Encryption and Steganography: a secret data using circle shapes in colored images

Zeena N. Al-kateeb¹*, Muna Jaffer AL-Shamdeen² and Farah Saad Al-Mukhtar ³

¹,² Computer Sciences Department, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq
³ Computer Science Department, College of Science, Al-Nahrain University, Baghdad/Iraq

*Corresponding author’s e-mail address: zeenaalkateeb@yahoo.com, zeenaalkateeb@uomosul.edu.iq

Abstract: Since the earliest times, people have used the encryption and hiding data to achieve a safe and reliable transfer of important data. This paper proposed a new method for encrypting important data based on the circular shapes information that extracted from the cover image. The encryption process is done using an update of a well known traditional method with simple calculations taking advantage of the coordinates of the center of the main circle as keys extracted from the cover image to reduce the number of keys exchanged between the sender and the recipient and to increase the level of security and confidentiality. The hiding process of the encrypted data is done in pixels that located in the circular areas of the cover image and in three forms of concealment, which providing second encryption, choosing the hiding form depending on the appearing sequence of the character in the text, which makes decode the secure data will be so difficult, the experiments showed that the proposed method was achieved excellent encryption and hiding depending on the coefficients Peak Signal to Noise Ratio analyses (PNSR), Mean Square Error (MSE), and other measurements. The proposed method achieves a complete data recovery ratio where it was Bit Error Rate BER=0.

1. Introduction

In recent years, the Internet has been considered an appropriate method for transmitting digital and multimedia data, where it can be considered a cheap and fast way to transfer multimedia, digital data and other files in different fields like the private sector, government, medical areas, and military[1]. The security weakness of data is the main disadvantage of using the internet, that is because any unauthorized users can be monitored the data, which prompted the use of steganography [2]. Steganography is a method of to protect communication and to reduce attack risking during transportation over communication media. Steganography was introduced with the example of "Prisoner's secret message" by Simmons in 1983. Generally can be used all types of files, like text, image, video, and audio as carriers for the steganography. However, a high redundancy medium is more suitable, so the image and audio files are the ideal format that used for steganography [3].
The classic steganography is interested in including a secret message in the cover medium, to increase security level, the keys are used, that making remove or detect the embedded original data very difficult without knowing the key used in it.

Capability and security are important objectives of steganography, capacity is the amount of data that can be hidden in the cover media. Security is interested in making important data unknown either by an unauthorized computer or a person. The hiding information process in a steganography system starts with identifying a redundant bits in cover's media. By exchanging the data from hidden messages with these redundant bits, the creation of a stage done by the embedding process.

Steganography and cryptography are methods to protect or hide secret data. However, in respect, they are different than steganography hides data exists, but cryptography hides data meaning. These techniques are important, that used for providing security of the network [4]. Many researchers suggested using the chaotic system to increase the reliability of cryptography and steganography [5], [6], [7]. In this paper, a method used to combine steganography and cryptography in one system

