Study of Hiding Text Messages Technique in Digital Images

Prof. Dr. Hiba Khudair Abbas Jasem Al-Jubouri

Al-Mustansiriyah University / College of Science / Department of Physics

Hebaka_phys@csw.uobaghda.edu.iq

Prof.Sameera Naji Kadhem

University of Baghdad / College of Science for Women / Department of Mathematics

Samirank_math@csw.uobaghdad.edu.iq

Asst. Prof. Dr. Haidar Jawad Mohammed
Al-Mustansiriyah University / Department of Physics

haidar.mohamad@uomustansiriyah.edu.iq

Abstract:

Steganography is a data security method that conceals information within a medium, ensuring no suspicion about a link between two parties. During the Arbaeen pilgrimage, a study used the least significant bit (LSB) concealment method, extracting letters from text within a coloured digital image, converting them into binary numbers, and embedding them within the image. This process resulted in an image containing textual information, allowing comparison with the original image to observe additive noise differences. The most significant noise effects were observed in homogenous areas and edge regions, with a pronounced impact of masking across all color packets. The study used statistical metrics like mean square error (MSE) and peak-to-noise ratio (PSNR) to analyze the quality and effectiveness of the outputs. The best stenographic effect occurs when the message size is small, the image size is large, and there are fewer bits to be hidden. The best reduction effect is achieved when the message size is small and the image size is large, with fewer bits to hide. The blue, red, and green bars exhibit the best steganography effects, ensuring the security of pilgrims in Karbala Governorate and elsewhere, and facilitating easy and secure data transmission.

Keywords: Cryptography, Steganography, Least Significant Bit Strategy, Statistical Detection

Introduction

Interpersonal communication is one of the most crucial aspects of human growth (Suresh & Parthasarathy, 2016). The secrecy of the data being communicated is necessary for this operation (Al-Saedi, 2016). Humans have looked for different strategies to guarantee the quick transfer of information (Resham et al., 2021). Information security and secrecy are maintained using various methods, including steganography and encryption (Iacovitti, 2022). The encryptor can now access and change data thanks to the development of hacking techniques (Clemen & Teleron, 2023). Information preservation required a more secret method (Abbas et al., 2021). Thus, steganography was employed, which hides the transferred data inside the transmitted media—text, music, pictures, and videos —so that no one can see it (Muhammad et al., 2015). The science of encrypting and decrypting data using mathematics is known as cryptography. Only the intended recipient may access sensitive data stored or sent over unprotected networks (like the internet) thanks to cryptography (Habeeb, 2020). Both cryptography and cryptanalysis are included in cryptography (Mustafa, 2020). Strong and poor encryption are both possible. The amount of time and resources needed to retrieve the plaintext is a measure of an encryption's strength(Derea et al., 2019). Strong encryption produces ciphertext that is challenging to decode without the right decryption software (Hassan & Gutub, 2021). The strength of the encryption algorithm and the key's secrecy are the only factors that affect the security of encrypted data (Khaldi, 2019). The technique of hiding a secret communication behind another harmless medium (text, image, sound, video, etc.) is called steganography (Greek: מראורה, meaning cover, and graphein, meaning writing). Security in steganography depends on the likelihood that a secret message won't be detected or found, whereas, in cryptography(Al-Obaidi et al., 2023),

security depends on the encrypted information being unintelligible to unauthorized individuals (Kim et al., 2021). Modifying portions of a chosen file's code is required to embed a message. Making these modifications undetectable or inaudible is the fundamental goal of steganography. The risk of modification will go unnoticed and increases with the message and file size (Jawad et al., 2022). Three factors form the basis of steganography properties: Robustness guarantees that confidential data cannot be erased without seriously harming the reputation (Mohamad et al., 2019).

This field has been investigated by several academics. In (2022), Nada Abdul Aziz Mustafa generates a practical steganography procedure to hide the text in the image. This operation allows the user to provide the system with both text and cover image, and to find a resulting image that comprises the hidden text inside. The suggested technique is to hide text inside the header formats of a digital image. The Least Significant Bit (LSB) method to hide the message or text, to keep the features and characteristics of the original image are used. A new method is applied using the whole image (header formats) to hide the image. From the experimental results, the suggested technique gives a higher embedding of several stages of complexity. Also, the LSB method uses the whole image to increase the security and robustness of the proposed method as compared to state-of-the-art methods (Abdul & Mustafa, 2022). In (2024), Ali Salem Ali and Suray Alsamaraee proposed a scheme consisting of four phases with different contributions. The first phase was used to preprocess the secret messages and cover images. In this phase, the confidential message is compressed using the Huffman method. The second phase involved the embedding procedure. This phase consists of HMPSO and DDV contributions. The HMPSO is responsible for the optimal pixels' selection. The DDV contribution is responsible for the embedding process. The third

phase involves the extraction method. In extraction, the reverse processes are implemented in the previous steps. SSIM, PSNR, HVS, Histogram analysis, and chi-square test were used to validate and test different evaluation parameters. Based on the findings, the proposed scheme has solved the privacy, and integrity challenges and provides a robust steganography system (Ali et al., 2024).

This research aims to employ varying levels of text concealment in digital photographs, thereby enhancing the secrecy of the concealed data and making it more challenging to recover, especially in Arbaeen pilgrimage. The program was created to solve the data masking and retrieval operation. To include information in a particular medium without raising suspicions about correspondence between two parties, one method used to protect information is the act of hiding. In this case, it is easy to send sensitive information without discovering during Arbaeen pilgrimage.

