Int. J. Nonlinear Anal. Appl. 13 (2022) 2, 227–235
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.6240

Using LU analysis to encryption the images formed after steganography of image into another image

Mohammed Abdul Hameed Jassim Al-Kufi[a], Hussein Abbas Shniar Al-Salihi[b,*]

[a] *Department of Mathematics, Faculty of Basic Education, University of Kufa, Iraq*

[b] *Department of Mathematics, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq*

(Communicated by Javad Vahidi)

Abstract

In this research, we will hide an image we call the secret image inside another image we call the repository. After converting the color values of both images from decimal to binary, we copy the stored images into four copies and use the eighth and seventh bits of these copies to hide the full bits of the secret image starting with the first. Two to be replaced in the eighth and seventh parts, respectively in the first version, then we hide the third and fourth bits of the secret image in the eighth and seventh parts, respectively, of the second version of the repository images, after that we hide the fourth and fifth parts of the secret image in the eighth and seventh parts of the third version of the repository image, then finally we put the last two bits of the secret image in the eighth and seventh parts of the fourth version of the image. After that, we retrieve the color values of the images formed from the binary system to the decimal system so that we have four new warehouse images, but the secret image that did not show any features in the images roduced in order to strengthen the masking process, we encrypt those formed images using one of the mathematical analyzes within the field of analysis Numerical, which is the analysis of LU factors, which analyzes the image or divides it into two images, and we will see this through the working methodology.

Keywords: Cryptography, Steganography, LU factorization, Digital images
2020 MSC: 94A60, 94A62, 68U05

1 Introduction

In the field of information security, maintaining the confidentiality of information is very important. There are two different methods used in this field, namely data steganography and cryptography, which maintain the integrity and confidentiality of message information between one party and another, The purpose of steganography is to hide the fact that there is a secret message in digital media through different methods so that it does not allow anyone to discover such secret messages. Safely communicating with secret messages through the use of images is the main purpose of steganography [13].

The science of data hiding is done in such a way that the secret message is hidden inside the digital media so that no one can see it. Therefore, this science does not change the structural structure of the secret message,

[*] Corresponding author
Email addresses: mohammeda.alkufi@uokufa.edu.iq (Mohammed Abdul Hameed Jassim Al-Kufi), hussainabbasshanear@gmail.com (Hussein Abbas Shniar Al-Salihi)

Received: December 2021 *Accepted:* February 2022

unlike cryptography, which changes the structure of the secret message, but it protects the encryption of confidential information from unauthorized individuals so that this information appears in an unauthorized manner. Its concept uses cryptography science of mathematics, and therefore this science is considered a mathematical study that has links to aspects of information security such as the credibility of entities, data integrity and credibility [11].

Images are one of the most important digital media used in the field of information steganography and cryptography. Digital images of various types, especially colored ones, are one of the most widely used digital data at the present time. This is due to many reasons, including the ease of circulating these images through various digital devices, in addition to the fact that the size of digital images is very large, and this provides huge amounts of data that require many applications that deal with digital images, because they can perform the process of hiding data or encrypting data for reasons including, those images may carry private and important information, or those images may be confidential, or they may contain embedded information, so they need to be protected and no party is allowed to read or view them [1].

In 1938, the LU analysis was introduced by the Polish mathematician Tadeusz Banachiewicz, and it is one of the important analyzes in linear algebra and numerical analysis. The product sometimes includes a substitution matrix. The LU decomposition can be viewed as a matrix form of Gaussian elimination. Since computers solve square systems of linear equations using LU analysis, it is a key step in calculating the determinant of the matrix, or calculating the inverse of the matrix [24].

LU Analysis was applied to an image. In this decomposition method, the image is decomposed into two images L and U, where L represents the lower elements and U the upper elements of the given image. The original image is obtained by multiplying$L \ * \ U$, and from it a relatively small difference is obtained due to the rounding values. Data compression technology typically provides a compression ratio of 2 to 10 in dual-band or gray-level images. The compression ratio of different images is calculated. Using LU decomposition, where the achieved compression ratio is less than20. The lower compression ratio is taken advantage of as the noise is determined in the data and also the size of the original decomposed image.[18]

2 Literature review

Through [23] a combination of steganography and encryption techniques is proposed, where the encryption algorithm (AES) is combined with the steganography algorithm (LSB). To embed confidential data in an image file, LSB technology was used, while the AES algorithm was used to encrypt the generated stegoimage, the study suggested this technology as an ideal way to transfer confidential information with a better security level.

A comparative study between cryptography and steganography was conducted by Al-Mohammadi et al [3]. They survey ways to combine cryptography and steganography techniques into one. Next, they provided a classification of these methods and compared them in terms of the algorithms used for encryption, the steganography used, the file used as the cover type. As a result, they concluded that encryption methods were more popular than steganography as they offered better security with less exposure to encrypted data. The only advantage of the methods starting with information steganography was to provide a high capacity for storing confidential information.

Hoffman's encryption method to hide data was presented by (names), which is a modern method [17]. Where, the cover image was a grayscale image of size m x n while the secret image was of size p x q. Here, Huffman coding is implemented on the secret image The LSB algorithm is used to embed every part of the Huffman code for the secret image in the cover content. (Names) [17] is proposed a new steganography that relies on encryption, secret key and image switching to achieve gray-level modulation of true color images. Whereas, many encryption algorithms are used for the first time to encrypt both the secret key and the confidential information before it is included in the cover image. In addition, the input image was changed before the embedding process occurred. This proposed method provides five levels of security through image swapping, bit shuffling and bit-XOR ring, gray-level modulation, stego key-based encryption, and . This makes data recovery a difficult task for attackers.

