Enhanced Data Hiding Using Some Attribute of Color Image

2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) | 979-8-3503-3752-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/HORA58378.2023.10156670

Thulfiqar Muayad Hameedi
Computer Enginering , Kirşehir Ahi
Evran University, Kirşehir,
AL-Ayen University
Turkey(Tholf_1993@yahoo.com)
ORCID: 0000-0001-8011-8524*)*

Gülsüm Akkuzu Kaya
Computer Enginering , Kirşehir Ahi
Evran University, Kirşehir, Turkey
(gulsum.akkuzukaya@ahievran.edu.tr)
ORCID: 0000-0003-1806-7759)

***Abstract*— Images are one of the most widely used multimedia in the correspondence between people, as some of the characteristics of these images can be used to hide important messages. Each image has different characteristics, and the method of concealment changes depending on the characteristics of the image used. In this research, an algorithm was proposed to increase the efficiency of the data embedding algorithm by relying on some of the characteristics of the colored digital image. First, the color image is dismantled to the basic color layers (red, green, blue). Then, the amount of variation in each layer is measured by using image processing techniques. After that, the high contrast layer is identified and used as a cover to include the message to be included, while the other two layers are used as a key to the encryption algorithm that is applied to the text before the embedding process to increase data security.The method of concealment depends on the first and second bit values in the selected layer as a cover for the embedding process. Three criteria were used to measure the efficiency of the proposed algorithm.**

Keywords— Enhanced data hiding using some attribute of color image.

I. Introduction

By concealing the existence of sensitive information within other digital material from a third party, steganography techniques make advantage of covert communication on unsecure networks, making it impossible for hackers to intercept the signal[1].

Digital media of many kinds, including text, images, audio, and video, are utilized as covers. Due to the images' enormous data volumes and the fact that changing particular bits of values has no impact on image resolution, they are frequently used as a cover-up to conceal sensitive information. The nature and type of images as well as the steganography techniques play a significant impact in defining the robustness of the steganography system, despite some restrictions in particular types of photos, such as images created using Julia Set[2].

Different ways can be used to express hidden info. Three components make up a steganographic system: the secret message, the cover media used to conceal the message within it, and the stego-cover, which is the cover utilized once the secret information has been embedded within it [3], as depicted in Figure (1-1).

The observer must not be able to detect the data that is embedded in the cover. By comparing the original image and its counterpart with embedded data to see if their visual or aural data is the same, it is possible to identify this imperceptibility. Mathematical relationships between the steganography cover and the original cover can also be used to express it. Techniques for steganography can be used in either the spatial or infrequency domain. Before the secret message is concealed within the cover medium for the frequency domain approaches, some transformations are used to change it. In contrast, no pre-processing is necessary when using spatial domain approaches because the hidden data is simply embedded inside the cover[3].

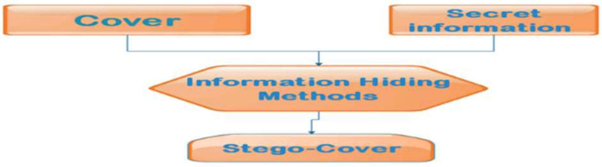


Fig 1. Inf0rmation hiding [4]

The digital image is made up of picture elements (also known as pixels) that are arranged in a two-dimensional array of numbers that represent different light intensities [5]. There are many different image types, including binary, gray, color, and multispectral images. For instance, each pixel in an RGB color image has a 24-bit binary value, with 8 bits for each color [6].

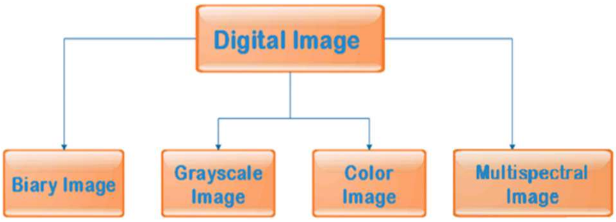


Fig 2. Types of Digital Images[5].