Theoretical Background

Least Significant Bit (LSB):

LSB gathers everything related to data concealment by modifying the low-order bit of an element. Modification of the value of a pixel or the modification of the value of a DCT coefficient in the case of the JPEG standard (Abbas & Mohamad, 2021). All are based on the insensitivity of the human visual system to a small change in colors. There are two LSB methods: LSB replacement consists of substituting the least significant bits of the pixels for the message bits to be inserted. LSB matching steganography, Least Significant Bit (LSB) matching steganography, also named ±1 embedding, is a slightly more sophisticated version of LSB embedding. The LSB correspondence steganography method does not alter

the first order statistical distribution of the host support. So All first-order statistical attacks are ineffective, Least Significant Bit Strategy Spatial (Image) domain strategy: in image domain, the LSB technique is the most important and the easiest one to embed information in a cover image. Popular stenographic tools that are based on LSB embedding vary in their approach for hiding information. Methods like Steganos and Stools use LSB embedding in the spatial domain, while others like Jsteg and Out-Guess embed the message in the frequency domain(Awad et al., 2018). With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference and Transform domain strategy: these strategies based on hiding information in more significant areas of the cover image making it more robust.

Algorithms of the hiding text:

ALGORITHM (I): Hiding the Text Message in One Row in the Color Digital Image

- Step1: Read color digital image I1
- Step2: Choose color band of digital image (R,G,B)
- Step3: Enter the number of bits to be hidden in the text [1 or 2]
- Step4: Determining the hiding location in which bits we want to hide [1 2] In other words, it is the place to hide the first bit and the second bit
- Step5: Select the row in which to hide the text row=50;
- Step6: Steganography Process
  - generate color image at the same color image entering resulting image in which hide the text I2
  - choose a color band (R,G,B) from the generated image in which the text will be hidden
  - Select the text message to be hidden in the image and the color band

- convert haracter in the text message to a binary number with 8 bits using code bins= dec2bin(str,8)
- transform each row into a column and each column is a row bin2
- Making reshap bins=bin2(:)' so that the message is in one line, its kind char, take these bits and hide them in the image
- transform each character into one location that contains each character binv=bins-48; where msg=binv
- determine the length of the text by the number of characters L=numel(str), and the length of the text by binary LL=8*L
- Determine the number of Step that moves through it: step= no. of bits entered* fix (no. of column / LL), where fix () is a function in MATLAB approximates in the positive infinity direction, LL<no. of column
- Specifies the pixel in which to hide the text: A=I2(no. of row, pixel position, band type)
- The pixel value has changed because of masking: A2=bitset(A, location hide bit, no. of bit)
- Repeat the step

– Step7: De- steganography process: To return the text message to characters

- Read steganography image I3
- Read the color band (R,G,B) from I3
- make a counter from 1 to LL step no. of bits
- Image element (pixel) in which text is hidden A1=I1(The number of the row in which it was hidden, position of pixel in the row)
- determine the value of the first bit and the second bit in which the hiding occurred for each element in which the operation was hidden so that generate a vector EE(j)of length LL using code EE(j)=A1; L=length (EE)
- divide it into 8 bits, each 8 bits representing a character NT=round (L/8)
- generate a function to convert each 8 bits into a character using the codeVT=bin2char (TT) where TT=EE(j:j+7)

- Step8: end algorithm

ALGORITHM (II): Hide the Text Message in All Rows of the Color Digital Image

- Step1: Read color digital image I1.
- Step2: Choose color band of digital image (R,G,B).
- Step3: Enter the number of bits to be hidden in the text [1 or 2].
- Step4: Determining the hiding location in which bits we want to hide [1 2] In other words, it is the place to hide the first bit and the second bit.
- Step5: Steganography Process.
  - generate color image at the same color image entered get an image in which hide the text I2
  - choose a color band(R,G,B) from the generated image in which the text will be hidden
  - Select the text message to be hidden in the image and the color band
  - convert each character in the text message to a binary number with 8 bits using code bins= dec2bin(str,8)
  - transform each row into a column and each column is a row bin2=
  - Making reshap bins=bin2(:)' so that the message is in one line, its kind char, take these bits and hide them in the image
  - transform character into one location binv=bins-48; where msg=binv
  - determine the length of the text by the number of characters L=numel(str), and the length of the text by binary LL=8*L
  - Determine the number of Step that moves through it: step= no. of bits entered* fix (no. of column / LL), where fix () is a function in MATLAB approximates in the positive infinity direction, LL<no. of column
  - Make a counter from row; for i=1: r where i counter for row and r no. of row in image
  - Specifies the pixel in which to hide the text: A=I2(i, pixel position,

band type)

- The pixel value has changed because of masking: A2=bitset (A, location hide bit, no. of bit)
- Repeat the step

- Step6: De- steganography process: To return the text message to characters
  - Read steganography image I3
  - Read the color band (R,G,B) from I3
  - make a counter from 1 to LL step no. of bits
  - Image element (pixel) in which text is hidden A1=I1(The number of the row in which it was hidden, position of pixel in the row)
  - determine the value of the first bit and the second bit in which the hiding occurred for each element in which the operation was hidden so that generate a vector EE(j)of length LL using code EE(j)=A1 ; L=length (EE)
  - divide it into 8 bits, each 8 bits representing a character NT=round (L/8)
  - generate a function to convert each 8 bit into a character using the code VT=bin2char(TT) where TT=EE(j:j+7)
- Step7: end algorithm

ALGORITHM (III): Calculation of statistical criteria to evaluate the quality and efficiency of the results

- Step1: read color digital image I1
- Step2: read steganography color digital image I2
- Step3: Calculate Mean Square Error between I1,I2 using MSE = immse(I1,I2)where immse function to calculate mean square error
- Step4: Calculate Peak Signal to Noise Ratio between I1,I2 using PPsnr= psnr(I1,I2)

Experimental steps

Hiding text messages in digital color images. Where it relied on colored digital images of different sizes, and text messages of different lengths were hidden. The process of hiding included two parts:

First was to hide text messages in one row of the colored digital image, and the second part included hiding text messages in all rows of the colored digital image. The quality and efficiency of the images resulting from the steganography process were evaluated based on two statistical criteria (Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR))(Abbas et al., 2019). The type of noise that will be caused by the process of adding information was also studied. As well as note the effect of the largest noise on the image and color bands (RGB). The programs were built and developed using MATLAB (2020). The work plan consists of four parts; Part one: It includes the process of hiding text messages of different lengths in one row from the color digital images approved in the study. The second part: includes the process of hiding text messages of different lengths in all the rows of the color digital image approved in the study. The third part includes calculating the statistical characteristics to estimate and know the efficiency of the resulting images. The fourth part includes calculating the difference between the original image and the steganography image, which represents the observation of the effect of noise in the image and color bands (RGB).