3 Cryptography

Cryptography means secret writing by encrypting explicit messages and decrypting encrypted messages. When there is communication between two parties through an insecure medium, the message can easily fall. Therefore, one of the situations in which it is recommended that this message be secret is cryptography. Encryption is described by Coleman as a set of methods and techniques that include frameworks for encryption and other frameworks for decryption. Checking and integration functions and digital signature frameworks work where encryption frameworks are used to change the structure of a secret message and convert it to another format in an unreadable format for an unauthorized person while using frameworks Decryption restores the secret message to its natural form, which is readable by the authorized person exclusively.[7] .The first principles of encryption engineering were developed by Kirkhoff in 1883[9], where this principle states the possibility that the public can know the technique in which the encryption is applied, but the decryption process needs the public to know the key that was used to perform the encryption in the process of performing the encryption and the process of reversing the encryption (decryption) requires that matter Having keys and without that key it is not possible to decrypt an encrypted message even if the algorithm that was worked on is known , Modern cryptographic frameworks are classified into a group of algorithms, including symmetric ciphers and asymmetric ciphers. The image is encrypted by subjecting the matrix of color values of the image pixels to scattering and scattering operations that are subject to a complex, calculated, studied and recommended mathematical system through the officially approved international standards of accuracy to change the parameters of the image depending on an encryption key of a certain type of types known to specialists

3.1 Steganography

Steganography is the method that refers to hiding the secret message in the content of a cover in a way that completely conceals its presence [16, 10, 8] so that this secret message is either plain text or encrypted or an image sometimes can be considered any as a bit is a secret message Parameters of the data steganography process are determined by the steo key which is a key Secret Before a secret message is discovered or extracted, that key must be known. The object containing the secret message is referred to as a stego object. The sender must first convert the secret message and then process some parts of the envelope object to produce a new object called a stego object and then send that object to the receiving party via a communication medium and when the file which is a stego object is received by the receiving party, the process is performed in reverse in order to extract the information secrecy.[15] Images are one of the preferred media for hiding information, because they contain a lot of redundant bits, so they have a high capacity to receive data and also have a low impact on visibility [2]. the following formula provides generic description of the pieces of the Steganography process

cover image + hidden information = stego image.

3.2 Evaluating the steganography techniques metrics

A number of measures are used to measure and evaluate the efficiency of the previous methods and the proposed methods used in the methods and techniques of steganography, some of these metrics are [4].

(1) Mean Square Error (MSE) [4]
The scale used to measure the distortion that occurs in the cover image after performing a process of masking the data inside this cover, and its equation is

$$MSE = \frac{1}{R \times C} \sum_{a=1}^{R} \sum_{b=1}^{C} (\text{o image}\,(a,b) - s\ image(a,b))^2 \tag{3.1}$$

Where C represents the number of columns of the image and R represents the number of rows, S image is the cover image after hiding the secret data within it, and O image is the original image before hiding the information in it.

(2) Peak Signal to Noise Ratio (PSNR) [4].
The metric that is used to measure the quality between the stego-cover and the original cover after data is hidden in the masking process, where Equation (3.2) is used to calculate PSNR

$$PSNR = 10 \times \log_{10}(\frac{R^2}{\text{MSE}} \tag{3.2}$$

Where R is the maximum value of the byte, or pixel, for 8-bit it is 255

(3) The signal-to-noise ratio (SNR)
It is the measure that is used to know and quantify how much a signal is distorted by noise, as it shows the least interference in the background noise, and is called the SNR. Equation (3) is used to calculate the SNR scale [4]

$$SNR = 10 \times \log_{10} \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} (\text{o image}\,(a,b)^2)}{\sum_{a=1}^{m} \sum_{b=1}^{n} (\text{o image}\,(a,b) - s\ image(a,b))^2} \tag{3.3}$$

(4) Entropy
A statistical measure of how much randomness appears in the cover. It is calculated using equation (3.4) [4].

$$Entropy = -\sum_{i=1}^{n} p_i \log \quad p_i \tag{3.4}$$

(5) Normalized cross correlation (NCC)
This scale is used to measure the degree of similarity or difference between the original cover and the Stigo cover, and equation (3.5) is used to calculate this measure [4].

$$NCC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} \text{o image}\,(a,b)\ \ \text{s image}\,(a,b)}{\sum_{i=1}^{m}\sum_{j=1}^{n} (\text{o image}\,(a,b)^2)} \tag{3.5}$$

Where O image is the Original cover and S image is the stego cover.

(6) Correlation (CORR)

$$COR = \frac{\sum_a \sum_b (o\ image\,(a,b) - \overline{\text{o image}\,(a,b))}(s\ image\,(a,b) - \overline{\text{s image}\,(a,b))}}{\sqrt{\sum_a \sum_b (o\ image\,(a,b) - \overline{\text{o image}\,(a,b))}^2 \sum_a \sum_b (s\ image\,(a,b) - \overline{\text{s image}\,(a,b))}^2}} \tag{3.6}$$

where $\overline{\text{o image}\,(a,b))}$ is the original image data average, $\overline{\text{s image}\,(a,b)}$ is the average of image data after hiding process [21].