There are many famous routing methods, some of which

A. importance of research

The importance of the study is concealment and encryption, which are used differently to confirm the reliability of data. In encryption, any party can discover that two parties are connected in an encrypted manner. In concealing information, the existence of communication is already hidden. No one can notice two parties exchanging messages through communication channels.

The purpose of concealing information is not to prevent others from knowing or detecting hidden information, but to eliminate original suspicion of the existence of hidden information. The distinctive aspect of concealment techniques is that it keeps pace with modern technologies,

978-1-6654-6835-0/22/$31.00 ©2022 IEEE

and can be used in all computer media such as images, texts, audio, video, and network packages.

B. Research Objectives

The aim of this thesis is the growing of multimedia applications within communication networks to increase the need to provide efficient methods that protect one's own data and ownership. It is, therefore, imperative to develop means to provide security for these media to protect them from theft and intercourse from tampering, misrepresenting, or disseminating sensitive information, and hence the need for data security.

Computer concealment techniques have changed information inclusion covers. The cover is one type of electronic data file, and confidential data or information is any data or information that can be represented in the form of a series of bits or bytes.

Also used for concealment, the characteristics of parts of the operating system are as the characteristics of magnetic disk splitting and the customized physical parts configuration formula for data storage and software, such as magnetic discs and other storage circuits.

In addition, there is the possibility of using a concealment protocol (Network Traffic Package). These communities provide holders of hidden information and have issued several techniques.

II. Related Work

In recent years, the increasing applications of dealing with multimedia and the contents of the World Wide Web, have made steganography the forefront of security and confidential communication techniques.

The word steganography consists of two syllables, the first (steganos), which means covered or confidential, and the second (graphic), which means writing or drawing, together forming the term steganography [7]. Steganography can be defined as the art of concealment and data transmission through other host or carrier data. It has a carrier, and the carried data is harmless to the host or the carrier. This is conducted in a way that leaves no doubt about its possible existence [8].

Steganography can be classified into two main categories according to the type of hidden data of the secret message, namely linguistic and technical steganography.

A. Linguistic Steganography

In this type, the data carrier (steganos) is the text. One of the ancient examples of linguistic concealment dating back to ancient China is that the Chinese used to print the paper using a special template that had precise holes used to distinguish the location of the secret words in the entire text, and the recipient had to receive the same template to restore the secret message [9]. Whereas, the modern examples of this type are the tools available on the site spammimic.com, which are based on the internet that generates propaganda messages to be a cover for the secret message based on the idea that most people neglect the spam message.

B. Technical Steganography

As for this category, the carrier data is not a text but any natural medium. One of the ancient examples of pure concealment is the use of invisible ink and microdots. Among recent examples is concealment within images and sound, concealment within executable files (exe) and others [10].

There are two ways to keep things secret [11]:

The first: Placing things in a secret place with the aim that no one will find them, except for those who know that place.

The second: Assembling the appearance of things in such a way that things cannot be distinguished except by those who know the method adopted to change them from their original appearance.

The Information Hiding Techniques adopt the first method to provide information security, while Cryptography techniques depend on the second method. The Ciphertext may raise suspicion, while the hidden information is not easy to see or notice, so suspicion is not raised [12].

The word Steganography was created in 1499 by Tritheism, who coded letters composed of religious words in a way that turns secret messages into prayers with an understandable meaning. Steganography means hidden writing, while the word Cryptography means coded writing (Secret Writing) [13].

Information concealment techniques are divided into two main parts: Steganography, and Watermarking.

Steganographic techniques work on the principle of obscuring observation, making things fragmented, small, and difficult to see, or hiding information with an overflow of different information to divert attention from the intended information. It is also known as the art of concealing and sending information through clear and unimportant carriers in an attempt to hide the presence of specific data, which is also known as camouflaging information to hide its existence and make it invisible. Thus, the existence of confidential information is completely concealed [14].

In steganography, the attention is focused on the hidden information, while the digital watermarks focus at the same time on the middle of the cover and the watermarks that provide additional information about the cover [14].