2. Related work

In modern times, many researchers have proposed many different systems to encrypt and hide secure data. In [8] Juneja and Sandhu, suggest an amended steganography technique based on (least significant bit) for images that impart the best security of information. It shows an embedding algorithm to hide encrypted messages in random and not neighboring locations of a pixel in the smooth region and edges of images. In the first step the secret message encrypted, then in the cover image the edges detected using amended detection filter. After that, the message's bits will be embedded in LSB of edges area pixels that selected randomly. This ensures that the eavesdroppers do not suspect that the media contains any hidden message and makes steganography techniques ineffective to properly guess the length of the secret message. Balvinder et al. shows a new LSB way for steganography technique, that enhances the existed least significant bit substitution to improve the security of hidden information [9]. An algorithm presented using an effective steganography technique to hide secret data in the images, that used an 8-bit random key for encrypting a secret message, also this key will be used for selected the pixel in the cover image, which encrypted data hide in it. In the first step, XOR operation applied between the secret message and 8-bit random key for encrypting the plain secret message, then, the encrypted message will be hidden in the least significant bit of selected pixels in the cover image. Finally, the 2nd least significant bit of each pixel and the 8-bit random key are used to choosing the pixel which stores the encrypted message by applying some operation. As compared to other techniques this method, hiding a large number of characters in the cover image of the secret message as well as it is more secure. Purnama and Rohayani produce ciphertext by modifying the Caesar cipher method, this is done by replacing the alphabet into two parts, the consonant alphabet was replaced with a consonantal alphabet and the vocals were replaced with the alphabet vocal too[10]. However, because of the frequency of the alphabet is seldom used in an Indonesian text, there are some alphabet consonants are not replaced. A ciphertext that can be read is obtained from the tested result, with this ciphertext, the message does not suspect by the cryptanalyst so, he does not attempt to solve the ciphertext. Singh, et al. suggest a novel method for data-hiding based on the least significant bit technique of digital images, this technique using a lossless data hiding technique [11]. To derive the stego-image, The LSB algorithm is performed in spatial domain in which the payload bits embedded into the LSB of the cover image. tavoli, et al. discus the multiple approaches of steganography in an image, the proposed algorithm capable of storing a large amount of information[12]. A desirable percentage of steganography was yield by combining the LSB approach with mixing the use of the application of a particular scan of an image with an appropriate mask and adding a step of encrypting with each, these steps decrease the odds of discovering the hidden data. Alhassan et al. combined the cryptography and steganography to supply a robust system that can be able to encrypt a secret message using RSA algorithm and the advanced least significant bit method is used to hide the message [13]. In the first step, the original message encrypted and then separated into
P1 and P2 portions, the first portion (P1), XOR operation applied to it using the odd location and to (p2) using the even position of the LSB+1. Then to hide the XORed encrypted message, the Position of the LSB is used. AbdelWahab et al. present a comparison between two different techniques, the first one (LSB) with no compression and no encryption, and the second one, before applying LSB technique, the secret message is encrypted [14]. Furthermore, transform the image into a frequency domain using Discrete Cosine Transform, to develop the stego-image, the least significant bit is performed in the spatial domain where the payload bits are inserted into a cover image in the LSB, while the DCT algorithm is performed in the frequency domain in which transforming the stego-image to the frequency domain and the payload bits are inserted into the cover image.

In 2018, Krishnaveni and Periyasamy suggested a secure system that gives high security and changed high implanting ability image steganography utilizing Least Significant Bit insert alongside chaotic supply map, During this system lossless and invisible amendment within the image steganography [15]. Whereas, Ogras (2019) proposed a spatial domain steganography technique which used the Logistic map for generating chaotic bitstream and bitwise XOR operation which is utilized to create a control bit [16].

3. The proposed algorithm:

The proposed algorithm is based mainly on the circular shapes available in the cover image as one of the geometric shapes to applying its steps fully and correctly. The cover image must contain at least one circular area. The algorithm finds the circular areas using circular hough transform as a first elementary step and assigns the centers of those circles if there is more than one circular area in the cover image we assign one of those circles as the main circle and used its center coordinates for the coding and decoding process. To reduce the keys which must be exchanged between the sender and the recipient, we have suggested that the middle-chain circle should be the main circle (MC), if the number of circles (NC), then MC= round (NC/2) for example, NC=3 then MC= round (3/2), MC=2.

The encoding process is done in two phases. The original text is encoded using the X-axis coordinate of the center of the main circle and X-axis coordinates of the pixel that will contain the hidden data, and then the resulting text is encoded using the Y-coordinate of the center of the main circle and Y-axis coordinate for the pixel that will contain the hidden data as a second phase. Then the encrypted text will be embedded in the cover image. Embedding of encrypted data is based on the Least Significant Bit (LSB) method, but in a manner that ensures a kind of distributed diffusion based on the pixel location. The byte of the secret encrypted message is hidden in one pixel only, embed three bits from the secret encrypted message in the red layer and three bits in the green layer and two bits in the blue layer. The method involves hiding the secret message bits in the layers of the cover image in three maps:

1. Blue Green Red (BGR): The first two bits of the letter are stored in the blue layer, followed by the three bits stored in the green layer and the remainder of the bits in the red layer.
2. Green Red Blue (GRB): The first three bits of the letter are stored in the green layer, followed by the three bits stored in the red layer and the two bits remainder are stored in the blue layer.
3. Red Green Blue (RGB): The first three bits of the letter are stored in the red layer, followed by the three bits stored in the green layer and the two bits remainder are stored in the blue layer.