Flag Image is downloaded online and used widely during Arbaeen pilgrimage. Image size is (225×225) elements and a gray intensity for each band ranging from (0-255). Bit depth is 24 bits/pixel, and its type is JPG, as shown in figure (1).

Figure (1): Flag color digital image

Text Messages to be hidden in the Image:

Three text messages of different lengths were used to hide them in the digital images adopted in the study

1.The text message is represented by 14 characters that are hidden in the images represented by the text phrase as in Figure (2).

Hello everyone

(a)

(b)

Figure (2): text message with 14 characters (a) decimal and (b) binary data.

Where each decimal character corresponds to 8-bit binary as shown in the table (1).

Table (1): The decimal character and its 8-bit binary equivalent for the message (A)

decimal	Binary	decimal	binary
H	01001000	E	01100101
e	01100101	V	01110110
l	01101100	E	01100101
l	01101100	R	01110010
o	01101111	Y	01111001
	00100000	O	01101111
		N	01101110
		E	01100101

2.The text message is represented by 31 characters that are hidden in the images represented by the text phrase as in Figure (3).

Hello everyone; have good time.

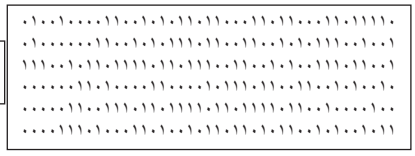


Figure (3): The text massage with 31 characters in (a) decimal and (b) binary data.

Where each decimal character corresponds to 8-bit binary as shown in the table (2).

Table (2): The decimal character and its 8-bit binary equivalent for the message in Figure (3)

decimal	Binary	decimal	binary
H	01001000	h	01101000
e	01100101	a	01100001
l	01101100	v	01110110
l	01101100	e	01100101
o	01101111		00100000
	00100000	g	01100111
e	01100101	o	01101111
v	01110110	o	01101111
e	01100101	d	01100100
r	01110010		00100000
y	01111001	t	01110100
o	01101111	i	01101001
n	01101110	m	01101101
e	01100101	e	01100101
;	00111011	.	00101110
	00100000		

Results and discussion

The most significant findings obtained from the implementation of the hiding operations suggested in the study are discussed to be send in the Arbaeen pilgrimage. Three text messages with a total length of 14, 31 characters were used, and several bits (1 and 2) were concealed in the first and second-bit positions of the pixel. This process includes two methods for hiding information: the first involves hiding text message in a single row of the color digital image, and the second includes hiding the text message in every row of the color digital image. The difference between the original and stenographical images was calculated to note the impact of noise on the image and the color band (RGB). The results were discussed for both methods, which involved applying the steganography process to each band of the color digital image. The effectiveness of the stenographical process's output was assessed using effective statistical criteria (MSE and PSNR)(Derea et al., 2019).

The Results of Hiding Information in One Row of the Color Digital Image:

The information was hidden in one row of the color digital image, as the process included reliance on two text messages and the process of hiding based on one bit and two bits, and this was applied to the approved digital images and their color bands (RGB).

1.The Results of the Hiding Process Based on the Text Message with a Length of 14 Characters and several bits

The hiding process, in (algorithm I), was applied to the digital images approved in the study. The information was hidden in one row, where the length of the text message was 14 characters, and the number of bits was 1.

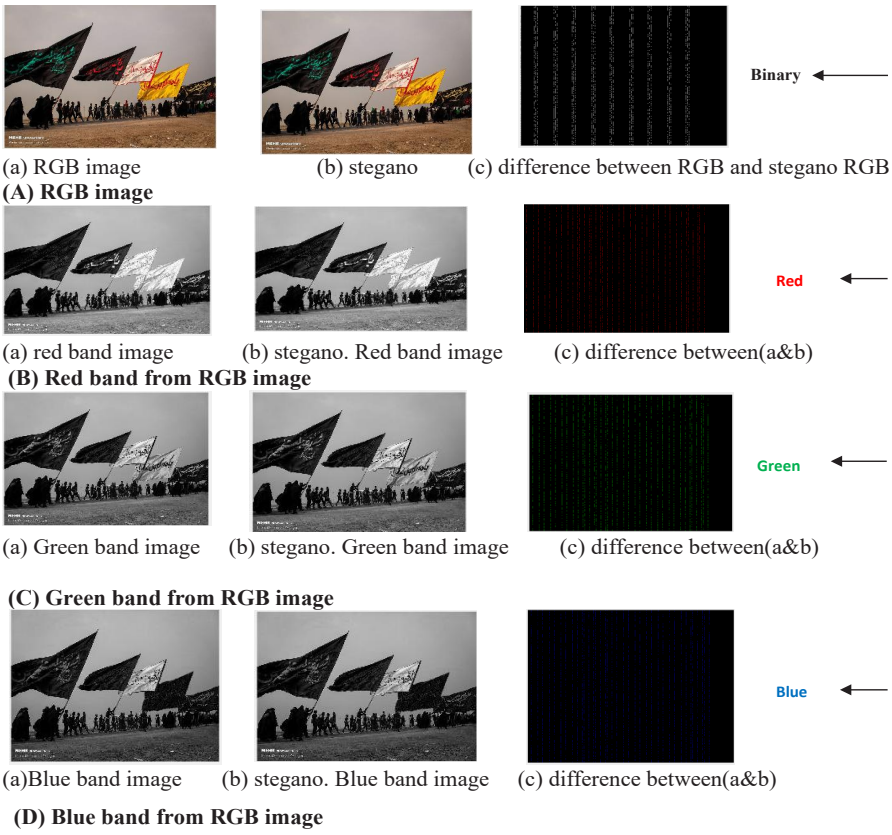


Figure (4): hiding process and difference for a color digital image (A) RGB image, (B) Red band image, (C) Green band image, and (D) Blue band image, From the figures (4), the difference was very clear because of the small size of the image.