3.3 LU factorization without pivot [12]

It said $\mathrm{A_{nn}}$ is matrix to have LU decomposition if there exists matrices L and U with the following properties:

(i) $L_{n\times n}$ is lower triangular matrix.
(ii) $U_{n\times n}$ is upper triangular matrix.
(ii) $A = L.U$

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} l_{11} & 0 & 0 & \dots & 0 \\ l_{21} & l_{22} & 0 & \dots & 0 \\ l_{31} & l_{32} & l_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \dots & l_{nn} \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & u_{13} & \dots & u_{1n} \\ 0 & u_{22} & u_{23} & \dots & u_{2n} \\ 0 & 0 & u_{33} & \dots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & u_{nn} \end{bmatrix}$$

To find L and U completely, such conditions are discussed below. [22] [5]

1- when $u_{ii} = 1,\ for\ i = 1, 2, \dots, n$, then the method is known as Crout's decom- position method.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix} = \begin{bmatrix} l_{11} & 0 & 0 & \dots & 0 \\ l_{21} & l_{22} & 0 & \dots & 0 \\ l_{31} & l_{32} & l_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \dots & l_{nn} \end{bmatrix} . \begin{bmatrix} 1 & u_{12} & u_{13} & \dots & u_{1n} \\ 0 & 1 & u_{23} & \dots & u_{2n} \\ 0 & 0 & 1 & \dots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

$$= \begin{bmatrix} l_{11} & l_{11}\ u_{12} & l_{11}\ u_{13} & \dots & l_{11}\ u_{1n} \\ l_{21} & l_{21}\ u_{12} + l_{22} & l_{21}\ u_{13} + l_{22}\ u_{23} & \dots & l_{21}\ u_{1n} + l_{22}\ u_{2n} \\ l_{31} & l_{21}\ u_{12} + l_{32} & l_{31}\ u_{13} + l_{32}\ u_{23} & \dots & l_{31}\ u_{1n} + l_{32}\ u_{2n} + l_{33}\ u_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n1}\ u_{12} + l_{n2} & l_{n1}\ u_{13} + l_{n2}\ u_{23} + l_{n3} & \dots & l_{n1}\ u_{1n} + l_{n2}\ u_{2n} + \dots + l_{nn} \end{bmatrix}$$

From first row and first column, we have:
$l_{i1} = a_{i1}\quad , for\ i = 1, 2, \dots, n$ and $u_{1j} = \frac{a_{1j}}{l_{11}}\quad , for\ j = 1, 2, \dots, n$
Similarly, from second column and second row we get the following equations

$$l_{i2} = a_{i2} - l_{i1}u_{12} \quad , for\ i = 2, 3, \dots, n$$

$$u_{2j} = \frac{a_{2j} - l_{i1}u_{1j}}{l_{22}} \quad , forj2, 3 \dots, n.$$

Solving these equations we obtained the second column of L and second row of U. In general, the elements of the matrix L, i.e. l_{ij} and the elements of U, i.e. u_{ij} are determined from the following equations.

$$l_{ij} = a_{ij} - \sum_{k=1}^{j-1} l_{ik}u_{kj} \quad , for\ i \geq j$$

$$u_{ij} = \frac{a_{ij} - \sum_{k=1}^{i-1} l_{ik}u_{kj}}{l_{ii}} \quad , for\ i < j$$

$$u_{ii} = 1, \qquad l_{ij} = 0, \quad j > i\ and \qquad u_{ij} = 0, \quad i > j.$$

2-when $l_{ii} =\ 1,\ for\ i = 1, 2, \ldots, n$ then the method is known as Doolittle's method for decomposition. In particular, [6]

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_{nn} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ l_{21} & 1 & 0 & \ldots & 0 \\ l_{31} & l_{32} & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \ldots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & u_{13} & \ldots & u_{1n} \\ 0 & u_{22} & u_{23} & \ldots & u_{2n} \\ 0 & 0 & u_{33} & \ldots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & u_{nn} \end{bmatrix}$$

Multiply the matrix L by the matrix U, we will get

$$u_{1j} = a_{1j}\ ,\ j = 1, 2, \ldots, n\ and$$

$$l_{j1} = \frac{a_{j1}}{u_{11}}\ , j = 1, 2, \ldots, n$$

$$u_{ij} = a_{ij} - \sum_{k=1}^{i-1} l_{ik}u_{kj}, \quad for\ j = i+1, \ldots, n$$

$$l_{ij} = \frac{a_{ji} - \sum_{k=1}^{i-1} l_{ik}u_{kj}}{u_{jj}}\ , \quad for\ j = i+1, \ldots, n$$

$$u_{ii} = a_{ii} - \sum_{k=1}^{i-1} l_{ik}u_{\mathrm{ik}}\ , for\ i = 2, 3, \ldots, n-1$$

3.4 LU factorization with pivoting

Pivoting is the method used to mitigate the problem of LU decomposition failure, where LU decomposition fails when the upper left entry of matrix A is compared to other entries in the matrix as zero or too small. Pivoting is used by rearranging the rows or columns of matrix so that the largest element is placed in the top- left position [20]. There are many pivot methods such as

3.4.1 Partial Pivoting *LU* factorization with partial pivoting [14]

The goal of partial pivoting is to use a permutation matrix to place the largest entry of the first column of the matrix at the top of that first column. The general factorization of a matrix A to a lower triangular matrix L and an upper triangular matrix **U** using partial pivoting is represented by the following:

$$PA = LU$$

$$P = P_k\ \ P_{k-1}\ \ldots P_2P_1$$

3.4.2 full pivoting or (Complete Pivoting) [14]

In this type of pivot the A is multiplied from the left in the permutation matrix P. Then the A on the right is multiplied by a second commutative matrix Q to switch between columns, the matrix product PAQ switching the rows and columns so that the largest entry in the matrix is at (a_{11}) position A is represented. Using full pivoting as follows:

$$PAQ = LU$$

$$P = P_k\ \ P_{k-1}\ \ \ldots\ P_2P_1$$

$$Q = Q_1\ Q_2\ \ldots\ Q_{k-1}\ Q_k$$

4 Methodology of Proposed Algorithm.

The modern way to hide and encrypt text, some researchers has used the method of masking (text) inside an image [19]. For the purpose of increasing the complexity, we send more than one image for the purpose of complicating the matter to intruders, and this is what we will do in this paper.