Determine the way which used to hide will be based on the storage location, if the remainder of the row multiplier in the column equals 0, the first way of embedding will be chosen, but if the remainder of the row multiplier in the column equals 1, the second way of embedding will be chosen, if the remainder equals 2 then the third way will be chosen for embedding.
The main objective of the work is to encrypt secret data, and then hides encrypt secret data in specific locations of the cover image, but in a different sequence each time which gives a type of hash that acts as another type of encryption.

The encryption process is designed to make the data incomprehensible by unauthorized persons. The encryption stage in our algorithm goes through two phases to get encrypted data. We relied on encryption in one of the easiest and most famous encryption systems, the Caesar method, it uses the substitution of a letter by another one based on the shift value (key), in our algorithm we use the X-axis coordinates of the center of the main circle is key1 and is Y-axis coordinates of the center of the main circle is key2.

3.1 Encryption The Secret Text Steps:
1. Enter the secret text, plain text (PT)
2. Choose the cover image (CovIm)
3. Find circles in color images (CA)
4. Determine the center coordinates of main circle CX, CY, to use those coordinates in the encryption process
5. Encrypt the secret text using Caesar method based on the center coordinates of the main circle such as the following:
   - Cipher text1 (CT1) = (PT) + (CX)
   - Cipher text 2 (CT2) = (CT1) - CY
6. Get encrypted text
7. Repeat step 5 until all plain text is encrypted

3.2 Embedding The Encrypted Secret Text Steps:
1. Enter the secret ciphertext (CT2)
2. Choose the cover image (CovIm)
3. Find circles in the cover color image (CA)
4. Store all coordinates of the points within the circular regions in N*2 array lets ACP, where N is a no. of points within the circular regions, ACP[i][1] contains the X-axis coordinates of i point within the circular region, ACP[i][2] contain the Y-axis coordinates of i point within the circular region
5. Convert a character of the secret ciphertext (CT2) to asci_code (AsciCT2)
6. Convert the asci_code for a character of the secret ciphertext (AsciCT2) to binary code (BCT2)
7. Select a map to hide the character, depending on the location which that contain the character based on the following:
   - If (ACP[i][1]* ACP[i][2])%3
     - =0 the hiding map a character is Blue Green Red (BGR)
     - =1 the hiding map a character is Green Red Blue (GRB)
     - =2 the hiding map a character is Red Green Blue (RGB)
9. Embedding a cipher character from secret ciphertext in a determined pixel of a cover image
10. Repeat step 5_7 until all ciphertext characters are embedding
11. Get the stego image (StegoIm)

3.3 Extracting Embedding Secret Text steps:
1. Enter the stego image (StegoIm)
2. Find circles in stego color image (CA)
3. Store all coordinates of the points within the circular regions in N*2 array lets ACP, where N is a no. of points within the circular regions, ACP[i][1] contain the X-axis coordinates of i point within the circular region, ACP[i][2] contains the Y-axis coordinates of i point within the circular region

4. Extract the embedding cipher character depending on the location that contains the character based on the following:
   If \((ACP[i][1]*ACP[i][2]) \mod 3\)
   - \(=0\) the hiding map a character is Blue Green Red (BGR)
   - \(=1\) the hiding map a character is Green Red Blue (GRB)
   - \(=2\) the hiding map a character is Red Green Blue (RGB)

5. Repeat step 4 until getting all extract cipher secret text (ECT).

3.4 Decryption The cipher Secret Text Steps:
1. Enter the extract secret ciphertext (ECT).
2. Enter the stego image (StegoIm)
3. Find circles in stego color image (CA)
4. Determine the center coordinates of main circle CX, CY, to use those coordinates in the encryption process
5. Decrypt the secret text character using Caesar method based on the center coordinates of the main circle such as the following:
6. Decrypt text1 (DT1) = (ECT) - (CY)
7. Decrypt text (DT) = (DT1) + (CX)
8. Repeat step 5 until Decrypt all extract cipher secret text.