Results of Estimation of the Efficiency and Quality of Images:

The results of the resulting images before and after the steganography process, represented by one line of a 14-character message length, were estimated to hide 1 bit in the first and second positions of the pixel, depending on the statistical quality criteria represented by (MSE) and (PSNR) according (algorithm III) as in the table (3).

Table (3): Statistical quality criteria for color images and color bands (massage 14 characters, 1bit)

Color images	MSE	PSNR
Red -band	0.0187	65.4144
Green –band	0.0186	65.4308
Blue-band	0.0189	65.3570

2.The Results of the Hiding Process Based on the Text Message with a Length of 14 Characters and several bits 2

The steganography process (algorithm I) was applied to digital color images when the text message length was 14 characters, and the number of bits was 2.

Results of the steganography process on digital color images:

The algorithm (I) was applied to the certified color digital images, applied to the color bands (RGB) of the image, and calculated the difference between the digital image and the stegano. image, then calculated the difference (noise effect) between the color bands (RGB) and the bands of the image steganography (RGB).

(a) color image (b) stegano (c) difference between RGB and stegano RGB

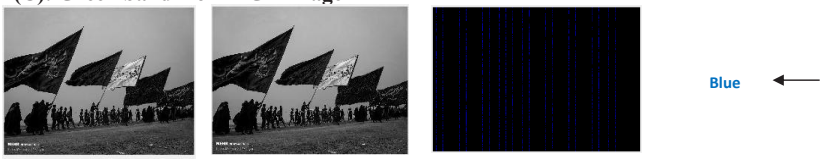
(A): RGB image

(a) red band (b) stegano (c) difference between (a & b)

(B): Red band from RGB image

(a) Green band (b) stegano (c) difference between (a & b)

(C): Green band from RGB image



(a)Blue band (b) stegano (c) difference between (a & b)

(D): Blue band from RGB image

Figure (5): hiding process and difference for a color digital image; (A) RGB mage, (B) Red band image, (C) Green band image, and (D) Blue band image, From the results of the images in the figures (4 and 5), the image is clearer in the difference between the original image and the stegano.

Results of Statistical Quality Criteria's

Statistical criteria were calculated for the images before and after the steganography process, represented by hiding information in one row of the image with a 14-character text message to hide 2 bits in the first and second positions of the color digital image element (pixel).

Table (4): Statistical quality criteria (massage 14 characters, 2bits)

Color images	MSE	PSNR
Red –band	0.0396	62.1497
Green –band	0.0399	62.1223
Blue-band	0.0401	62.0945

Where notice that the value of (MSE) is very small and the value of (PSNR) in it is very large and note that the effect of adding information to the image is not equal between color bands (RGB).

The Results of the Hiding Process Based on the Text Message with a Length of (31) Characters and several bits 1.

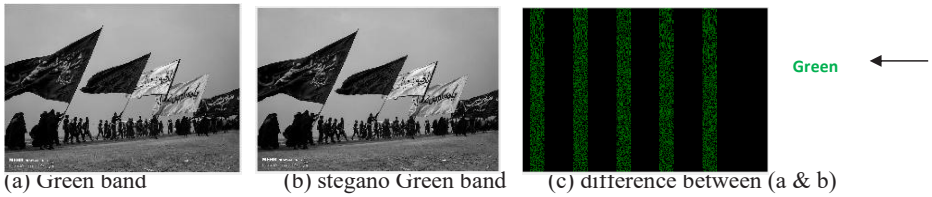
The hiding process in (algorithm I) was applied to the digital images approved in the study, and the information was hidden in one row, where the length of the text message was 31 characters.

(a) RGB image (b) stegano (c) difference between RGB and stegano RGB

(A) RGB image

(a) red band (b) stegano Red band (c) difference between (a & b)

(B): Red band from RGB image



(a) Green band (b) stegano Green band (c) difference between (a & b)

(C) Green band from RGB image

(a)Blue band (b) stegano Blue band (c) difference between (a & b)

(D) Blue band from RGB image

Figure (6): stegano process and difference for a color digital image (A) RGB image, (B)Red band image, (C) Green band image and (D) Blue band image, From the figures (6), the process of hiding between the bands was different, as we notice that the blue band has more concealment, than the red band, then the green band.

Results of Statistical Quality Criteria's

Statistical criteria were calculated for the images before and after the steganography process, represented by hiding information in one row of the image with 31 characters text message to hide 1 bit in the first and second positions of the color digital image element (pixel), as in Table (5).

Table (5): Statistical quality criteria for color images and color bands.