In this paragraph, we present a number of studies that have been adopted in the process of hiding data with different characteristics of digital images such as color, nature of the picture or used transform coefficients [15].

In 2016, The impact of digital color systems on the data embedding procedure was discussed by a group of researchers. To test the impact of color layers on information concealment, nine color systems were utilized, and data from the least significant bit technique (mean square error and peak signal noise ratio) was included [16].A comparison study on the impact of chromatic schemes on the process of data concealing was presented by other researchers. The impact of color layers on information concealing was evaluated using five different color schemes and the least important bit approach (mean square error, signal noise ratio, and peak signal noise ratio). Other researchers presented a study on the use of strategies to conceal information by watermarking specific areas of a picture and utilizing the least important bit method when embedding information in data. When two photos are secreted and used as a cover sample using a contourlet transform based approach, other contourlet transform coefficients are used to hide the images while other images are used as cover. The low energy coefficients are then employed after calculating the energy of the transform coefficients. There are other other studies that employ images as their covers as well[17-26].

III. Methodology

A. . Main Points Functional of Proposed Method

The suggested work's primary goal is to improve the images as one of the most widely used multimedia in the correspondence between people, and some of the characteristics of these images can be used for hiding important messages. Each image has different characteristics, and the method of concealment changes depending on the characteristics of the image used by combining several functional points which are:

1. growing growth of multimedia applications on communication networks to increase the need to provide efficient methods that protect one's own data and ownership.

2. developing means to provide security for these media to protect them from theft, intercourse and tampering, misrepresenting or disseminating sensitive information, and hence the need for data security.

3. The embedding procedure should produce a stego image that satisfies un-detectability criteria such the visual imperceptibility and the PSNR measure, making it less likely to be detected.

4. By comparing the data bit pair and the decoy bit pair in each bite, locate the bytes of the secret picture that have been modified in case an attack is identified.

B. Region of Interest Image

For image analysis, we typically want to look into a certain region of the image termed the region of interest more closely (ROI). This requires operations, known as image geometry operations, that change the spatial coordinates of the image. The operations on picture geometry that are covered here include (Crop, Zoom, Enlarge, Shrink, Translate, Rotate).

The image crop process involves choosing a tiny area of the image, often known as a sub-image, and separating it from the remainder of the image. Enlarging a sub-picture that has been cropped from the original image allows us to focus in closer. There are several techniques to execute the zoom process:

1-ZeroOrder Hold: is performed by repeating previous pixel values, thus creating a blocky effect.

Original Image Array

$$\begin{bmatrix} 8 & 4 & 8 \\ 4 & 8 & 4 \\ 8 & 2 & 8 \end{bmatrix}$$

Image with Rows Expanded

$$\begin{bmatrix} 8 & 8 & 4 & 4 & 8 & 8 \\ 4 & 4 & 8 & 8 & 4 & 4 \\ 8 & 8 & 2 & 2 & 8 & 8 \end{bmatrix}$$

In zero order hold, the output image size is double the original image size.

$$\begin{bmatrix} 8 & 8 & 4 & 4 & 8 & 8 \\ 8 & 8 & 4 & 4 & 8 & 8 \\ 4 & 4 & 8 & 8 & 4 & 4 \\ 4 & 4 & 8 & 8 & 4 & 4 \\ 8 & 8 & 2 & 2 & 8 & 8 \\ 8 & 8 & 2 & 2 & 8 & 8 \end{bmatrix}$$

(2n * 2n), which (n x n) is the dimension of image.

2-First Order Hold: is carried out by determining the average value between two pixels and using that as the pixel value between those two, and by determining linear interpolation between adjacent pixels. For the first rows, we can accomplish it as follows:

Original Image Array

$$\begin{bmatrix} 8 & 4 & 8 \\ 4 & 8 & 4 \\ 8 & 2 & 8 \end{bmatrix}$$

Image with Rows Expanded

$$\begin{bmatrix} 8 & 6 & 4 & 6 & 8 \\ 4 & 6 & 8 & 6 & 4 \\ 8 & 5 & 2 & 5 & 8 \end{bmatrix}$$

The average of the first two pixels in the first row (8+4)/2=6) is used to place this value between those two pixels. Every pixel pair in every row receives this treatment.