The following block diagram clear Encryption&Embedding process in the sender side and Extracting &decryption process on the receiver side of the proposed algorithm, Fig.1.
4. Result and Analysis:

The proposed algorithm was built using Matlab 2019, and it has applied to a group of different size images to demonstrate the possibility of using it for all images size, we have chosen an images that contains one circular area and other images that containing more than one circular area to demonstrate the efficiency of defining circular areas in the proposed algorithm and the results were shown in table.1 which is below.

Table 1. The images before and after HidingMany metrics are used to demonstrate the efficiency of

| Image Name | Original Image | Stego Image |
|------------|----------------|-------------|
| Image 1    | ![Image 1 Original](image1.png) | ![Image 1 Stego](image1_stego.png) |
| Image 2    | ![Image 2 Original](image2.png) | ![Image 2 Stego](image2_stego.png) |
| Image 3    | ![Image 3 Original](image3.png) | ![Image 3 Stego](image3_stego.png) |
| Image 4    | ![Image 4 Original](image4.png) | ![Image 4 Stego](image4_stego.png) |
| Image 5    | ![Image 5 Original](image5.png) | ![Image 5 Stego](image5_stego.png) |
| Image 6    | ![Image 6 Original](image6.png) | ![Image 6 Stego](image6_stego.png) |
The Mean Square Error (MSE), the Peak Signal to Noise Ratio (PSNR) and the Signal to Noise Ratio (SNR), correlation coefficient (Corr), The Structural Similarity index (SSIM) are used to test the quality of image Steganography, Bit error rate (BER) are used to test retrieval data.

MSE represents the squared difference between the original image and the stego image, whereas PSNR represents a measure of the peak error [17],[18],[19]. The general form of PSNR, MSE, and SNR is as follows.

\[ PSNR = 10 \log_{10} \left( \frac{C_{\text{max}}}{MSE} \right) \]  \hspace{1cm} (1)

Where \( C_{\text{max}} \) represents the maximum value in the image.

\[ MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2 \]  \hspace{1cm} (2)

\[ SNR = 10 \log_{10} \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} x_{ij}^2}{\sum_{i=1}^{N} \sum_{j=1}^{M} (x_{ij} - y_{ij})^2} \]  \hspace{1cm} (3)

Where \( M,N \)  Represents the row and column of the image, \( x_{ij} \) represents the cover image and \( y_{ij} \) represents an image that contains hidden information.

The correlation coefficient is used for the purpose of comparing two images and noting the extent of their convergence. The best value for the correlation coefficient is to be close to one [20][21][22][23].

\[ Corr = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (x_{ij} - \bar{x})(y_{ij} - \bar{y})}{\sqrt{\sum_{i=1}^{N} \sum_{j=1}^{M} (x_{ij} - \bar{x})^2} \sqrt{\sum_{i=1}^{N} \sum_{j=1}^{M} (y_{ij} - \bar{y})^2}} \]  \hspace{1cm} (4)

Where \( \bar{x}, \bar{y} \) Represents the mean of image x and y and can be found by the following equation

\[ \bar{x} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} x_{ij}}{NM} \]  \hspace{1cm} (5)  And  \[ \bar{y} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} y_{ij}}{NM} \]  \hspace{1cm} (6)

The Structural Similarity index (SSIM) is a method for calculating the similarity between two images and its points how much a stego image is similar to the original image[24].

Bit error rate (BER) calculates the actual number of bit positions that are varied in the stego-image compared with the original image [25].
The results of the image metrics are shown in Table 1 and Table 2 give the values of MSE, Corr, SNR and PSNR, SSIM and BER of different types of images of different types of images.