The first stage: Stage of steganography is carried out through the following steps

In this method, we hide the secret image in the cover image by making the size of the cover image equal to the size of the secret image, then converting both images from the decimal number system to the binary number system, and then making four copies. Cover image and eight-bit binary secret image masking process in the last part of the four versions of binary cover images to illustrate this Let's suppose the secret image to be hidden $A_{m,n}$ And let's suppose the cover image $B_{m,n}$.

$$A_{m,n} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix}, \quad B_{m,n} = \begin{bmatrix} b_{11} & b_{12} & b_{13} & \dots & b_{1n} \\ b_{21} & b_{22} & b_{23} & \dots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{m1} & b_{m2} & b_{m3} & \dots & b_{mn} \end{bmatrix}$$

Step1: First, let the image size $A_{m,n}$be the same as the image size $B_{m,n}$
Step2: we are converting the color values of both images from decimal to binary. It will look like this

$$A = \left[\begin{array}{cccccccc} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \\ \left|\begin{matrix} r_{11} \\ r_{21} \\ r_{31} \\ \vdots \\ r_{m1} \end{matrix}\right| & \left|\begin{matrix} r_{12} \\ r_{22} \\ r_{32} \\ \vdots \\ r_{m2} \end{matrix}\right| & \left|\begin{matrix} r_{13} \\ r_{23} \\ r_{33} \\ \vdots \\ r_{m3} \end{matrix}\right| & \left|\begin{matrix} r_{14} \\ r_{24} \\ r_{34} \\ \vdots \\ r_{m4} \end{matrix}\right| & \left|\begin{matrix} r_{15} \\ r_{25} \\ r_{35} \\ \vdots \\ r_{m5} \end{matrix}\right| & \left|\begin{matrix} r_{16} \\ r_{26} \\ r_{36} \\ \vdots \\ r_{m6} \end{matrix}\right| & \left|\begin{matrix} r_{17} \\ r_{27} \\ r_{37} \\ \vdots \\ r_{m7} \end{matrix}\right| & \left|\begin{matrix} r_{18} \\ r_{28} \\ r_{38} \\ \vdots \\ r_{m8} \end{matrix}\right| \end{array}\right]$$

Such that $r_{11}, r_{12}, \dots,\ r_{m8} = 0\ or\ 1$

$$B = \left[\begin{array}{cccccccc} k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & k_7 & k_8 \\ \left|\begin{matrix} t_{11} \\ t_{21} \\ t_{31} \\ \vdots \\ t_{m1} \end{matrix}\right| & \left|\begin{matrix} t_{12} \\ t_{22} \\ t_{32} \\ \vdots \\ t_{m2} \end{matrix}\right| & \left|\begin{matrix} t_{13} \\ t_{23} \\ t_{33} \\ \vdots \\ t_{m3} \end{matrix}\right| & \left|\begin{matrix} t_{14} \\ t_{24} \\ t_{34} \\ \vdots \\ t_{m4} \end{matrix}\right| & \left|\begin{matrix} t_{15} \\ t_{25} \\ t_{35} \\ \vdots \\ t_{m5} \end{matrix}\right| & \left|\begin{matrix} r_{16} \\ t_{26} \\ t_{36} \\ \vdots \\ t_{m6} \end{matrix}\right| & \left|\begin{matrix} t_{17} \\ t_{27} \\ t_{37} \\ \vdots \\ t_{m7} \end{matrix}\right| & \left|\begin{matrix} t_{18} \\ t_{28} \\ t_{38} \\ \vdots \\ t_{m8} \end{matrix}\right| \end{array}\right]$$

Such that $t_{11}\ , t_{12}, \dots, t_{m8} = 0\ or\ 1$

Step3: In this step, we copy the cover images into four copies that we call(B_1, B_2, B_3, B_4)

Step4: *We place the first and second columns of matrix A in the eighth and seventh, respectively, of the first* copy *(B_1) of the* cover *images* B, *$(c_1 \rightarrow k_8\ ,\ c_2 \rightarrow k_7)$*

$$B_1 = \left[\begin{array}{cccccccc} k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & c_2 & c_1 \\ \left|\begin{matrix} t_{11} \\ t_{21} \\ t_{31} \\ \vdots \\ t_{m1} \end{matrix}\right| & \left|\begin{matrix} t_{12} \\ t_{22} \\ t_{32} \\ \vdots \\ t_{m2} \end{matrix}\right| & \left|\begin{matrix} t_{13} \\ t_{23} \\ t_{33} \\ \vdots \\ t_{m3} \end{matrix}\right| & \left|\begin{matrix} t_{14} \\ t_{24} \\ t_{34} \\ \vdots \\ t_{m4} \end{matrix}\right| & \left|\begin{matrix} t_{15} \\ t_{25} \\ t_{35} \\ \vdots \\ t_{m5} \end{matrix}\right| & \left|\begin{matrix} t_{16} \\ t_{26} \\ t_{36} \\ \vdots \\ t_{m6} \end{matrix}\right| & \left|\begin{matrix} r_{12} \\ r_{22} \\ r_{32} \\ \vdots \\ r_{m2} \end{matrix}\right| & \left|\begin{matrix} r_{11} \\ r_{21} \\ r_{31} \\ \vdots \\ r_{m1} \end{matrix}\right| \end{array}\right]$$