Next, take the results and expand the columns in the same way as follows: Image with rows and columns expanded.

$$\begin{bmatrix} 8 & 6 & 4 & 6 & 8 \\ 6 & 6 & 6 & 6 & 6 \\ 4 & 6 & 8 & 6 & 4 \\ 6 & 5.5 & 5 & 5.5 & 6 \\ 8 & 5 & 2 & 5 & 8 \end{bmatrix}$$

This method allows us to enlarge an N×N sized image to a size of (2N-1) × (2N-1) and is repeated as desired.

3- Convolution: is a technique for mathematically enlarging images.

This method requires two steps:

1. Extending image by existing rows and columns are separated by rows and columns of zeros.

2. Performing the convolution.

Image is extended as illustrated :

Original Image Array

$$\begin{bmatrix} 3 & 5 & 7 \\ 2 & 7 & 6 \\ 3 & 4 & 9 \end{bmatrix}$$

Image extended with zeros

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 5 & 0 & 7 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 7 & 0 & 6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 4 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Next, at each pixel point, we carry out straightforward arithmetic operations using a convolution mask, which is a slide through the enlarged image.

IV. RESULTS

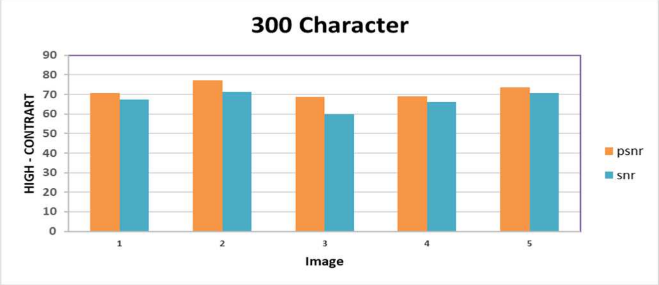
As for Table 1, a set of high-resolution images are used. These are encrypted by the concealment algorithm and encrypted information within the images as shown in the first image. The number of characters used are (500100 ،200 ،300 ،400 ،), respectively. The output results (PSNR, SNR) are slightly higher than their images which are of medium resolution. This indicates that the larger the image size the better the concealment and encryption process is. A number of only (5) images are used to obtain more conclusions.

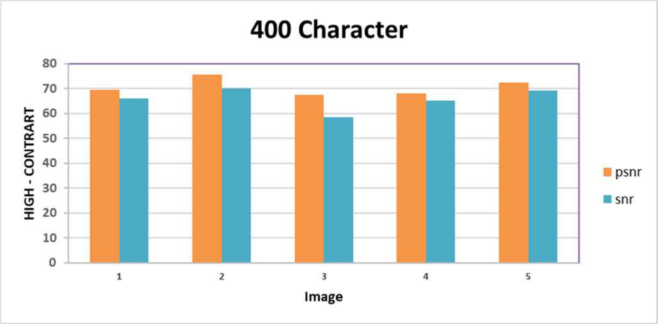
The algorithms were applied to a set of high-resolution images: Table 1. A group of (5) images