**Table 1** (Mean Square Error (MSE), correlation coefficient (Corr), Signal to Noise Ratio (SNR)) metrics for the proposed method

| Image name | MSE            | Corr            | SNR            |
|------------|----------------|-----------------|----------------|
| 2f         | 0.00152582626809431 | 0.999999517163353 | 65.9138180628453 |
| 3f         | 0.000206063716456326 | 0.999999861813952 | 72.1752538005781 |
| 6f         | 0.00208308455731136 | 0.999999142735082 | 66.9183276780933 |
| 7f         | 0.00171821305841924 | 0.999999283277961 | 62.8273572062556 |
| 8f         | 0.00214650205761317 | 0.999999042575196 | 65.0787168613582 |
| 9f         | 0.00192655187074830 | 0.99999935151924  | 63.552694492583  |

**Table 2** (Peak Signal to Noise Ratio (PSNR), Structural Similarity index (SSIM), Bit Error Rate (BER)) metrics for the proposed method

| Image name | PSNR            | SSIM            | BER            |
|------------|-----------------|-----------------|----------------|
| 2f         | 71.6848146429595 | 0.999998290473524 | 0              |
| 3f         | 79.1728726584688 | 0.999999710432994 | 0              |
| 6f         | 71.7638992832398 | 0.999993563995055 | 0              |
| 7f         | 71.6458058943006 | 0.999988174265215 | 0              |
| 8f         | 70.5956350035664 | 0.999998567312157 | 0              |
| 9f         | 71.9830596275765 | 0.999960004761695 | 0              |

Examining the results in table 1, we note that the value of the MSE scale for all images is a small amount if it does not exceed the value 0.00214650205761317, which gives a clear impression on the quality of the algorithm, as we note that the value of Corr between the original image and the image after hiding is a value close to one Where was the lowest value 0.999999042575196, which indicates that the ratio of the image correlation before hiding and the image after hiding is a high correlation For BER, its value equals to zeros for all images, which indicates that the hidden text is fully retrieved without any decrease. This is a clear indication of the quality and efficiency of the proposed algorithm. (If the value of BER is closer to zero it means the quality of the image is good).

**Conclusion**

The idea of using circular area coordinates in the encryption and steganography processes in digital color images is an efficient and new idea at the same time, because of the availability of many images that include circular shapes such as football images, circular coin images, traffic images, and many others images that are not questionable or suspicious. The proposed algorithm encrypted secret text data using the simple and traditional Caesar method, but in an innovative way based on the coordinates of the central circular shape that the algorithm finds. This is followed by hiding or embedding encrypted data in specific locations within the color image using a method that provides a second encryption process depending on the location where the data will be embedded, this will be providing the possibility of encrypting the same character two different encryptions in the same
message, which will be providing high security in the data transfer, The difficulty of decoding by unauthorized persons, as well as the full retrieval of that data at the receiving end of the communication. The experiments confirmed the efficiency and quality of the work.

Acknowledgments

The authors are very grateful to the University of Mosul/ College of Computer Science and Mathematics and Al-Nahrain University / College of Science for their provided facilities, which helped to improve the quality of this work.