Color images	MSE	PSNR	
Red -band	0.0494	61.1936	31 characters text massage length 1bit
Green –band	0.0492	61.2150	
Blue-band	0.0489	61.2337	

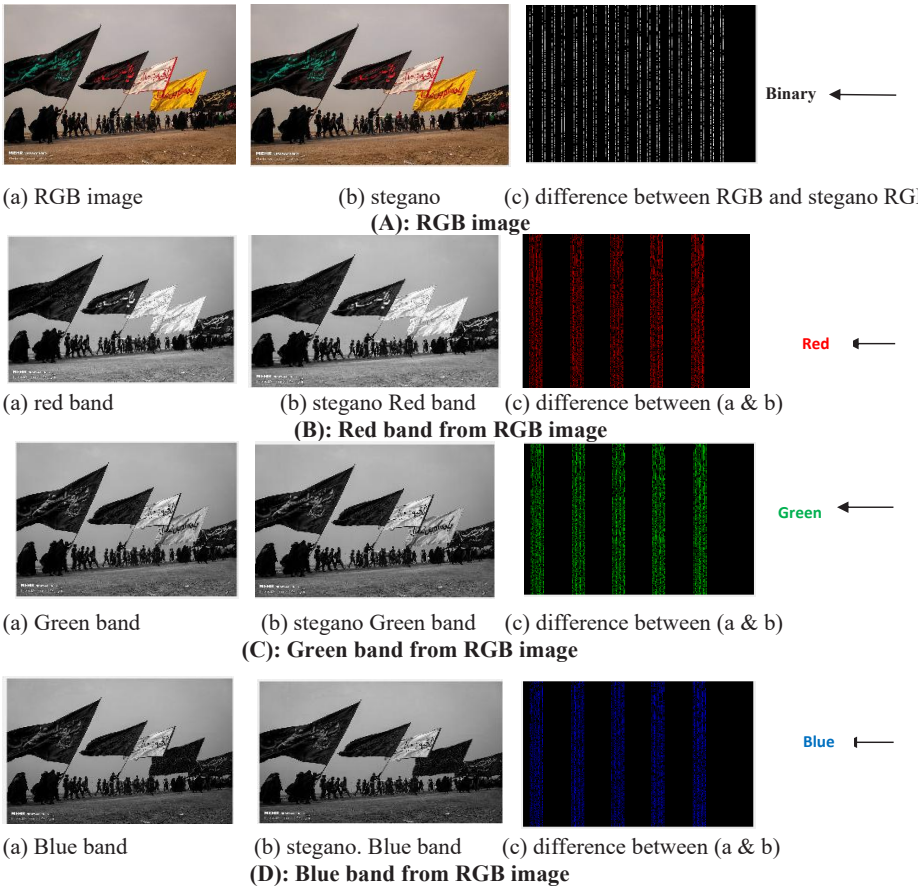
From the results of the table (5), the koala image recorded the lowest value for MSE and the highest value for the criterion PSNR, which confirms that the process of information disappearance in the image with a large size is better than the image of a small size, also note that the process of hiding information in color bands is not equal, as note that the blue band is better at hiding information than red and green, and the green band is not good at hiding information because its MSE value is greater than the rest of the color band values RB.

The Results of the Hiding Process Based on the Text Message with a Length of (31) Characters and several bits 2:

The hiding process in (algorithm I) was applied to the digital images approved in the study, and the information was hidden in one row, where the length of the text message was 31 characters, and the number of bits was 1 for Arbaeen pilgrimage image.

Results of the method applied to approved images:

The steganography method was applied to color digital images by hiding a text message of (31) characters in length in one row of the image, and the number of bits 2 that were hidden in the first and second positions of the image element(pixel), as well as applied to the images of the three-color bands of the image (RGB).



(a) RGB image (b) stegano (c) difference between RGB and stegano RGB

(A): RGB image

(a) red band (b) stegano Red band (c) difference between (a & b)

(B): Red band from RGB image

(a) Green band (b) stegano Green band (c) difference between (a & b)

(C): Green band from RGB image

(a) Blue band (b) stegano. Blue band (c) difference between (a & b)

(D): Blue band from RGB image

Figure (7): stegano process and difference for a olor digital image; (A) RGB image, (B) Red band image, (C) Green band image (D) Blue band image, From Figures (7), the stegano process has become weak, because the image of the difference appeared more clearly than the previous methods, but despite that it also notes that the stegano.

Results of Statistical Quality Criteria's:

Statistical criteria were calculated for the images before and after the steganography process, represented by hiding information in one row of the image with 31 characters text message to hide 2 bits in the first and second positions of the color digital image element(pixel), as in Table (6)

Table (6): Statistical quality criteria for color images and color bands.

Color images	MSE	PSNR	
Red -band	0.01154	57.5088	31 characters text massage length 2 bit
Green –band	0.01146	57.5399	
Blue-band	0.01149	57.5275	

From the results of the table (6), the process of hiding information in color bands is not equal, as note that the green band is better at hiding information than red and blue, and the red band is not good at hiding information because its MSE value is greater than the rest of the color band values.

The Results of Hiding Information in All Rows of the Color Digital Image

The information was hidden in all rows of the color digital image, as the process included reliance on two text messages in Arbaeen pilgrimage image, as well as the process of hiding based on one bit and two bits, and this was applied to the approved digital images and their color bands (RGB).

The Results of the Hiding Process Based on the Text Message with a Length of 14 Characters and several bits 1:

The hiding process in (algorithm II) was applied to the digital images approved in the study, and the information was hidden in all rows, where the length of the text message was 14 characters, and the number of bits was 1.

Results of the method applied to approved images

The second method was applied to the approved color digital images, as well as to the color bands (RGB) dependent on the Arbaeen pilgrimage image, and the difference (noise effect) image was calculated between the digital image and the steganography image, then calculated the difference (noise effect) between the color bands (RGB) and steganography image bands (RGB) as shown in figure (8).

(a) RGB (b) stegano (c) difference between RGB and stegano RGB

(A): RGB image

(a) red band (b) stegano red band (c) difference between (a & b)

(B): Red band from RGB image

(a) Green band (b) stegano Green band (c) difference between (a & b)

(C): Green band from RGB image

(a) Blue band (b) stegano Blue band (c) difference between (a & b)

(D): Blue band from RGB image

Figure (8): stegano process and difference for a color digital image; (A) RGB image, (B)Red band image, (C) Green band image and (D) Blue band image ,From Figures (8), the difference in the image and color bands was very clear.

