decimal before hiding | 241 111 251 90<br>132 85 21 199<br>200 100 210 144   | Ali: 65 108 105  |
| The duo before hiding | 11110001<br>10000100<br>11001000<br>01101111<br>01010101<br>01100100<br>11111011<br>00010101<br>11010010<br>01011010<br>11000111<br>10010000 |  |
| The duo after hiding  | 11110001<br>10000100<br>11001000<br>01101110<br>01010100<br>01100100<br>11111011<br>00010101<br>11010011<br>01011010<br>11000111<br>10010001 | <p>We note that the default image matrix which contains 12 pixels, is not enough to hide the letter numbers of the word Ali, as the word Ali includes three letters, each letter has 7 ranks in the binary system, meaning that the word needs 21 pixels to store all its numbers in the binary system. Here we have a question: How do we deal with large texts? The answer to this question will be later in search context (*).</p> |
| Decimal after hiding  | 241 110 251 90<br>132 84 21 199<br>200 100 211 144   |  |

Table 1: shows our need for pixels in a normal image according to the length of the text that we want to hide

| The number of letters and symbols that make up the text | 10 | 100 | 200  | 300  | 400  | 500  | 1000 | 2000  |
|---|----|-----|------|------|------|------|------|-------|
| Number of pixels required for hiding                    | 70 | 700 | 1400 | 2100 | 2800 | 3500 | 7000 | 14000 |

Table 2: The maximum possibility of the normal warehouse image in hiding texts: -

| Dimensions of the gray matrix image    | (500 × 500) | (600 × 600) | (700 × 700) | (800 × 800) | (1000 × 1000) |
|--|-------------|-------------|-------------|-------------|---------------|
| Maximum text length that can be hidden | 35714       | 51428       | 70000       | 91428       | 142857        |

And it is possible to develop the algorithm in the use of the color image in three dimensions, which will lead to doubling the possibility of hiding to three times, as is clear in the following table:

Table 3: Represents the maximum potential of the colored warehouse image to hide texts:-

|  |                 |                 |                 |                 |                   |
|--|-----------------|-----------------|-----------------|-----------------|-------------------|
| Dimensions of the color image matrix   | (500 × 500 × 3) | (600 × 600 × 3) | (700 × 700 × 3) | (800 × 800 × 3) | (1000 × 1000 × 3) |
| Maximum text length that can be hidden | 107142          | 154285          | 210000          | 274285          | 428571            |

The program that we used to convert the array numbers from the decimal system to the binary system and then return them to the decimal system. Now we hide the text by cramming the algorithm steps between the third statement and the fourth statement of the above program. We return to our example above in which we hid the word (Ali) and notice how we retrieve the word. We explain this through the short table below:

Table 4: How to retrieve hidden text in gray scale image.

| the system                                | Image  | Text  |   |  |   |  |
|---|--|---|---|--|---|--|
| Decimal before text retrieval             | 241 110 251 90<br>132 84 21 199<br>200 100 211 145   | Ali:- [65 108 105]  |   |  |   |  |
| Binary before text retrieval              | 11110001<br>10000100<br>11001000<br>01101110<br>01010100<br>01100100<br>11111011<br>00010101<br>11010011<br>01011010<br>11000111<br>10010001 | 1000001<br>1101100<br>1101001   |   |  |   |  |
| Binary after text retrieval               | 11110000<br>10000100<br>11001000<br>01101110<br>01010100<br>01100100<br>11111010<br>00010100<br>11010010<br>01011010<br>11000110<br>10010000 | <p>Comparison of the image array before hiding and after retrieval</p> <table border="1"> <tr> <td>The original image before hiding the text</td> <td>[241 111 251 90<br/>132 85 21 199<br/>200 100 210 144]</td> </tr> <tr> <td>The original image after showing the text</td> <td>[240 110 250 90<br/>132 85 20 198<br/>200 100 210 144]</td> </tr> </table> <p>We note that there is a difference and this difference does not matter because the goal is to hide a text and then retrieve it and it has been retrieved and it does not matter how the stored image is after that.</p> | The original image before hiding the text | [241 111 251 90<br>132 85 21 199<br>200 100 210 144] | The original image after showing the text | [240 110 250 90<br>132 85 20 198<br>200 100 210 144] |
| The original image before hiding the text | [241 111 251 90<br>132 85 21 199<br>200 100 210 144]   |   |   |  |   |  |
| The original image after showing the text | [240 110 250 90<br>132 85 20 198<br>200 100 210 144]   |   |   |  |   |  |
| Decimal after text retrieval              | 240 110 250 90<br>132 84 20 198<br>200 100 210 144   |   |   |  |   |  |

This algorithm is one of the most famous and simplest algorithms used to hide texts. Through this introduction, we have developed the possibility of using the colored image to hide the text.