Step5: We will place the third and fourth columns of image A in the eighth and seventh columns, respectively, in the second copy (B_2) of the cover images. $(c_3 \to k_8\ ,\ c_4 \to k_7)$

$$B_2 = \begin{array}{cccccccc} k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & c_4 & c_3 \\ \left|\begin{matrix} t_{11}\\ t_{21}\\ t_{31}\\ \vdots\\ t_{m1}\end{matrix}\right| & \left|\begin{matrix} t_{12}\\ t_{22}\\ t_{32}\\ \vdots\\ t_{m2}\end{matrix}\right| & \left|\begin{matrix} t_{13}\\ t_{23}\\ t_{33}\\ \vdots\\ t_{m3}\end{matrix}\right| & \left|\begin{matrix} t_{14}\\ t_{24}\\ t_{34}\\ \vdots\\ t_{m4}\end{matrix}\right| & \left|\begin{matrix} t_{15}\\ t_{25}\\ t_{35}\\ \vdots\\ t_{m5}\end{matrix}\right| & \left|\begin{matrix} t_{16}\\ t_{26}\\ t_{36}\\ \vdots\\ t_{m6}\end{matrix}\right| & \left|\begin{matrix} r_{14}\\ r_{24}\\ r_{34}\\ \vdots\\ r_{m4}\end{matrix}\right| & \left|\begin{matrix} r_{13}\\ r_{23}\\ r_{33}\\ \vdots\\ r_{m3}\end{matrix}\right| \end{array}$$

Step6: We will then place the fifth and sixth columns of image A instead of the eighth and seventh columns, respectively, of the third (B_3) of the cover images. $(c_5 \to k_8\ ,\ c_6 \to k_7)$

$$B_3 = \begin{array}{cccccccc} k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & c_6 & c_5 \\ \left|\begin{matrix} t_{11}\\ t_{21}\\ t_{31}\\ \vdots\\ t_{m1}\end{matrix}\right| & \left|\begin{matrix} t_{12}\\ t_{22}\\ t_{32}\\ \vdots\\ t_{m2}\end{matrix}\right| & \left|\begin{matrix} t_{13}\\ t_{23}\\ t_{33}\\ \vdots\\ t_{m3}\end{matrix}\right| & \left|\begin{matrix} t_{14}\\ t_{24}\\ t_{34}\\ \vdots\\ t_{m4}\end{matrix}\right| & \left|\begin{matrix} t_{15}\\ t_{25}\\ t_{35}\\ \vdots\\ t_{m5}\end{matrix}\right| & \left|\begin{matrix} t_{16}\\ t_{26}\\ t_{36}\\ \vdots\\ t_{m6}\end{matrix}\right| & \left|\begin{matrix} r_{16}\\ r_{26}\\ r_{36}\\ \vdots\\ r_{m6}\end{matrix}\right| & \left|\begin{matrix} r_{15}\\ r_{25}\\ r_{35}\\ \vdots\\ r_{m5}\end{matrix}\right| \end{array}$$

Step7: We will place the seventh and eighth columns of image A in the eighth and seventh columns, respectively, in the second copy (B_4) of the cover images. $(c_7 \to k_8\ ,\ c_8 \to k_7)$

$$B_4 = \begin{array}{cccccccc} k_1 & k_2 & k_3 & k_4 & k_5 & k_6 & c_8 & c_7 \\ \left|\begin{matrix} t_{11}\\ t_{21}\\ t_{31}\\ \vdots\\ t_{m1}\end{matrix}\right| & \left|\begin{matrix} t_{12}\\ t_{22}\\ t_{32}\\ \vdots\\ t_{m2}\end{matrix}\right| & \left|\begin{matrix} t_{13}\\ t_{23}\\ t_{33}\\ \vdots\\ t_{m3}\end{matrix}\right| & \left|\begin{matrix} t_{14}\\ t_{24}\\ t_{34}\\ \vdots\\ t_{m4}\end{matrix}\right| & \left|\begin{matrix} t_{15}\\ t_{25}\\ t_{35}\\ \vdots\\ t_{m5}\end{matrix}\right| & \left|\begin{matrix} t_{16}\\ t_{26}\\ t_{36}\\ \vdots\\ t_{m6}\end{matrix}\right| & \left|\begin{matrix} r_{18}\\ r_{28}\\ r_{38}\\ \vdots\\ r_{m8}\end{matrix}\right| & \left|\begin{matrix} r_{17}\\ r_{27}\\ r_{37}\\ \vdots\\ r_{m7}\end{matrix}\right| \end{array}$$

Step8: we return the color values of the fourth copies of the cover images $(B_1, B_2, B_3, B_4,)$ in which the color values of the secret image A were hidden from the binary number system to the decimal number system. We will get the cover image B, which does not have any hints to the secret image.

$$B_1 = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n}\\ b_{21} & b_{22} & \dots & b_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ b_{m1} & b_{m2} & \dots & b_{mn}\end{bmatrix}, B_2 = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n}\\ b_{21} & b_{22} & \dots & b_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ b_{m1} & b_{m2} & \dots & b_{mn}\end{bmatrix}, B_3 = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n}\\ b_{21} & b_{22} & \dots & b_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ b_{m1} & b_{m2} & \dots & b_{mn}\end{bmatrix}, B_4 = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n}\\ b_{21} & b_{22} & \dots & b_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ b_{m1} & b_{m2} & \dots & b_{mn}\end{bmatrix}$$

The second stage: the stage of encryption the resulting images after the steganography

At this stage, the images formed after the masking process are encrypted and go through the following:

Step 1: Four encryption keys are chosen with the number of copies formed for the images after the hiding process, and these keys are in the form of images (k_1, k_2, k_3, k_4)

Step 2: The four images generated after the hiding process (B_1, B_2, B_3, B_4) are analyzed using an analysis (LUP)The analysis will be taken for the image (B_1) , which is applied to the rest of the three images

$$B_1 = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n}\\ b_{21} & b_{22} & \dots & b_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ b_{m1} & b_{m2} & \dots & b_{mn}\end{bmatrix}, \quad Let\ P_s = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n}\\ c_{21} & c_{22} & \dots & c_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ c_{m1} & c_{m2} & \dots & c_{mn}\end{bmatrix}$$

Since (P_s) is permutation matrix, the elements of each row of these matrix are from the number zero, except for one element that is from the number one.

