



New Technique to Encryption and Embed Secret Messages Based on Lightness Layer in Color Model and Image Processing Methods

Nayif Mohammed Hammash¹

Computer science department, Collage of computer and mathematics science, Tikrit University, Iraq
ahmedalbasha@tu.edu.iq

Mohammed Waleed Nofan²

Computer science department, Collage of computer and mathematics science, Tikrit University, Iraq
ahmedalbasha@tu.edu.iq

Ahmed S. Abdullah³

Computer science department, Collage of computer and mathematics science, Tikrit University, Iraq
ahmedalbasha@tu.edu.iq

ABSTRACT

One of the most important topics seeks to develop algorithms previously or through the discovery of other algorithms that help maintain secret data that has great importance and which the sender seeks not to be discovered by any person who is not authorized to access it, in this article is provided Proposed by digital photo processing methods in increasing the efficiency of this proposed method and at the same time the nature of a non-known chromatic system for many people trying to identify hidden data through the knowledge of the most commonly used ecosystems such as green, red and blue chromatography system, the algorithm have been implemented Suggested on many different images with different nature as well as different texts are included after converting these ports to a binary representation, after applying this algorithm has relied on many criteria that can measure the efficiency of the algorithm were PSN, MSE, and the results of the algorithm force Used.

Keywords:

Information hiding, Image processing, security, color space, YCbCr color space

1. Introduction

The process included important messages from the subjects of many consequences, the important messages differ in nature, where these messages can be sent and abandoned by any unreliable person to these messages where these messages can be texts or Sometimes these messages can be a meaningful image or sometimes a video may be included in these secret messages that have a high value and there is no one for anyone from the link only to this information only authorized to access it. The cover used to include confidential information is a picture or a video clip as well as some texts can be incorporated into other texts but

whenever the data size in this large cover is better in the currency to include data because the process will be easier and compact in discovery. [1,2,3]

Digital image processing is any digital image process, there are many processes that can be used as part of enhance the concealment of information. A digital image such as improved contrast or improve surfaces for the digital image [3]. The coloring system for digital images is the declaration of the image where there are many color systems that can be represented by the color of the most famous these systems is RGB as this chromatic system consists of three basic layers is the green and blue layer as well

as the red The most famous color systems used in digital images in this chromatic system are all pixels in the picture consisting of 24-bit and each layer of these three layers contain 8-bit, in addition, there are many other color systems such as HSI, HSV HSV YCBCR[4].

The oldest way of steganography was introduced by the Greeks back in 440 BC. It was initiated by shaving the hair head of the person who will send him to the destination after they wrote a message on his head then waiting for hair growing up to send him to their allies without the enemy knowing. Furthermore, in the US revolution, invisible ink has been used for hiding critical messages. this technology was also used by the German army in both world wars. [5,6]

At present, steganography became not enough for guaranteeing arrival data and important information to its destination. Steganography is applied with cryptography techniques for enhancement and increasing security so that the keeping significant messages from any attacks. Cryptography indicates all encryption and decryption processes. The main idea of cryptography is to protect the message by writing it incomprehensible configuration and then sending it to the recipient. [7]

This article will be divided into a set of departments and the second section shows many previous studies that are currently in the same research field. YCBCR). The fourth section of this article will submit the proposed algorithm in this article for each step that has been adopted in the process of including these important messages, which are difficult to access, either section fifth are displayed through the experiment using a length Different and at the same time rely on images of different nature either the last section will present a range of conclusions that are reached through the results that are indicated by analyzing the results reached as well as can offer a range of future businesses that can be used before A group of researchers either to develop this system or take advantage of some ideas in producing another system [8]

2. Related work

In 2015, an article relies on the colored digital image in the process of confidentiality insurance where the chromatic system has been converted from the RGB system to another chromatic system which is the HSV chromatography, where the three layers are dismantled for this chromatic system and then use the HUE color layer and then use Choose specific areas within this layer and include confidential texts within this layer and then these layers are reinstated and the chromatography is returned to the RGB [10].