Of course, this algorithm is not considered a solid encryption method because it did not depend on an encryption key, and it is very possible to decrypt the concealment easily once the method is known. But at the same time it is considered a good masking method.

## 2 Hiding a folder inside an image

This is one of the methods that most computer users are ignorant of, which is the ability to hide important folders inside an image. Many, if not all, computer users have important and personal information and data and do not want anyone to see it, whether family members or co-workers, and also these general things differ from one person to another. The important thing is that most users want to hide these files, and everyone has his own way and method of hiding, some of them use the traditional method, and some of them use a specific program, and unfortunately all of these methods can be easily discovered by any professional computer user. One of the best ways to hide files is to hide them inside an image. We are not going to explain the steps of this somewhat complicated method, but we will suffice to refer to them [19].

We suffice with this amount of touching on previous works in the use of the method of hiding files and data, and we return to the essence of the title of our research [15]. We indicated at the beginning of this research and in the context of the summary that we will discuss how to hide a text or an image of a global painting inside an image that we called the warehouse image[12]. We have chosen a picture of a painting from the abstract art of the artist Dr. Luqman Al-Mudhaffar, and we will focus through our research on how to hide the text or image of this painting inside the warehouse image.

### 3 Abstract art

Abstract art depends on the simplicity of shapes and colors and moves away from an accurate description of the reality of things or their nature and giving the recipient or viewer an opportunity to interpret the work as he sees it with his own view. It is the most difficult of the arts because it needs to know how to draw well, to have a very formed sense of colors, and to be a true poet.

The abstract painting is only a figurative piece, and does not express a subject, it is a subject by itself and the values of its internal construction are focused on the cohesion of its parts and the organization of its elements. Abstraction in the artwork is a picture of the inner feelings present in the human conscience

And the abstract artist in his first works, we see him using some of the abstract figurative symbols. found in nature and taking them to the farthest extents of abstraction and considering them an element derived from the elements of the material surroundings and giving them titles that are abstract of meaning. He works on the basis of the shapes he creates, as they have a meaning greater than just a natural or decorative painting. Because he is liberated from reality through certain materials that have special expressive capabilities in which he repeats rhythms, proportions, colors, delusions and places of light and in which images of the universe are reflected. It carries interpretations, possibilities, and visual interference within the artist's imagination, which he and the image of reality as his mind sees, and does not record the glimpse presented by the mental image, but rather the image of reality in the essential nature of a complex continuous intertwined with complex relationships. The experimental artist paints what he knows and what he feels in his imagination, as in this painting that represents Color values where the artist looks at the abstract painting that he tries to translate into a group of colors and lines and when he feels the value of the color (dark and Al-Fatih) and then defines the expression of color temperature [5, 1, 10, 16, 20, 9]. Whenever the artist masters the degree of color and its temperature, he presents a wonderful painting characterized by the clarity of the psychological and dramatic state of the artwork, for example, the light and dark values that appear in the artwork (a city on the beach, an oil painting on canvas 30×40) It has the aesthetics of the abstract shapes in this painting of buildings and houses overlooking the beach of different colors, a mixture of blue, which represents the sky and water, and the warm colors such as yellow, red and orange represent the vitality of the city, then the white color around the shape, and the overlapping colors that represent formations and blocks for some buildings and houses and their reflection in the water It is not necessary for the color to follow a representational form in order to be beautiful. It is possible to introduce colors and harmonious rhythmic and kinetic relationships to simulate the world of ideas, imaginary images and emotions abstract from the material world. There are three types of abstract art, namely (absolute abstract vision), and the owners of this art use horizontal and vertical lines and main colors ( Cubist abstract vision), most notably the artist Picasso who used the abstraction of shapes and used Lines, angles, showing color and light (experimental expressive vision) and the owners of this art used abstraction of colors as a method for them in drawing their paintings and showing the single form in the painting by highlighting the colors. A city on the beach painting belongs to the first type, which is the absolute abstract vision in the artist's use of horizontal and vertical lines and highlighting the main colors of yellow, red and blue [11, 3].

### 4 Research idea

The idea of the research is focused on the issue of hiding text or an image of international panels that we want to withhold any information about to anyone other than authorized. Although hiding is a method of encryption, we cannot consider this algorithm as an encryption algorithm in the true sense of the word unless it is enhanced by one of the encryption algorithms that includes an encryption key, but the goal is achieved through this method, which is to hide text or an image of a global panel . The idea is to combine color values into matrixes of values. The color of the image that we want to hide and the image of the warehouse between them in a new mathematical style that was not used previously. Which makes our algorithm unique in this way and this way. It is worth noting that we will develop this algorithm later, and make it an algorithm for hiding and encrypting at the same time.



Figure 1: A painting titled (The City on the Beach), which we will hide.