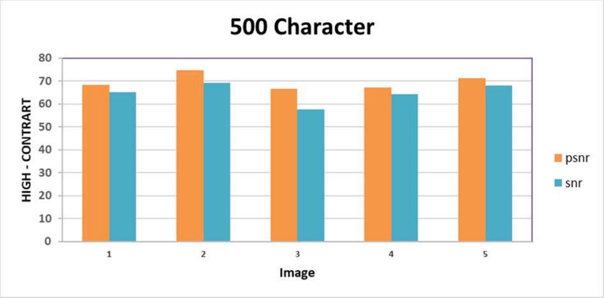
Image	No. Character	HIGH - CONTRART	
		psnr	Snr
Image 1	100	95.2174	83.2355
	200	91.9788	79.9969
	300	90.4911	78.5092
	400	89.1057	77.1238
	500	88.2255	76.2436
Image 2	100	96.2857	89.6811
	200	93.1995	86.5949
	300	91.4999	84.8953
	400	90.3423	83.7378
	500	89.3135	82.7089
Image 3	100	80.4693	67.7740
	200	77.6356	64.9403
	300	75.7332	63.0379
	400	74.5361	61.8408
	500	73.6116	60.9163
Image 4	100	80.0720	73.9271
	200	76.9622	70.8173
	300	75.2626	69.1177
	400	74.0851	67.9402
	500	73.0157	66.8708
Image 5	100	87.2203	76.7082
	200	84.1087	73.5966
	300	82.4615	71.9494
	400	81.2868	70.7747
	500	80.3420	69.8299

a. Result Charts (psnr, snr)

The results of the following charts are compared in Table (4-1) with the number of (5) images and (psnr, snr) values. In each chart shows the values of the characters within the image are divided into five graphs according to the characters worked on in the current study which are (500 400 300 200 100).







V. CONCLUSION

Using the steganography technique, the work in this thesis has presented a security enhancement strategy to safeguard confidential information that is encoded in cover images. The approach was implemented in accordance with(MATLAB 2020).

This is evident from the study of the proposed system and through the application of the system to a different set of images and different lengths of texts to be hidden.

Although the images have been used in different sizes, formats and lengths, this has not affected the proportional relationship between the number of characters within the digital images and the values (psnr, snr).

By comparing the results obtained for (psnr) per image, it is shown that there is a high difference when applying (100,200) characters within the image, but this difference decreases when applying (300,400,500) characters within the image.

This applies to snr results, and these conclusions apply to all 15 images.

By comparing images when using the encryption algorithm with a fixed number of 100 characters, we note that the values of psnr results change. The change is due to the characteristics of images from one to the other in terms of size, accuracy and dimensions.

1- All that was the size of the image used as a large cover the better the results because the data to be included will not clearly affect the image used as a cover.

2- Relying on colored images in the embedding process is better than relying on grey-graded images because the color image data is more than grey image data.

3- The inclusion process, if preceded by an encryption process, is stronger because if the unauthorized party is able to know the method used in the inclusion process, the encryption problem will be encountered and the security of this information will be increased.

4- Adopting keyword on photo layers is better than adopting a fixed key.

References

[1] Abdullah. Muhammad, "Hiding the Text in Image of Variable Size", Diyala Journal for Pure Science, Volume: 11 Issue: 2 Pages: 44-55,2015.

[2] Ahmed S. Abdullah." Text Hiding Based on Hue Content in Hsv Color Space ", International Journal of Emerging Trends & Technology In Computer Science (Ijettcs), Volume 4, Issue 2, March-April 2015.

[3] Ahmed Saadi Abdullah." Improving Message Embedding by Using Some Attributes of Color Image", Raf. J. of Comp. & Math's., Vol. 13, No.2, 2019.

[4] Ali Fattah Dakhil," Steganography: Applying LSB Algorithm to Hid Text in Image", Journal of AL-Qadisiya for computer science and mathematics Vol.9 No.1 Year 2017.

[5] Ali Nasser Hussain, Enricher MH awes Zghairb," Efficient Text Message Hidden Technique Using YIQ Model", JOURNAL OF MADENAT ALELEM COLLEGE, Volume: 9 Issue: 1 Pages: 217-228, 2017.

[6] Allen Tom, Anu V Thomas, Jerin Jose, Maria, P. Darsana," Hiding Host Image using a Cover Image", International Journal of Engineering Research & Technology,2015.

[7] Alyaa Hasan Zwiad," Proposal Compression Algorithm to Hide Multiple Text Images Based on Bit Plane Slicing", Iraqi Journal of Information Technology. V.8 N.4. 2018.