References

[1] K. Joshi, S. Gill, and R. Yadav, 2018, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image", Journal of Computer Networks and Communications, (8),1-10, Article ID 9475142.
[2] P. Chandarana, P. Ahirao, 2018, "ADVANCED IMAGE STEGANOGRAPHY", International Journal Of Innovative Research in Information Security (IJIRIS), 5(7).
[3] A. S. Ansar, M. S. Mohammadi, and M. T. Parvez, 2019, “A Comparative Study of Recent Steganography Techniques for Multiple Image Formats”, I.J. Computer Network and Information Security, 11(1), 11-25.
[4] A. AL-Shaaby, T. AlKharobi, 2017,“Cryptography and Steganography: New Approach”, TRANSACTIONS ON NETWORKS AND COMMUNICATIONS, 5(6), 25-38.
[5] S. F. Al-Azzawi and M. M. Aziz, “Chaos Synchronization of Nonlinear Dynamical Systems via a Novel Analytical Approach,” Alexandria Engineering Journal, vol. 57, no. 4, pp. 3493-3500, Dec 2018.
[6] S. F. Al-Azzawi, et al., "Chaotic Lorenz System and it's Suppressed," Journal of Advanced Research in Dynamical and Control Systems, vol.12, no. 2, pp. 548-555, 2020.
[7] A. S. Al-Obeidi and S. F. AL-Azzawi, “Chaos Synchronization in a 6-D Hyperchaotic System with Self-Excited Attractor,” TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 18, no 3, pp. 1483-1490, June 2020.
[8] M. Juneja, P. S. Sandhu, 2013, “An Improved LSB Based Steganography Technique for RGB Color Images”, International Journal of Computer and Communication Engineering, 2(4), 513-517
[9] B. Singh, S. Kataria, T. Kumar, and N. S. Shekhawat, 2014, “A Steganography Algorithm for Hiding Secret Message inside Image using Random Key”, International Journal of Engineering Research & Technology (IJERT), 3(12).
[10] B. Purnama, H. Rohayani, 2015, ”A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted", Procedia Computer Science, 59, 195-204.
[11] A. K. Singh, J. Singh, H. V. Singh, 2015, “Steganography in Images Using LSB Technique”, International Journal of Latest Trends in Engineering and Technology (IJLTET), 5(1), 426-430.
[12] R. Tavoli, M. Bakhshi, F. Salehian,2016, “A New Method for Text Hiding in the Image by Using LSB”, (IJACSA) International Journal of Advanced Computer Science and Applications, 7(4), 126-132.
[13] J. K. Alhassan, I. Ismaila, V. O. Waziri, and A. Abdulkadir, 2016, “ A Secure Method to Hide Confidential Data Using Cryptography and Steganography”, Federal University of Technology, Minna, Nigeria November, 28-30.
[14] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. Khalaf, H. M. Ali, 2019, “Hiding data in images using steganography techniques with compression algorithms”, Telkomnika, 17(3), 1168-1175.

[15] N. Krishnaveni, S. Periyasamy, 2018, “Image steganography using LSB embedding with chaos ”, 118,505-509.

[16] H. Ogras, 2019, “An Efficient Steganography Technique for Images using Chaotic Bitstream” International Journal of Computer Network and Information Security, 11(2), 21.

[17] A. Sundar, V. Pahwa, C. Das, M. Deshmukh, N. Robinson, 2016, “A Comprehensive Assessment of the Performance of Modern Algorithms for Enhancement of Digital Volume Pulse Signals ”, International Journal of Pharma Medicine and Biological Sciences, 5(1), 91.

[18] Y. Inan, 2018, “Assessment of the Image Distortion in Using Various Bit Lengths of Steganographic LSB ”, Near east University, Computer Engineering Department, Nicosia, TRNC, Mersin 10 Turkey, ITM Web of Conferences 22, 01026.

[19] E. Noroozi, S. B. M. Daud, A. Sabouhi, 2011, “Critical Evaluation on Steganography Metrics “, In Advanced Materials Research,748, 927-931, Trans Tech Publications Ltd.

[20] E. A. Albahrani, 2017, "A New Audio Encryption Algorithm Based on Chaotic Block Cipher", Annual Conference on New Trends in Information & Communications Technology Applications -(NTICT 2017), 22-27, IEEE.

[21] Z. N. Al-Khatee, M. F. Jader, 2020, “Encryption and Hiding Text Using DNA Coding and Hyperchaotic System,” Indonesian Journal of Electrical Engineering and Computer Science, 19(2)Aug 2020.

[22] Z. N. Al-katee , M. R. Al-Bazaz, 2019 ,“Steganography in Colored Images Based on Biometrics,” Tikrit Journal of Pure Science, 24(3), 111-117.

[23] Z. N. Al-Khatee , S J. Mohammed, 2020, “A Novel Approach for Audio File Encryption Using Hand Geometry,” Multimedia Tools and Applications,Mar 2020

[24] E. Margalikas, S. Ramanauskaitė, 2019, “Image steganography based on color palette transformation in color space “ , EURASIP Journal on Image and Video Processing 2019(1), 82.

[25] M. S. Hiwe, S. I. Nipanikar, 2014, “An Analysis of Image Steganography Methods”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, 3(2),