Through the course of our research, we will learn about the steps of applying the cloaking process according to the implementation of this algorithm of ours (MKTEXT-7) for texts and (and MK-12,13,14,15) which are integrated algorithms for cloaking, which will be followed by other later algorithms to develop them to perform the hiding function only To hide and encrypt based on matrix analyzes (SVD, GSVD, LU, QR) [6][8] and other matrix analyzes, which is a new generation in the world of cryptography and informatics, due to its superior flexibility in analyzing matrices based on eigenvalues, eigenvectors, individual values, and individual right-based vectors or left, and this is a long topic to explain. Therefore, we leave the discussion about it at the time when we start the scientific research that develops this algorithm into concealment and encryption [6][8]. An illustrative example of hide text in color image is displayed in figure (2), see Appendix B.

## 5 Methodology of proposed algorithm

We have explained through the abstract the methodology of work in detail and we will repeat it here within this item of research The working principle of our proposed algorithm is

- Convert the numerical values of the text or the color values of the image that we want to Steganography from the decimal system to the binary system.
- Convert the color values of the stored image that we will use to Steganography the text or image from decimal to binary (We are preparing eight copies of them No. 1, No. 2... No.8).
- For the text or image that we want to Steganography it, the matrix of numeric or color values will be transformed into an matrix of numerical values in the binary system and with eight columns.
- The same is the case with the repository matrix.
- We will explain if we want to Steganography an image, and the same thing will be with the text.
- We put the first column from the left of the image matrix that we want to Steganography (in binary system) instead of the first column from the right of the warehouse image matrix No. 1 (also in binary).
- We put the second column from the left of the image matrix that we want to Steganography (in binary system) instead of the first column from the right of the warehouse image matrix No. 2 (also in binary).
- And so on until we get to put the eighth column from the left of the image matrix that we want to Steganography (in binary system) instead of the first column from the right of the warehouse image matrix No. 8 (also in binary).
- So we have hidden the image in eight copies of the warehouse image.
- We can used four copies of the warehouse image. Where we can hide the first and second columns from the left of the image that we want to hide in the place of the first and second columns from the right in the warehouse image No. 1. And can hide the third and fourth columns from the left of the image that we want to hide in the

place of the first and second columns from the right in the warehouse image No. 2. And can hide the Fifth and sixth columns from the left of the image that we want to hide in the place of the first and second columns from the right in the warehouse image No. 3. And can hide the seventh and eighth columns from the left of the image that we want to hide in the place of the first and second columns from the right in the warehouse image No. 4.

- We can use only two copies of the warehouse image. Where we can hide the first, second, third and fourth columns from the left of the image that we want to hide in the place of the first, second, third and fourth columns from the right in the warehouse image No. 1. And can hide the fifth, sixth, seventh and eighth columns from the left of the image that we want to hide in the place of the first, second, third and fourth columns from the right in the warehouse image No. 2.
- By any of these three ways, we have Steganography the image within another image. The details of the method and the results of the work will be clarified by the following

An illustrative example of hide text in color image:










|   |   |   |   |
|---|---|---|---|
| Text before hiding                      | Dale Carnegie is considered one of the world-renowned writers for his smooth narration of the story and his way of convincing the reader of his point of view. Here is the international writer and writer whom I read a lot. Especially the book How to Make Friends taught me the wisdom that says that nothing in life is more precious than a friend. |   |   |
| repository image name                   | Mohammed Alkufi   | Luqman Almudhafar   | Mohammed Dosh   |
| Repository image before hiding the text |   |   |   |
| Repository image after hiding the text  |    |  |  |
| Repository image after showing text     |    |  |  |
| text after display                      | Dale Carnegie is considered one of the world-renowned writers for his smooth narration of the story and his way of convincing the reader of his point of view. Here is the international writer and writer whom I read a lot. Especially the book How to Make Friends taught me the wisdom that says that nothing in life is more precious than a friend. |   |   |
| Hiding time/sec                         | 13.627  | 17.9070   | 2.9170  |
| Display time/sec                        | 3.3620  | 3.6000  | 0.8820  |

Figure 2: The text we want to hide and three images used as a repository before and after hiding.

## 6 Results for hidden text

We will explain the results through detailed tables as it is shown in table (7).

We are satisfied with this amount of explanation of the algorithm of hiding text in an image (MKTEXT-7), and now we move to our second algorithm in this research, which is to hide an image in an image (MK-12). This work is not as easy as hiding text inside an image, because the image has a lot of color values that are difficult to hide in the way we used in the text.

It must be said that it is possible to use the same method of masking the text (MKTEXT-7) to hide the image, but in this case we will need four images provided that two numbers of numbers are used in the binary system of the stored image. But if we use only one order of numbers for the stored image, we will need eight images to hide.