[8] Amer A. Al-Lehi be," Ciphered Text Hiding in an Image using RSA algorithm. Of College Of Education For Women, volume 26, issue 3 , 2015.

[9] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh," Steganography in Images Using LSB Technique, International Journal of Latest Trends in Engineering and Technology,2015.

[10] Ashwini Palimkar, Dr.S.H. Patil," Using SBR Algorithm to Hide the Data into The JPEG Image",

[11] Ayman Mudheher Badr, &Mohamed laythtalal and Ghassan Sabehc," Image in Image Steganography based on modified Advanced Encryption Standard and Lest Significant Bit Algorithms", Journal of University of Babylon for Pure and Applied Sciences. (26), No. (8): 2018.

[12] Azal Habeeb," A NEW METHOD FOR HIDING TEXT IN A DIGITAL IMAGE", JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, Vol. 55 No. 2,2020.

[13] Deepali Singla and Dr. Mamta Juneja," New Information Hiding Technique using Features of Image", JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 6, NO. 2, MAY 2014.

[14] Deepesh Rawat, Vijaya Bhandal, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Volume 64– No.20, February 2013.

[15] Dr. Yossra H. Ali Ahmed Y. Yousif Tayseer S. Atia," Distributed AMELSB Replacement Method for Text Hiding",", Iraqi Journal of Information Technology, volume 2, issue 2, 2018.

[16] Falih Hassan Owaid," INFORMATION HIDING USING STAGAEROGRAPHS SYSTEM USING LSB-TECHNIQUE", Journal of Baghdad College of Economic sciences University, Issue: 38 Pages: 376-394, 2015.

[17] Abbood, Z. A., Yasen, B. T., Ahmed, M. R., & Duru, A. D. (2022). Speaker identification model based on deep neural networks. Iraqi Journal For Computer Science and Mathematics, 3(1), 108-114.

[18] shaker, A. S., & Ahmed, S. R. (2022). Information Retrieval for Cancer Cell Detection Based on Advanced Machine Learning Techniques. Al-Mustansiriyah Journal of Science, 33(3), 20-26.

[19] Yaseen, B. T., Kurnaz, S., & Ahmed, S. R. (2022, October). Detecting and Classifying Drug Interaction using Data mining Techniques. In 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 952-956). IEEE.

[20] Abdulateef, O. G., Abdullah, A. I., Ahmed, S. R., & Mahdi, M. S. (2022, October). Vehicle License Plate Detection Using Deep Learning. In 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 288-292). IEEE.

[21] Ahmed, S. R., Sonuç, E., Ahmed, M. R., & Duru, A. D. (2022, June). Analysis survey on deepfake detection and recognition with convolutional neural networks. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-7). IEEE.

[22] Ahmed, S. R. A., & Sonuç, E. (2021). Deepfake detection using rationale-augmented convolutional neural network. Applied Nanoscience, 1-9.

[23] Ahmed, M. R., AHMED, S. R., DURU, A. D., UÇAN, O. N., & BAYAT, O. (2021). An expert system to predict eye disorder using deep convolutional neural network. Academic Platform-Journal of Engineering and Science, 9(1), 47-52.

[24] Al Barazanchi, I., Abdulshaheed, H. R., Jaaz, Z. A., Gheni, H. M., Niu, Y., Almutairi, H., ... & Ahmed, S. R. (2022, June). Blockchain: The Next Direction of Digital Payment in Drug Purchase. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-7). IEEE..

[25] Alkaragole, M., Karim, S. M., & Ahmed, S. R. (2021, July). A New Approach To Study The Challenges Of E-Learning Advantages And Disadvantage. In Journal of Physics: Conference Series (Vol. 1963, No. 1, p. 012135). IOP Publishing.

[26] AHMED, S. R. A., Najm, I. A., Abdulqader, A. T., & Fadhil, K. B. (2020, November). Energy improvement using Massive MIMO for soft cell in cellular communication. In IOP Conference Series: Materials Science and Engineering (Vol. 928, No. 3, p. 032009). IOP Publishing.