Results of Estimation of the Efficiency and Quality of Images:

The results of the resulting images before and after the steganography process, represented by all rows of 14-character message length, were estimated to hide 1 bit in the first and second positions of the pixel, depending on the statistical quality criteria represented by (MSE) and (PSNR) according (algorithm III) as in table (7).

Table (7): Statistical quality criteria for color images and color bands (massage 14 characters, 1bit)

Color images	MSE	PSNR
Red -band	0.03745	62.3957
Green –band	0.03737	62.4051
Blue-band	0.03745	62.3953

From the results of table (7), the noise effect of the color bands (RGB) is not equal. From this can be concluded that the larger the image size, the more efficient and good hiding results.

The Results of the stegano Process Based on the Text Message with a Length of 14 Characters and several bits 2.

The steganography process (algorithm II) was applied to digital color images when the text message length was 14 characters, and the number of bits was 2.

Results of the steganography process on digital color images:

Algorithm (II) was applied to the certified Arbaeen pilgrimage digital image, applied to the color bands (RGB) of the image, and calculated the difference between the digital image and the stegano. Then calculated the difference (noise effect) between the color bands (RGB) and the bands of the image steganography (RGB), as shown in Figure (9).

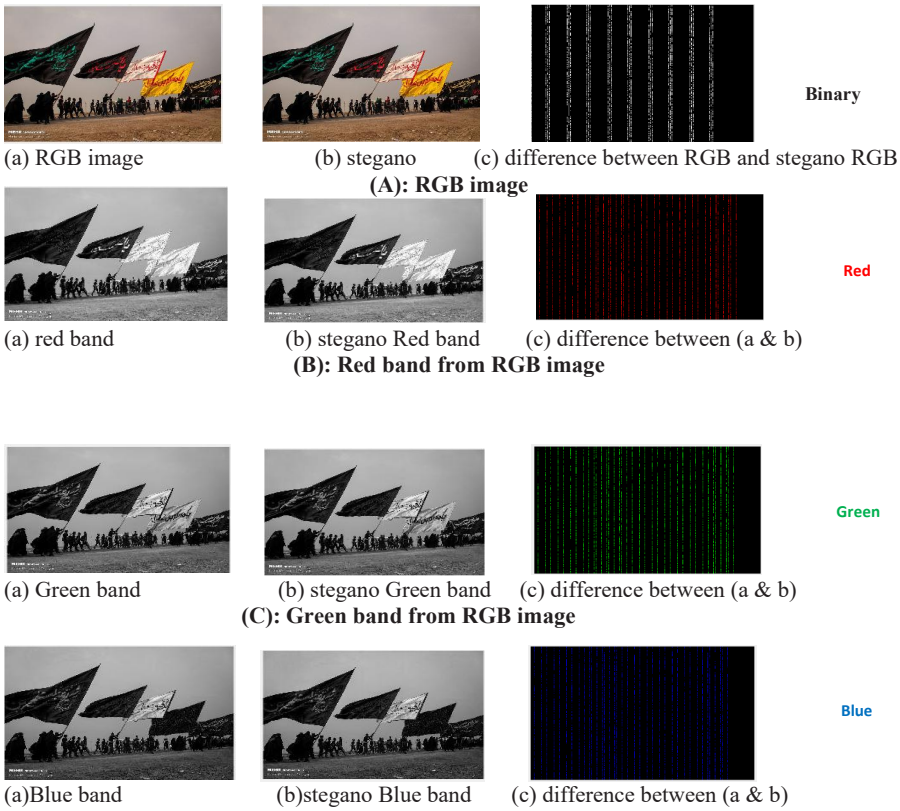


Figure (9): stegano process and difference for a color digital image (A) RGB image, (B) Red band image, (C) Green band image and (D) Blue band image

Figure (9): stegano process and difference for a color digital image (A)RGB image, (B) Red band image, (C) Green band image and (D) Blue band image, From the results of the images in the figures (9), the sharpness of the difference increased between the original image and the steganography image, as the difference in image was very large and clear and in all rows of the image.

Results of Statistical Quality Criteria's

Statistical criteria were calculated for the images before and after the steganography process, represented by hiding information in all rows of the image with 14-character text message to hide 2 bits in the first and second positions of the color digital image element (pixel), as in Table (8).

Table (8): Statistical quality criteria for color images and color bands (massage 14 characters, 2bits)

Color images	MSE	PSNR
Red -band	0.0806	59.0664
Green –band	0.0797	59.1136
Blue-band	0.0805	59.0727