$[L_{B_1}, U_{B_1}, P_{B_1}]$= LU$(B_1)$

$P_{B_1}B_1{=}L_{B_1}U_{B_1}$

$$\begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ l_{21} & 1 & 0 & \dots & 0 \\ l_{31} & l_{32} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \dots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & u_{13} & \dots & u_{1n} \\ 0 & u_{22} & u_{23} & \dots & u_{2n} \\ 0 & 0 & u_{33} & \dots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & u_{nn} \end{bmatrix}$$

$B_1 = P^T_{B_1} L_{B_1} U_{B_1}$

$$\begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \dots & c_{mn} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ l_{21} & 1 & 0 & \dots & 0 \\ l_{31} & l_{32} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \dots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & u_{13} & \dots & u_{1n} \\ 0 & u_{22} & u_{23} & \dots & u_{2n} \\ 0 & 0 & u_{33} & \dots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & u_{nn} \end{bmatrix}$$

Step 3: The keys(k_1, k_2, k_3, k_4) chosen to perform the encryption process are analyzed using an analysis (LUP) the analysis will be taken for the key image (k_1), which is applied to the rest of the seven key, Let

$$k_1 = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mn} \end{bmatrix}, \quad P_k = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mn} \end{bmatrix}$$

Since (P_k) is permutation matrix, the elements of each row of these matrix are from the number zero, except for one element that is from the number one.

$[L_{k_1}, U_{k_1}, P_{k_1}]$= LU($k_1$)

$P_{k_1}k_1{=}L_{k_1}U_{k_1}$

$$\begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mn} \end{bmatrix} \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mn} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ l_{21} & 1 & 0 & \dots & 0 \\ l_{31} & l_{32} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & l_{n3} & \dots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & u_{13} & \dots & u_{1n} \\ 0 & u_{22} & u_{23} & \dots & u_{2n} \\ 0 & 0 & u_{33} & \dots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & u_{nn} \end{bmatrix}$$

Step 4: We replace the matrices resulting from the analyzes and take the transition of some matrices to form a confused and incomprehensible model

$$\begin{array}{ll} [L_{B_1}, U_{B_1}, P_{B_1}] = LU(B_1) & \qquad [L_{K_1}, U_{K_1}, P_{K_1}] = LU(k_1) \\ P_{B_1}.B_1 = L_{B_1}.U_{B_1} & \qquad P_k.k_1 = L_k.U_k \\ B_1 = P^T_{B_1}.L_{B_1}.U_{B_1} & \qquad k_1 = P^T_{k_1}.L_{k_1}.U_{k_1} \end{array}$$

The image is before the encryption process

$[B_1][k_1] = [\, P^T_{B_1}.L_{B_1}.U_{B_1} \,][\, P^T_{k_1}.L_{k_1}.U_{k_1} \,]$

Some of the matrices resulting from the analysis of an image $(B_1\ \ )$ are replaced by the place of some of the matrices resulting from the analysis of the image of the key (k_1), $(U_{B_1}\ \ \leftrightarrow U_{k_1})$ after which a confused and incomprehensible shape is obtained, a mixture of colors

$C_1 = [\, P^T_{B_1}.L_{B_1}.U_{k_1} \,][\, P^T_{k_1}.L_{k_1}.U_{B_1} \,]$

To strengthen the encryption, another encryption key is used, which is a real number (r), where the image resulting from the encryption is multiplied in this key

$C_1 = ([\, P^T_{B_1}.L_{B_1}.U_{k_1} \,][\, P^T_{k_1}.L_{k_1}.U_{B_1} \,]).\ \mathrm{r}$

$C_1 = [\, P^T_{B_1}.L_{B_1}.U_{k_1} \,].\ \mathrm{r}\ [\, P^T_{k_1}.L_{k_1}.U_{B_1} \,].\ \mathrm{r}$

$C_1 = [D_1][D_2]$

$$\left[\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix} . \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ l_{31} & l_{32} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & \cdots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \cdots & u_{2n} \\ 0 & 0 & \cdots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & u_{nn} \end{bmatrix} \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix} . \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 0 & \cdots & 0 \\ l_{31} & l_{32} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & \cdots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \cdots & u_{2n} \\ 0 & 0 & \cdots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & u_{nn} \end{bmatrix}\right].r$$

$$\left[\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix} . \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ l_{31} & l_{32} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & \cdots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \cdots & u_{2n} \\ 0 & 0 & \cdots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & u_{nn} \end{bmatrix} .r \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix} . \begin{bmatrix} 1 & 0 & \cdots & 0 \\ l_{21} & 1 & \cdots & 0 \\ l_{31} & l_{32} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ l_{n1} & l_{n2} & \cdots & 1 \end{bmatrix} . \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ 0 & u_{22} & \cdots & u_{2n} \\ 0 & 0 & \cdots & u_{3n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & u_{nn} \end{bmatrix} .r\right]$$