Our algorithm (MK-12) is completely different from the text masking algorithm (MKTEXT-7). We will later hide a specific image in three ways.

Table 5: Application of the algorithm to English and Arabic text.

| Language | Text Before hiding | The numerical values of the text of the decimal system Before hiding | Numerical values for text in binary system Before hiding | Numerical values for text in binary system After hiding | The numerical values of the text of the decimal system After hiding | Text After hiding | hiding time Sec. | Unhide time Sec. |
|----------|--------------------|--|--|---|---|-------------------|------------------|------------------|
| English  | M                  | 77   | 1001101  | 1001101   | 77  | M                 | 2.5700           | 0.4780           |
|          | o                  | 111  | 1101111  | 1101111   | 111   | o                 |                  |                  |
|          | h                  | 104  | 1101000  | 1101000   | 104   | h                 |                  |                  |
|          | a                  | 97   | 1100001  | 1100001   | 97  | a                 |                  |                  |
|          | m                  | 109  | 1101101  | 1101101   | 109   | m                 |                  |                  |
|          | m                  | 109  | 1101101  | 1101101   | 109   | m                 |                  |                  |
|          | e                  | 101  | 1100101  | 1100101   | 101   | e                 |                  |                  |
|          | d                  | 100  | 1100100  | 1100100   | 100   | d                 |                  |                  |
| Arabic   | م                  | 1605   | 11001000101  | 11001000101   | 1605  | م                 | 2.9660           | 0.7100           |
|          | ح                  | 1581   | 11000101101  | 11000101101   | 1581  | ح                 |                  |                  |
|          | م                  | 1605   | 11001000101  | 11001000101   | 1605  | م                 |                  |                  |
|          | د                  | 1583   | 11000101111  | 11000101111   | 1583  | د                 |                  |                  |
|          | د                  | 32   | 00000100000  | 00000100000   | 32  | د                 |                  |                  |
|          | /                  | 1575   | 11000100111  | 11000100111   | 1575  | /                 |                  |                  |
|          | ك                  | 1604   | 11001000100  | 11001000100   | 1604  | ك                 |                  |                  |
|          | و                  | 1603   | 11001000011  | 11001000011   | 1603  | و                 |                  |                  |
|          | و                  | 1608   | 11001001000  | 11001001000   | 1608  | و                 |                  |                  |
|          | ف                  | 1601   | 11001000001  | 11001000001   | 1601  | ف                 |                  |                  |
|          | ي                  | 1610   | 11001001010  | 11001001010   | 1610  | ي                 |                  |                  |

The first / using the same algorithm (MKTEXT-7), by dealing with one order of numbers in the binary system of the stored image and we will call this algorithm (MK-12).

The second / using the same algorithm (MK-12) by dealing with two orders of numbers in the binary system of the stored image and we will call this algorithm (MK-13).

Third / using a new algorithm that we will call (MK-14), which is completely different from (MKTEXT-7), (MK-12), (MK-13) algorithms. First method (MK-12):-

We will illustrate the first method through a simple illustrative example that approximates the idea. Assume the image that we want to hide is  $A=[(124\&111@93\&108)]$ . Suppose the warehouse image is  $B=[(250\&98@154\&36)]$ . We convert the color values of the two arrays of images from the decimal system to the binary system, and we will put them in the form of columns for clarity. Conclusions should state concisely the most important propositions of the paper as well as the author’s views of the practical implications of the results.

|      |    |    |    |    |    |    |    |    |
|------|----|----|----|----|----|----|----|----|
|      | c1 | c2 | c3 | c4 | c5 | c6 | c7 | c8 |
| A1 = | 0  | 1  | 1  | 1  | 1  | 1  | 0  | 0  |
|      | 0  | 1  | 0  | 1  | 1  | 1  | 0  | 1  |
|      | 0  | 1  | 1  | 0  | 1  | 1  | 1  | 1  |
|      | 0  | 1  | 1  | 0  | 1  | 1  | 0  | 0  |

|      |    |    |    |    |    |    |    |    |
|------|----|----|----|----|----|----|----|----|
|      | c1 | c2 | c3 | c4 | c5 | c6 | c7 | c8 |
| B1 = | 1  | 1  | 1  | 1  | 1  | 0  | 1  | 0  |
|      | 1  | 0  | 0  | 1  | 1  | 0  | 1  | 0  |
|      | 0  | 1  | 1  | 0  | 0  | 0  | 1  | 0  |
|      | 0  | 0  | 1  | 0  | 0  | 1  | 0  | 0  |

We copy the matrix B1 eight copies in order to save the eight columns of matrix A instead of the eighth column in the matrix B1 as it is shown in table (8).

Thus, we have hidden the columns of the matrix of color values for the default image A in the binary system A1, in the last column of the repository matrix B in the binary system B1, after we copied B1 to eight copies, so we have eight new images B, all of which are considered repositories to hide image A. The image has not changed B only the intensity of brightness sometimes by 1 increase or decrease and this can never be distinguished.