In 2016, a group of researchers made a study compared to the adoption of the color image with different color systems and as a cover in hiding the information where the digital image system was converted from RGB into other coloring systems and thus dismantled these colored systems to the cordial layers and then be included in the eighth bit or is included dependable on the seventh bit and then the digital image is returned to the original chromatic system and then the impact of the nature of the chromatic system is studied on the process of inclusion of the important texts, but this article is missing on how to rely on some colored image properties and then can be increased Confidentiality of the inclusion process as well as no means of processing digital image processing methods in order to increase the efficiency of confidential texts[11]

In 2017, an article was presented that relies on the color image and in the RGB color system, where all layers in these color systems are relied upon, which gives you a large space in the embedding process because the data is now all available in the image, which is better than relying on one layer of the layers color picture[12].

In 2017, he also presented articles based on a color scheme other than RGB, where the process begins with the process of converting the color system from RGB to the YIQ system, as well as another article in the same year that relied on another color system, which is the YUV color system after the conversion to this color system and from Then the secret data is included in these layers after these texts are converted into numbers in the binary system by knowing the

ASCII code and after the embedding process is done using the least significant bit algorithm and then re-left the image and then the image is converted to the original image system[13].

In 2018, the color image with the basic red, blue and green color layers were relied upon, as well as the reliance on artificial intelligence algorithms in the data embedding processes. In fact, the images that are relied upon in the masking process and that were relied on as a cover is in the spatial domain [14].

In 2019, some digital image properties were relied on in order to increase the efficiency of the processing of messages in color digital images where some image properties are studied as the amount of contrast in the image and thus choose any better layer among the classes in chromatography and thus The least decisive method relies on the process of including but this system relies on the most common chromatography is the RGB chromatography and this system and the nature of this system may be known by many attackers so it was better converted to another chromatic system more mystery For attackers[15] also presented an article in 2021, a way to include confidential data through the use of images of cucumber leaves for the process of including this confidential data . In fact, the use of such types of images is better because the process of sending and receiving such images does not raise suspicion and therefore a person can only be the trusted person who is suspicious of the

images that are sent and that are relied upon as a cover in the embedding process [16].

3. Digital Image And Color Space

In general, the digital image represents the digital image in the computer in the form of a two-dimensional matrix, which represents the dimensions of the image. In addition, each element in the image is known as a pixel. In each type of digital image, the number of bits used to represent the pixel is differentiated from one type of image to an image. Others where the number of bits in the black and white image is 1 bit per pixel. Therefore, the storage space that can be used to store this type of image is small. The second type of image is the grayscale image[16] In this type of image, the number of bits that It is used to represent each pixel in this type of image, which is z bits, and therefore the number of colors that can be given in this type of image is 256. Therefore, the storage space needed by this type is more than that of images that are black and white, equivalent to eight times as much as the black and white image if it is The dimensions of the image are the same as the dimensions of the black and white image, but in the color image the number of data is three times the data in the grayscale images because this type of image consists of three color layers and each layer of These layers are a grayscale image, and as it is known, the higher the cover data, the better the data embedding process. Figure (1) shows the types of digital images[15].

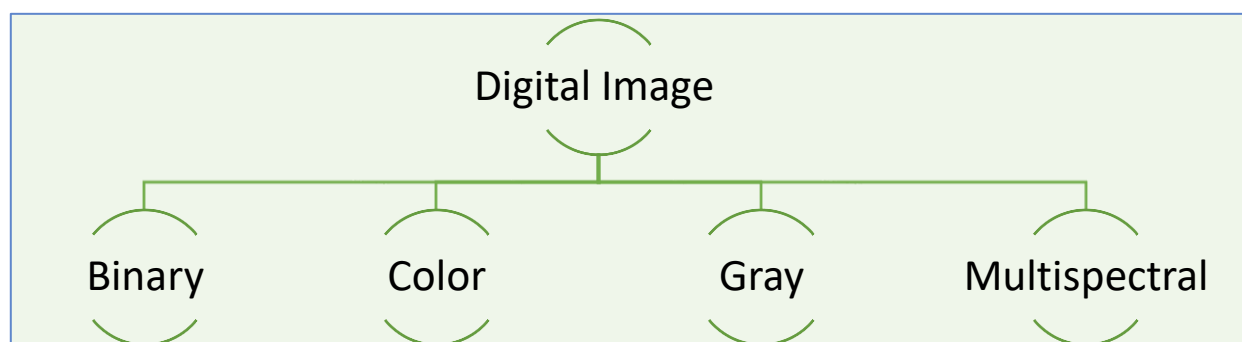


Figure 1. Digital image types

The colored image requires 24 bits to represent because it is made up of three layers of color, each of which involves 8 bits to represent, resulting in a total of 16777216 colors [15].