Other images are dealt with in the same way as the above encryption, and in the end, encrypted images are obtained in the following form

Table 1: Sources of variance for a two-factor experiment

The image is before the encryption	The image is after theencryption
$[B_2][k_2] = [P_{B_2}^T.L_{B_2}.U_{B_2}][P_{k_2}^T.L_{k_2}.U_{k_2}]$	$C_2 = [P_{B_2}^T.L_{B_2}.U_{k_2}].r\ [P_{k_2}^T.L_{k_2}.U_{B_2}].r$
$[B_3][k_3] = [P_{B_3}^T.L_{B_3}.U_{B_3}][P_{k_3}^T.L_{k_3}.U_{k_3}]$	$C_3 = [P_{B_3}^T.L_{B_3}.U_{k_3}].r\ [P_{k_3}^T.L_{k_3}.U_{B_3}].r$
$[B_4][k_4] = [P_{B_4}^T.L_{B_4}.U_{B_4}][P_{k_4}^T.L_{k_4}.U_{k_4}]$	$C_4 = [P_{B_4}^T.L_{B_4}.U_{k_4}].r\ [P_{k_4}^T.L_{k_4}.U_{B_4}].r$

5 Results and readings

Lena's photo will be used as a secret photo to hide it in four copies of the car photo as cover photos for the algorithm application. These images will be tested by a program prepared for that in the MATLAB program, and the results are as shown in the following figures:

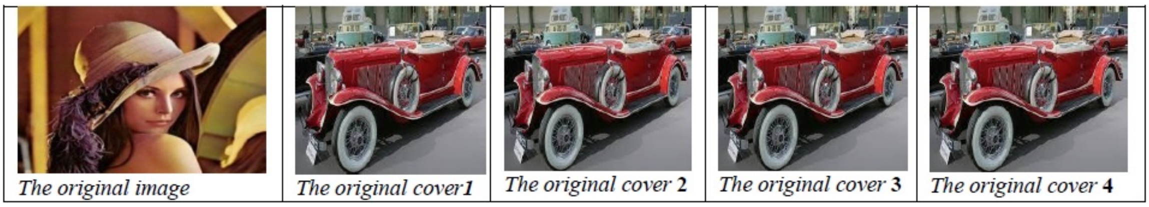


Figure 1: The secret image with the cover image that is reproduced in four copies

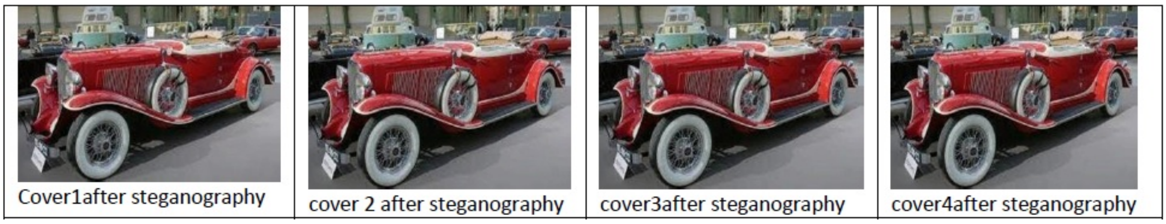

Cover1after steganography
cover 2 after steganography
cover3after steganography
cover4after steganography

Figure 2: Copying the cover image after hiding the secret image inside it

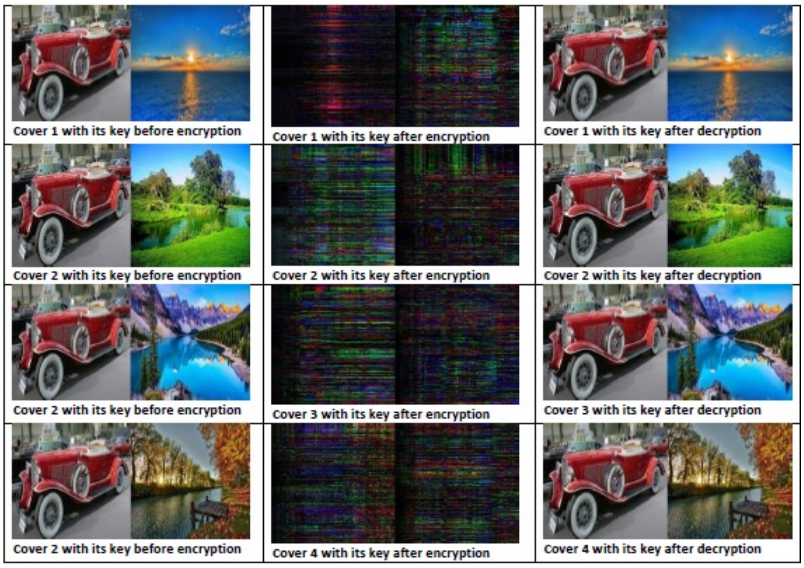
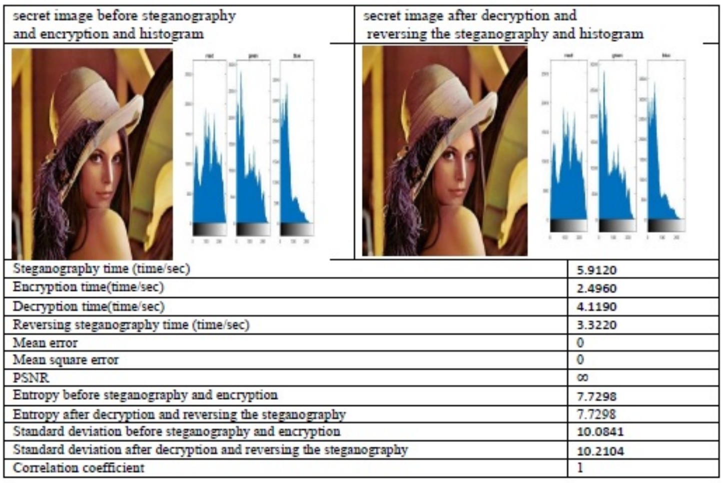