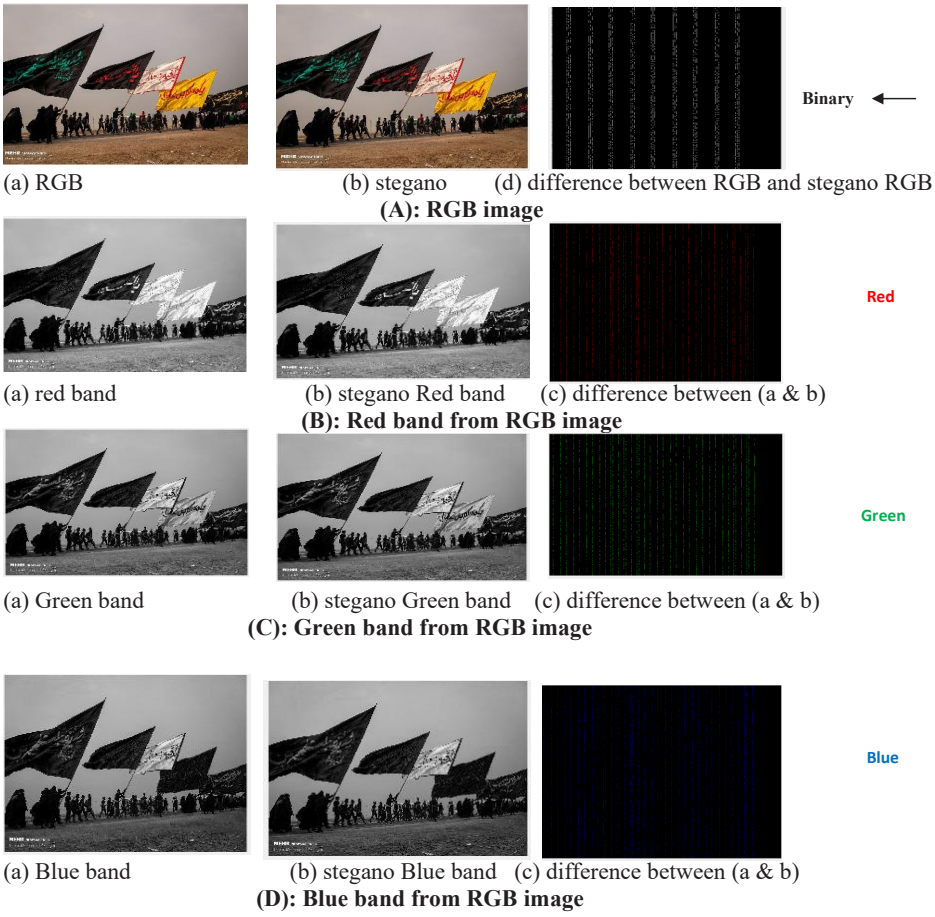
From the results of the table (8), the process of hiding the message in the image, where notice that the value of (MSE) very small and the value of (PSNR) in it is very large and note that the effect of adding information to the image is not equal between color bands (RGB).

The Results of the Steganography Process Based on the Text Message with a Length of (31) Characters and several bits 1

The process of masking in (Algorithm II) was applied to the digital images adopted in the study, and information was hidden in all rows, where the length of the text message was 31 characters, and the number of bits was 1 for Arbaeen pilgrimage image.

Results of the method applied to approved images:

The steganography method was applied to color digital images by hiding a text message of (٣١) characters in length in all rows of the Arbaeen pilgrimage image, and the number of bits that were hidden in the first and second positions of the image element (pixel), as well as applied to the images of the three color bands of the image (RGB), as shown in Figures (10).



(a) RGB (b) stegano (d) difference between RGB and stegano RGB

(A): RGB image

(a) red band (b) stegano Red band (c) difference between (a & b)

(B): Red band from RGB image

(a) Green band (b) stegano Green band (c) difference between (a & b)

(C): Green band from RGB image

(a) Blue band (b) stegano Blue band (c) difference between (a & b)

(D): Blue band from RGB image

Figure (10): stegano process and difference for a olor digital image (A) RGB image, (B) Red band image, (C) Green band image and (D) Blue band image

Results of Statistical Quality Criteria's

Statistical criteria were calculated for the images before and after the steganography process, represented by hiding information in one row of the image with a 31-character text message to hide 1 bit in the first and second positions of the color digital image element(pixel), as in Table (9).

Table (9): Statistical quality criteria for color images and color bands.

Color images	MSE	PSNR	
Red -band	0.018691	65.4144	31 characters text massage length 1bit
Green –band	0.018620	65.4308	
Blue-band	0.018940	65.3569	

From the results of the table (9), which note that the process of hiding information in color bands is not equal, as note that the green band is better at hiding information than red and blue, because its MSE value is greater than the rest of the color band values RB.

The Results of the Hiding Process Based on the Text Message with a Length of (31) Characters and several bits 2:

The hiding process in (algorithm II) was applied to the digital images approved in the study, and the information was hidden in one row, where the length of the text message was 31 characters, and the number of bits was 2 for Arbaeen pilgrimage image.

Results of the method applied to approved images

The steganography method was applied to color digital images by hiding a text message of (31) characters in length in one row of the image, and three-color bands of the image (RGB), as shown in Figures 11.

(a) RGB image (b) stegano (c) difference between RGB and stegano RGB

(A): RGB image

(a) red band (b) stegano Red band (c) difference between (a & b)

(B): Red band from RGB image

(a) Green band (b) stegano Green band (c) difference between (a & b)

(C): Green band from RGB image

(a) Blue band (b) stegano Blue band (c) difference between (a & b)

(D): Blue band from RGB image

Figure (11): stegano process and difference for a color digital image (A) RGB image, (B) Red band image, (C) Green band image and (D) Blue band image, From Figures (11), can be seen that the stegano process has become weak, because the image of the difference appeared more clearly than the previous methods, but despite that also note that the stegano.

Results of Statistical Quality Criteria's

Statistical criteria were calculated for the images before and after the steganography process, represented by hiding information in one row of the image with a (31)-character text message to hide 2 bits in the first and second positions of the color digital image element(pixel), as in Table (10).

Table (10): Statistical quality criteria for color images and color bands

Color images	MSE	PSNR	
Red -band	0.03963	62.14966	31 characters text massage length 2 bit
Green –band	0.03988	62.12226	
Blue-band	0.04014	62.09449	

From the results of the table (10), notice that the koala image recorded the lowest value for (MSE) and the highest value for the criterion(PSNR), which confirms that the process of information disappearance in the image with a large size is better than the image of a small size, also note that the process of hiding information in color bands is not equal, as note that the blue band is better at hiding information than red and green, and the green band is not good at hiding information because its(MSE) value is greater than the rest of the color band values(RB).