As for the color systems in which a digital color image can be represented, the most common color system used in color digital images is the RGB color system, which in general consists of three basic layers: the red color layer, the blue layer, and the green color layer, and each of

these layers is each pixel. In the image, it represents 8 bits, and therefore the total number of bits that the digital image represents is 24 bits. The color system used in this article is YCbCr, and in this system also it consists of three layers. Figure (2) shows the difference between the two shapes YCbCr color space contains the image's Y as luminance, Cb as blue difference, and r as re difference[16].

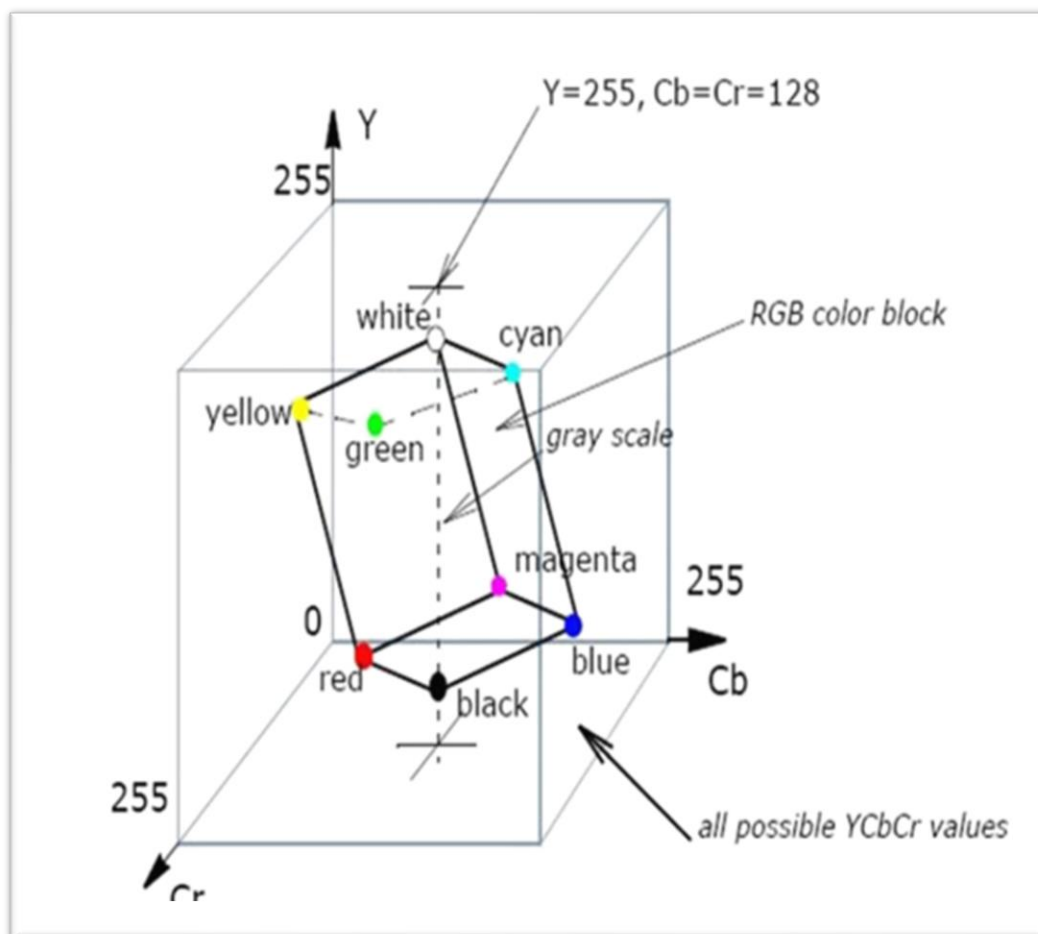


Figure 2. RGB cube and YCbCr cube Relationship

4. Proposed Algorithm

The algorithm used in this work consists of three phases: -

- **First phase:** Reading the image that will be used as a cover in the hiding process, the reading operation is either from the images in the database or captured directly using cameras, or the video clips can be relied upon

after dismantling the video into a group of frames.