### Results and readings

Below are the results and readings we obtained by executing our MK-12 algorithm using MATLAB software.

#### Second method (MK-13):

We will illustrate the second method through the same example as the first method (MK-12). Assume the image that we want to hide is  $A = \begin{bmatrix} 124 & 111 \\ 93 & 108 \end{bmatrix}$ . Suppose the warehouse image is  $B = \begin{bmatrix} 250 & 98 \\ 154 & 36 \end{bmatrix}$ . We convert the color values of the two arrays of images from the decimal system to the binary system, and we will put them in the form of columns for clarity.







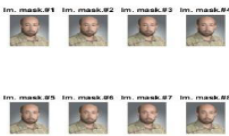










|   |   |   |
|---|---|---|
| The image that we want to hide  |   |   |
| Masking Image before hide   | Masking Image of eight copies after hide  | Image after decoding hide   |
|    |    |    |
|    |    |    |
|   |    |   |
| <b>Masking Image #1 after hide</b>  |   |   |
| Mohammed Alkufi   | Luqman Almodhafar   | Mohammed Dosh   |
|  |  |  |

Figure 3: Results that we obtained by executing our MK-12 algorithm using MATLAB program

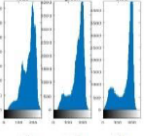
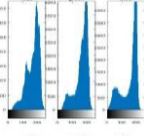
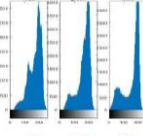
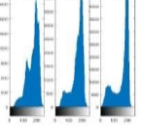
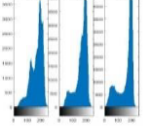
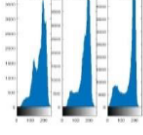
#### Note on the (MK-14) algorithm:

The stored image shows some distortion and this is evident by revealing the histogram of the original image before masking and the image after masking according to algorithms (MK-14), (MK-13), (MK-12) we will notice the difference as follows:-

## 7 Conclusion

- 1- This algorithm is considered a new method of encryption for text and image.
- 2- The (MK-14) algorithm is characterized by that it can represent a way to hide two images at the same time. Where it is possible to swap the positions of the columns in the color values of the warehouse matrix in the binary system by the way of the mirror. Where the positions of the first, eighth, second, seventh, third, sixth, fourth and fifth columns are changed to show us a new image. This is an idea for a new research that will be completed at a later time.
- 3- The algorithm (MKTEXT-7) and (MK-14) can be implemented. Simultaneously to hide an entire message that includes text and an image, due to the great flexibility granted by the binary system in manipulating color values. This will be activated through a new research that will be completed at a later time.

Table 7: Readings we obtained by executing our MK-12 algorithm using MATLAB program.

| Masking Image of hide                  | Mohammed Alkufi   | Loqman Almudhaffar  | Mohammed Doush  |
|--|---|---|---|
| Image histogram before hide            |  |  |  |
| Image histogram after decoding hide    |  |  |  |
| Hiding time sec.                       | 16.206  | 18.1540   | 17.1840   |
| Decoding hide time sec.                | 4.9180  | 4.754   | 4.4380  |
| Mean error                             | 0   | 0   | 0   |
| MSE                                    | 0   | 0   | 0   |
| PSNR                                   | ∞   | ∞   | ∞   |
| Entropy before hide                    | 7.2421  | 7.2421  | 7.2421  |
| Entropy after decoding hide            | 7.2421  | 7.2421  | 7.2421  |
| Standard deviation before hide         | 11.8786   | 11.8786   | 11.8786   |
| Standard deviation after decoding hide | 11.8786   | 11.8786   | 11.8786   |
| Correlation coefficient                | 1   | 1   | 1   |

$$A1 = \begin{matrix} & c1 & c2 & c3 & c4 & c5 & c6 & c7 & c8 \\ \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 1 \\ 0 \end{matrix} \end{matrix}$$

$$B1 = \begin{matrix} & c1 & c2 & c3 & c4 & c5 & c6 & c7 & c8 \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{matrix}$$

|                         |     |     |     |     |     |     |     |     |
|-------------------------|-----|-----|-----|-----|-----|-----|-----|-----|
| Column from A1          | c1  | c2  | c3  | c4  | c5  | c6  | c7  | c8  |
| Hiding column           | c8  | c7  | c8  | c7  | c8  | c7  | c8  | c7  |
| Metres of hiding column | B11 | B11 | B12 | B12 | B13 | B13 | B14 | B14 |

Table 8: Showing how to store the columns of matrix A instead of the seventh and eighth columns in matrix B1.