Conclusions

The Iraqi government prioritizes hiding information within images during the Arbaeen pilgrimage. The best method is to use color digital images, with larger images requiring less bit hiding and smaller message sizes. Steganography in color bands is uneven, with the best hiding in blue, red, and green bands. Hiding information in one row is better than hiding all rows. The length of the text message should match the image size. The Arbaeen pilgrimage image had minimal information hiding due to its small size and few features and colors. Steganography results with 1 bit masking are better than masking with 2 bits. The MSE for 1 bit in 14 characters is 0.0186 and PSNR is 65.4308, while if the 14 characters are inserted in all rows, the MSE is 0.03745 and PSNR is 62.4051. It means the change in the image details are changed and the is a small noise appearing in the resulting image because of the added information. The new ideas located in testing audio, video, and high text information. Then trying to adopt different methods to hide security data in Arbaeen pilgrimage. Moreover, trying different locations in the image to hide the text information.

References

1. Abbas, H. K., Al-Saleh, A. H., Mohamad, H. J., & Al-Zuky, A. A. (2021). New algorithms to Enhanced Fused Images from Auto-Focus Images [Article]. Baghdad Science Journal, 18(1), 124-131. https://doi.org/10.21123/bsj.2021.18.1.0124
2. Abbas, H. K., & Mohamad, H. J. (2021). Feature extraction in six blocks to detect and recognize english numbers [Article]. Iraqi Journal of Science, 62(10), 3790-3803. https://doi.org/10.24996/ijs.2021.62.10.37
3. Abbas, H. K., Mohamad, H. J., Al-Saleh, A. H., & Al-Zuky, A. A. (2019). Modelling vision angles of optical camera zoom using image processing algorithm. IOP Conference Series: Materials Science and Engineering,
4. Abdul, N., & Mustafa, N. (2022). An Improved Method for Hiding Text in Image Using Header Image. Wasit Journal of Computer and Mathematics Science, 1. https://doi.org/10.31185/wjcm.79
5. Al-Obaidi, F. E. M., Salman, S. S., Al-Saleh, A. H., Al-Zuky, A. A. D., & Abbas, W. A. (2023). Real-Night-time Road Sign Detection by the Use of Cascade Object Detector. Iraqi Journal of Science, 64(6), 3164-3175. https://doi.org/10.24996/ijs.2023.64.6.43
6. Al-Saedi, A. K. H. (2016). A method to hide text in image. Journal of Missan Researches, 12(24).
7. Ali, A. S., Alsamaraee, S., & Hussein, A. A. (2024). Optimize Image Steganography Based on Distinction Disparity Value and HMPSO to Ensure Confidentiality and Integrity. Journal of Computer Networks and Communications, 2024(1), 2516567. https://doi.org/https://doi.org/10.1155/2024/2516567
8. Awad, R., Al-Zuky, A. A., Al-Saleh, A. H., & Mohamad, H. J. (2018). Enhance Video Film using Retnix method. Journal of Physics: Conference Series,

9. Clemen, J. M., & Teleron, J. (2023). Advancements in Encryption Techniques for Secure Data Communication. International Journal of Advanced Research in Science, Communication and Technology, 444-451. https://doi.org/10.48175/IJARSCT-13875

10. Derea, A. S., Abbas, H. K., Mohamad, H. J., & Al-Zuky, A. A. (2019). Adopting Run Length Features to Detect and Recognize Brain Tumor in Magnetic Resonance Images. 1st International Scientific Conference of Computer and Applied Sciences, CAS 2019,

11. Habeeb, A. (2020). A New Method for Hiding Text in a Digital Image. Journal of Southwest Jiaotong University, 55. https://doi.org/10.35741/issn.0258-2724.55.2.4

12. Hassan, F. S., & Gutub, A. A.-A. (2021). Improving data hiding within colour images using hue component of HSV colour space. CAAI Trans. Intell. Technol., 7, 56-68.

13. Iacovitti, G. (2022). How technology influences information gathering and information spreading. Church, Communication and Culture, 7(1), 76-90. https://doi.org/10.1080/23753234.2022.2032781

14. Jawad, E. M., Daway, H. G., & Mohamad, H. J. (2022). Retinal Image Enhancement by using Adapted Histogram Equalization based on Segmentation and Lab Color Space [Article]. International Journal of Intelligent Engineering and Systems, 15(3), 614-622. https://doi.org/10.22266/ijies2022.0630.52

15. Khaldi, A. (2019). Steganographic Techniques Classification According to Image Format. International Annals of Science, 8, 143-149. https://doi.org/10.21467/ias.8.1.143-149

16. Kim, C., Yang, C.-N., Baek, J., & Leng, L. (2021). Survey on Data Hiding Based on Block Truncation Coding. Applied Sciences.

17. Mohamad, H. J., Hashim, S. A., & Al-Saleh, A. H. (2019). Recognize printed Arabic letter using new geometrical features [Article]. Indonesian Journal of Electrical Engineering and Computer Science, 14(3), 1518-1524. https://doi.org/10.11591/ijeecs.v14.i3.pp1518-1524

18. Muhammad, K., Ahmad, J., Farman, H., & Zubair, M. (2015). A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model. ArXiv, abs/1503.00388.

19. Mustafa, N. (2020). Text hiding in text using invisible character. International Journal of Electrical and Computer Engineering (IJECE), 10, 3550. https://doi.org/10.11591/ijece.v10i4.pp3550-3557.

20. Resham, N. H., Abbas, H. K., Mohamad, H. J., & Al-Saleh, A. H. (2021). Noise Reduction, Enhancement and Classification for Sonar Images [Article]. Iraqi Journal of Science, 62(11), 4439-4452. https://doi.org/10.24996/ijs.2021.62.11(SI).25

21. Suresh, D., & Parthasarathy, K. A. (2016). Secret data hiding with images using data compression and embedding algorithm. IIOAB, 7, 144-151.