- **Second phase:** in this stage, the color system of the image is converted from the YCbCr to RGB color system, this conversion is very important because the color system depends on the three main colors red, green, and blue are more famous than other systems. Therefore, the experience in this system is less

than in the first system figure (3) show image in different color spaces.



Figure 3. image in RGB and YCbCr color space

- **Third phase:** The division of this color scheme is broken down into the basic layers. The lighting layer is used as a cover in the masking process, while the other layers are used to hide

the key used to encrypt the text to be hidden within the image, figure (4) shows the basic layer of Ycbcr color space

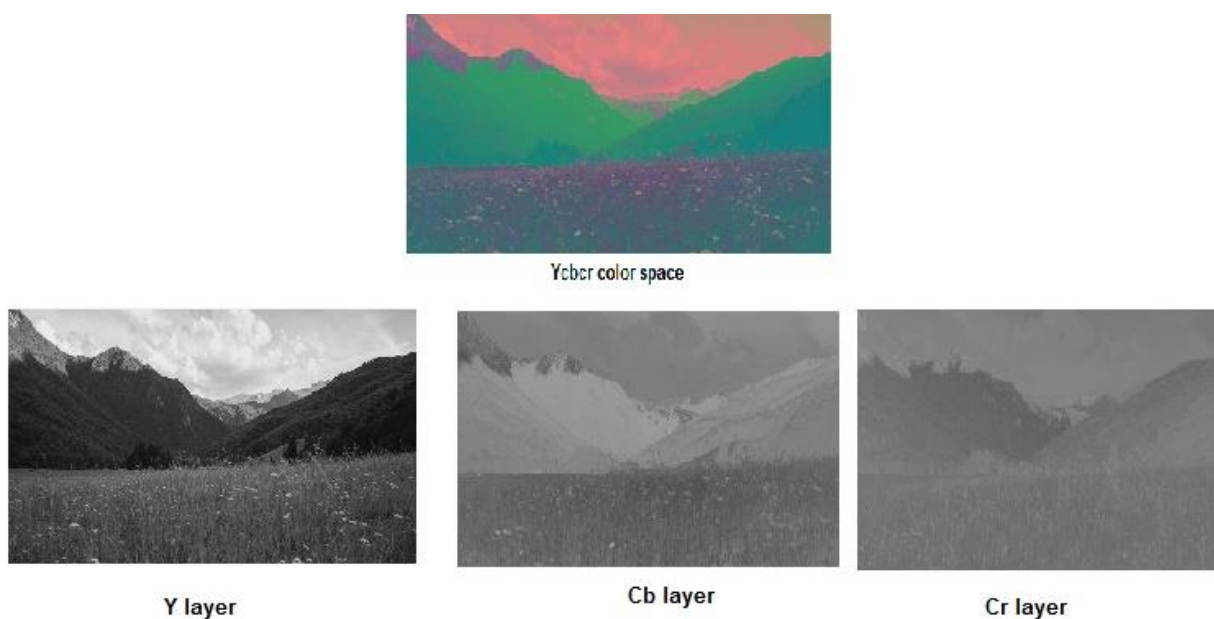


Figure 4. basic layer of Ycbcr color space

- **Fourth phase:** The text to be hidden is read and then encrypted using an encryption algorithm and the key used in the encryption process is included in the Cr, Cb layers. Where the text to be included within the image is read, and then these characters are converted based on the ASCII code, and then these numbers are converted into binary numbers,

but before this process, the important information is encrypted through encryption based on a private key for each word, where the value in The two layers cb and cr are in the first position of each of these layers and then choose the largest value and consider it a key in the encryption of the first word. One key in the embedding process, but each word of the

text to be hidden has its own key, and therefore even if any password is decrypted, this means that the rest of the words cannot be discovered because the key used is different from this key.

- **Fifth phase:** At this step, the hidden text has been included in an inventive approach that

involves taking five pixels, calculating the highest value from among these five, and then using that value to include the hidden text. However, if there are multiple pixels with the same value, the first value from the left side is chosen, figure (5) shows the embedded process.