| The matrix A   | $A1 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 0 \\ 0 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 1 \\ 0 \end{matrix} \end{bmatrix}$  |  |  |  |  |  |  |  |                           |  |  |  |
|--|--|--|--|--|--|--|--|--|---------------------------|--|--|--|
| The matrix B1 before change the eighth column  | $B11 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ |  |  |  | The matrix B1 after change the eighth column             |  |  |  | The matrix B After hiding |  |  |  |
| $B11 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ | $B11 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ |  |  |  | $B = \begin{bmatrix} 250 & 98 \\ 154 & 38 \end{bmatrix}$ |  |  |  |                           |  |  |  |
| $B12 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ | $B12 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ |  |  |  | $B = \begin{bmatrix} 251 & 97 \\ 154 & 37 \end{bmatrix}$ |  |  |  |                           |  |  |  |
| $B13 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ | $B13 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ |  |  |  | $B = \begin{bmatrix} 251 & 99 \\ 155 & 39 \end{bmatrix}$ |  |  |  |                           |  |  |  |
| $B14 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ | $B14 = \begin{bmatrix} (c1) & (c2) & (c3) & (c4) & (c5) & (c6) & (c7) & (c8) \\ \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 0 \\ 1 \\ 1 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 0 \\ 1 \\ 0 \\ 0 \end{matrix} \end{bmatrix}$ |  |  |  | $B = \begin{bmatrix} 248 & 99 \\ 154 & 36 \end{bmatrix}$ |  |  |  |                           |  |  |  |

## 8 Discussion

The algorithm is considered a new chapter in the world of cryptography, but it needs extensive study to strengthen it by adding an encryption key that makes the invisibility immune and intruders cannot penetrate it.



Figure 4: results that we obtained by executing our MK-13 algorithm using MATLAB program.

Table 9: Readings that we obtained by executing our MK-13 algorithm using MATLAB program.

| Masking image of hide                  | Mohammed Alkufi | Luqman Almudhaffar | Mohammed Doush |
|--|-----------------|--------------------|----------------|
| Image histogram before hide            |                 |                    |                |
| Image histogram after decoding hide    |                 |                    |                |
| Hiding time sec.                       | 7.1700          | 7.5580             | 7.1190         |
| Decoding hide time sec.                | 2.2000          | 2.237              | 2.2570         |
| Mean error                             | 0               | 0                  | 0              |
| MSE                                    | 0               | 0                  | 0              |
| PSNR                                   | ∞               | ∞                  | ∞              |
| Entropy before hide                    | 7.2421          | 7.2421             | 7.2421         |
| Entropy after decoding hide            | 7.2421          | 7.2421             | 7.2421         |
| Standard deviation before hide         | 11.8786         | 11.8786            | 11.8786        |
| Standard deviation after decoding hide | 11.8786         | 11.8786            | 11.8786        |
| Correlation coefficient                | 1               | 1                  | 1              |

- The algorithm can be developed to (MK-15) by adding the fourth column of the matrix of color values of the image stored in binary system to the columns that are used to hide the image. But in this case, a clear confusion will appear on it after hiding, and this of course does not matter because we aim to hide an image.
- There is the possibility of minimizing the images that we want to hide and merging so that all four images are merged into a single digital matrix with dimensions equal to the dimensions of the single image, for you to facilitate and shorten the masking process.
- For the gray image. Three images can be hidden simultaneously in a color image with the same dimensions, because the gray image is in a two-dimensional matrix, while the color warehouse image is in a three-dimensional matrix.