Cover 1 with its key before encryption
Cover 1 with its key after encryption
Cover 1 with its key after decryption
Cover 2 with its key before encryption
Cover 2 with its key after encryption
Cover 2 with its key after decryption
Cover 2 with its key before encryption
Cover 3 with its key after encryption
Cover 3 with its key after decryption
Cover 2 with its key before encryption
Cover 4 with its key after encryption
Cover 4 with its key after decryption

Figure 3: Copies of the four cover images in which the secret image was hidden with the images of the encryption key before the encryption process and after the encryption process and after decryption



secret image before steganography and encryption and histogram	secret image after decryption and reversing the steganography and histogram
Steganography time (time/sec)	5.9120
Encryption time(time/sec)	2.4960
Decryption time(time/sec)	4.1190
Reversing steganography time (time/sec)	3.3220
Mean error	0
Mean square error	0
PSNR	∞
Entropy before steganography and encryption	7.7298
Entropy after decryption and reversing the steganography	7.7298
Standard deviation before steganography and encryption	10.0841
Standard deviation after decryption and reversing the steganography	10.2104
Correlation coefficient	1

Table 2: The results and readings of the application of Lena image using the second algorithm

6 Conclusions

We deduce the accuracy of the proposed algorithm, where the results were high-resolution, after the masking process that was done for the image in another cover image, as well as after the encoding process that was done to copy the cover images using LU-analysis with partial pivoting, if the image recovered after this complex process of Masking and coding are exactly the same as before coding, if the mean error and mean square error between the two images are zero, and also the correlation coefficient at the highest value is 1, the PSNR values are too high to be expressed∞.

References

[1] M. Alasdair, *An introduction to digital image processing with Matlab*, Course Technology, 2004.

[2] 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.

[3] S. Almuhammadi and A. Al-Shaaby, *A survey on recent approaches combining cryptography and steganography Computer Science*, Information Technology (CS IT), 2017.

[4] 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.

[5] P. Anita, *Numerical analysis*, National Institute of Technology Durgapur, Durgapur-713209.

[6] S. Adjerid, *Notes for numerical analysis*, Math 4445, Virginia Polytechnic Institute and State University.

[7] T.S. Barhoom and S.M. AMousa, *A steganography lsb technique for hiding image within image using blowfish encryption algorithm*, Int. J. Res. Eng. Sci. **3** (2015), 61–66.

[8] M. Douglas, K. Bailey, M. Leeney and K. Curran, *An overview of steganography techniques applied to the protection of biometric data*, Multi.Tools Appl. **77** (2018), 17333–17373.

[9] D. Gollmann, *Computer security Wiley interdisciplinary reviews*, Comput. Statist. **2** (2010), 544–554.

[10] M.M. Hashim, M.S.M. Rahim, F.A. Johi, M.S. Taha, A.A. Al-Wan and N.N. Sjarif, *An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching*, Int. J. Engin. Technol. **7** (2018), 4008–4023.

[11] J. Katz, A.J. Menezes, P.C. Van Oorschot and S.A. Vanstone, *Handbook of applied cryptography*, CRC press. 1996.

[12] I.A. Khalil and M.S. Meaad, *Contourlet transformation for text hiding in hsv color image*, Int. J. Comput. Networks Commun. Secur. 1 (2013), no. 4.

[13] S.A. Laskar and K. Hemachandran, *Combining JPEG steganography and substitution encryption for secure data communication*, Computer Science & Information Technology, 2012.

[14] W.R. Matthew, *Pivoting for LU factorization*, University of Puget Sound, 2014.

[15] S. Mishra, V.K. Yadav, M.C. Trivedi and T. Shrimali, *Audio steganography techniques*, A Survey in Advances in Computer and Computational Sciences, Springer, Singapore, 2018, p. 581–589.

[16] T. Morkel, *Image steganography applications for secure communication Doctoral dissertation*, University of Pretoria, 2012.

[17] K. Muhammad, J. Ahmad, M. Sajjad and M. Zubair, *Secure image steganography using cryptography and image transposition*, arXiv preprint arXiv:1510.04413. 2015.

[18] 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.

[19] F.A.P. Petitcolas, *Information hiding: a survey*, Proc. IEEE **87** (1999), no. 7, 1062–1078.

[20] G. Phillip, M. Walter and H.W. Margaret, *Numerical linear algebra and optimization*, Addison-Wesley Publishing Company, 1991.

[21] M.H. Qasim, *New Metrics for steganography algorithm quality*, Int. J. Adv. Sci. Technol. **29** (2020), no. 2.

[22] L. Riccardo and B. Mauro, *Lossless compression of encrypted gray-level and color images*, 16th Eur. Signal Process. Conf. (EUSIPCO 2008), Lausanne, Switzerland, **25** (2008), no. 29, p. 1-5.

[23] D.R. Sridevi, P. Vijaya and K.S. Rao, *Image steganography combined with cryptography council for innovative*, Council Innov. Res. Peer Rev. Res. Pub. Syst. J. **9** (2013), no. 1.

[24] A. Schwarzenberg-Czerny, *On matrix factorization and efficient least squares solution*, Astron. Astrophys. Suppl. Ser. **110** (1995), no. 405, 110–405.