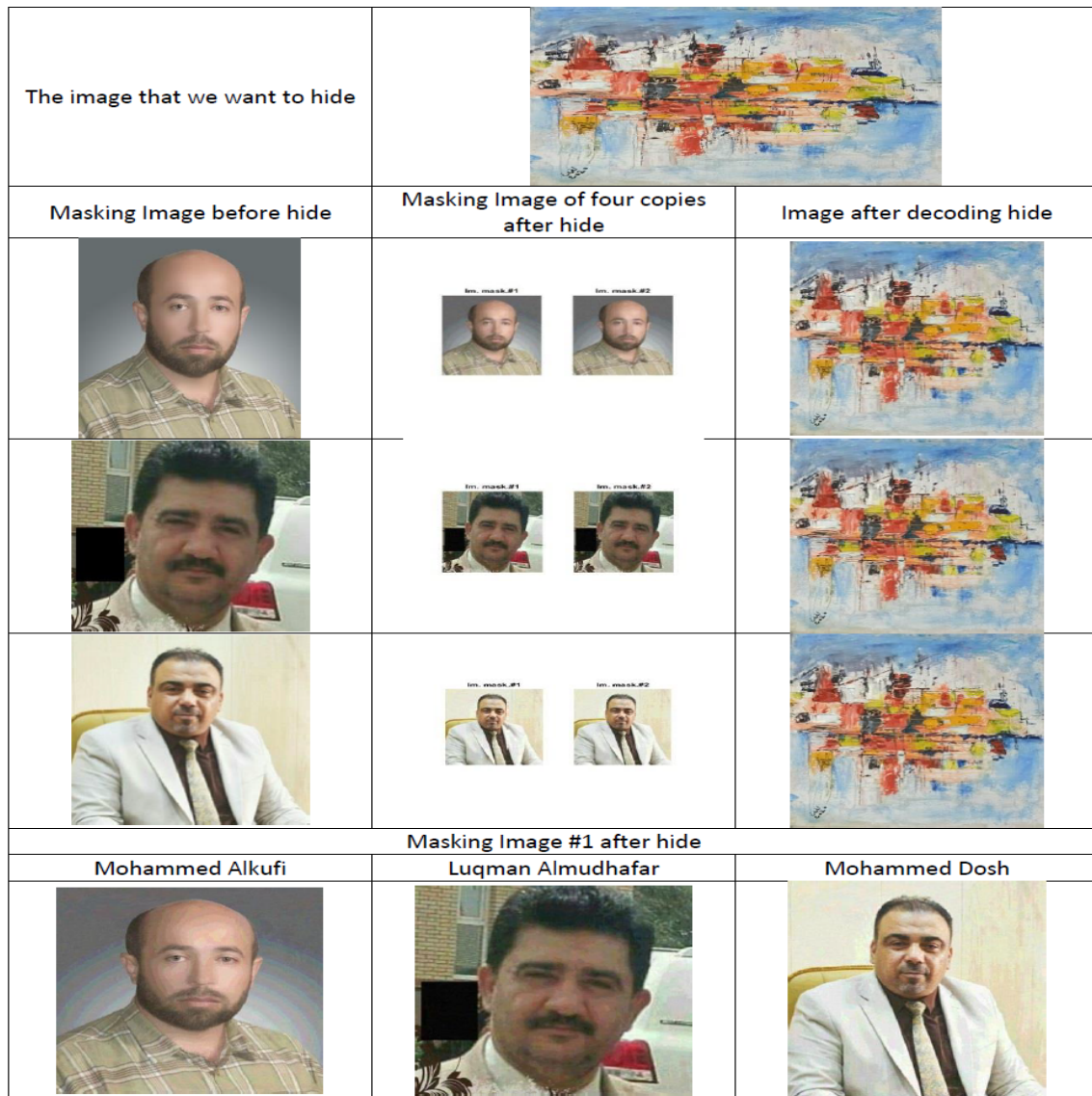


Figure 5: Results that we obtained by implementing our MK-14 algorithm using MATLAB program.

- The algorithm can be developed by adding a steganographic key that makes it impossible for intruders to decipher the cloak. As it all currently represents a non-integrated encryption process because it hides only and does not depend on a key that is safe for the hiding process.

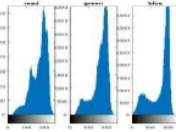
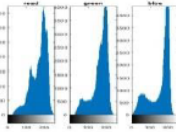
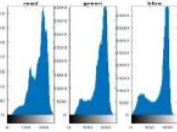
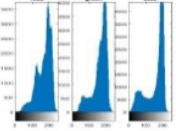
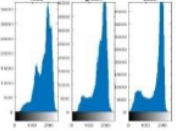
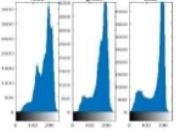
## 9 Future researches

We will perform a research that depends on the recursive masking algorithm. That is, we hide picture No. (1) in picture No. (2), then we hide picture No. (2) in picture No. (3). Then, through another research, we increase the stages of concealment by adding picture No. (4) and picture No. (5), and so on.

## 10 Acknowledgment

At the end of our research, and first of all, I would like to thank everyone who Dr. Luqman Almudhafar and Dr. Mohammed Dosh that help me by their personal photos to implement the algorithm. As well we must record our thanks and appreciation to Miss (Maryam Muhammad al-Kufi), who helped us translate and organize the research, wishing her success and continued success. research team

Table 10: Readings that we obtained by implementing our MK-14 algorithm using MATLAB program.

| Masking Image of hide                  | Mohammed Alkufi   | Loqman Almudhaffar   | Mohammed Doush  |
|--|---|--|---|
| Image histogram before hide            |  |  |  |
| Image histogram after decoding hide    |  |  |  |
| Hiding time sec.                       | 5.4800  | 6.2400   | 4.4830  |
| Decoding hide time sec.                | 2.8300  | 2.4470   | 1.7830  |
| Mean error                             | 0   | 0  | 0   |
| MSE                                    | 0   | 0  | 0   |
| PSNR                                   | $\infty$  | $\infty$   | $\infty$  |
| Entropy before hide                    | 7.2421  | 7.2421   | 7.2421  |
| Entropy after decoding hide            | 7.2421  | 7.2421   | 7.2421  |
| Standard deviation before hide         | 11.8786   | 11.8786  | 11.8786   |
| Standard deviation after decoding hide | 11.8786   | 11.8786  | 11.8786   |
| Correlation coefficient                | 1   | 1  | 1   |

| Image             | The original image  | (MK-12)   | (MK-13)  | (MK-14)   |
|-------------------|---|---|--|---|
| Mohammed Alkufi   |   |   |   |   |
| Luqman Almudhafar |  |  |  |  |
| Mohammed Dosh     |  |  |  |  |



## References

- [1] M.A.F. Al-Husainy and D.M. Uliyan, *Image steganography technique based on extracted chains from the secret Key*, J. Engin. Appl. Sci. **13** (2018), 4235–4244

- [2] S. Almuhammadi and A. Al-Shaaby, *A survey on recent approaches combining cryptography and steganography*, *Comput. Sci. Inf. Technol.* **2017** (2017), 63–74.
- [3] K.I. Al-Saif and A.S. Abdullah, *Color image enhancement based on contourlet transform coefficients*, *Aust. J. Basic Appl. Sci.* **7** (2013), no. 8, 207–213.
- [4] T.S. Barhoom and S.M.A. Mousa, *A steganography LSB technique for hiding image within image using blowfish encryption algorithm*, *Int. J. Res. Eng. Sci.* **3** (2015), 61–66.
- [5] M. Douglas, K. Bailey, M. Leeney and K. Curran, *An overview of steganography techniques applied to the protection of biometric data*, *Multimedia Tools Appl.* **77** (2018), no. 13, 17333–17373.
- [6] D. Gollmann, *Computer Security*, Wiley Interdiscip. Rev.: Comput. Statist. **2** (2010), no. 5, 544–554.
- [7] Q.M. Hussein, *New metrics for steganography algorithm quality*, *Int. J. Adv. Sci. Technol.* **29** (2020), no. 2, 2092–2098.
- [8] J.L. Kamm, *SVD-Based Methods For Signal And Image Restoration*, PhD Thesis, Emory University, United States, 1998.
- [9] S.A. Laskar and K. Hemachandran, *Combining JPEG steganography and substitution encryption for secure data communication*, *Comput. Sci. Inf. Technol.* **5** (2012), 149–160.
- [10] H. Mal Allah, *The semiotic development of the structure of the abstract form*, *Arab Horizons Magazine* **5-6** (2001), 97.
- [11] A. McAndrew, *An Introduction to Digital Image Processing with Matlab*, Course Technology, 2004.
- [12] P.P. Meier, *Steganography 2.0: Digital resistance against repressive regimes*, 5 June 2009, [irevolution.wordpress.com](http://irevolution.wordpress.com).
- [13] S. Mishra, V.K. Yadav, M.C. Trivedi and T. Shrimali, *Audio steganography techniques: A survey*, *Advances in Computer and Computational Sciences*, Springer, Singapore, 2018, pp. 581–589.
- [14] T. Morkel, *Image steganography applications for secure communication*, Doctoral dissertation, University of Pretoria, 2012.
- [15] K. Muhammad, J. Ahmad, M. Sajjad and M. Zubair. *Secure image steganography using cryptography and image transposition*, arXiv preprint arXiv:1510.04413 (2015).
- [16] A.K.J. Mujaisir, *The Code of Abstraction between Communication and the Aesthetic Concept in Modern Painting*, Master's Thesis, University of Baghdad, College of Fine Arts, Department of Fine Arts, 2003.
- [17] V. Nagarajan, N.K. Abitha Gladis and D. Nagarajan, *Compression and denies of an image by LU and QR decomposition*, *Int. J. Res. Engin. Appl. Sci.* **6** (2016), no. 9, 1–4.
- [18] F.A.P. Petitcolas, *Information hiding: A survey*, *Proc. IEEE* (special issue) **87** (1999), no. 7, 1062–1078.
- [19] A. Schwarzenberg-Czerny, *On matrix factorization and efficient least squares solution*, *Astron. Astroph. Suppl. Ser.* **110** (1995), 405.
- [20] D.R. Sridevi, P. Vijaya and K.S. Rao, *Image steganography combined with cryptography*, *Counc. Innov. Res. Peer Rev. Res. Pub. Syst. J.* **9** (2013), no. 1.
- [21] K. Szczypiorski, *Steganography in TCP/IP networks. State of the art and a proposal of a new system-HICCUPS*, Warsaw University of Technology, Poland Institute of Telecommunications, Warsaw, Poland, 2003.
- [22] H.A. Talib, *Hide Text in Image By MATLAB- Technical Library*, <https://books-library.net/free-717582257-download>.