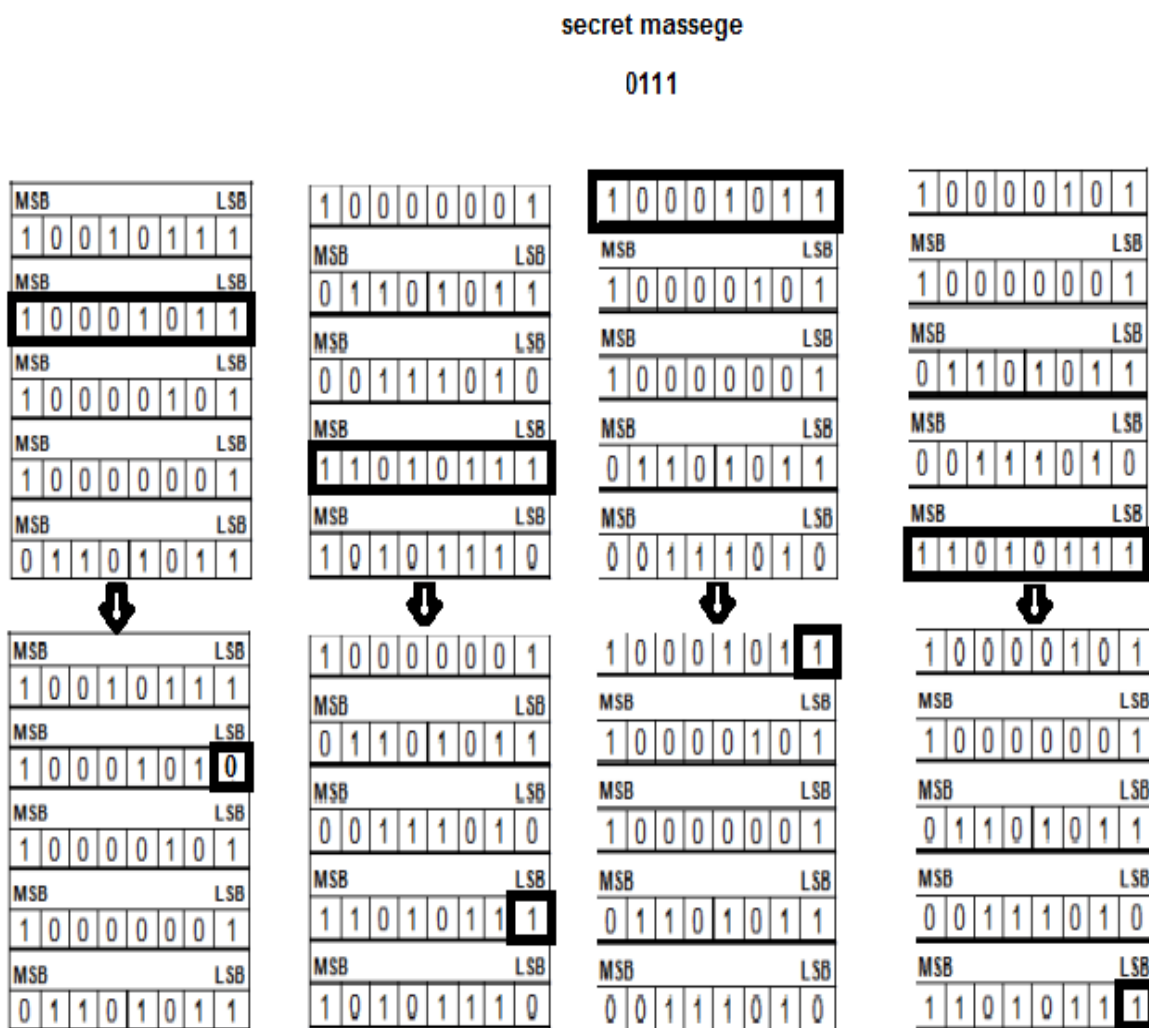


Figure 5.a. choose maximum values between five pixels

The second word is taken from the lowest value between five pixels, i.e. the opposite of the first word, and so the process continues in succession

secret massege

1001

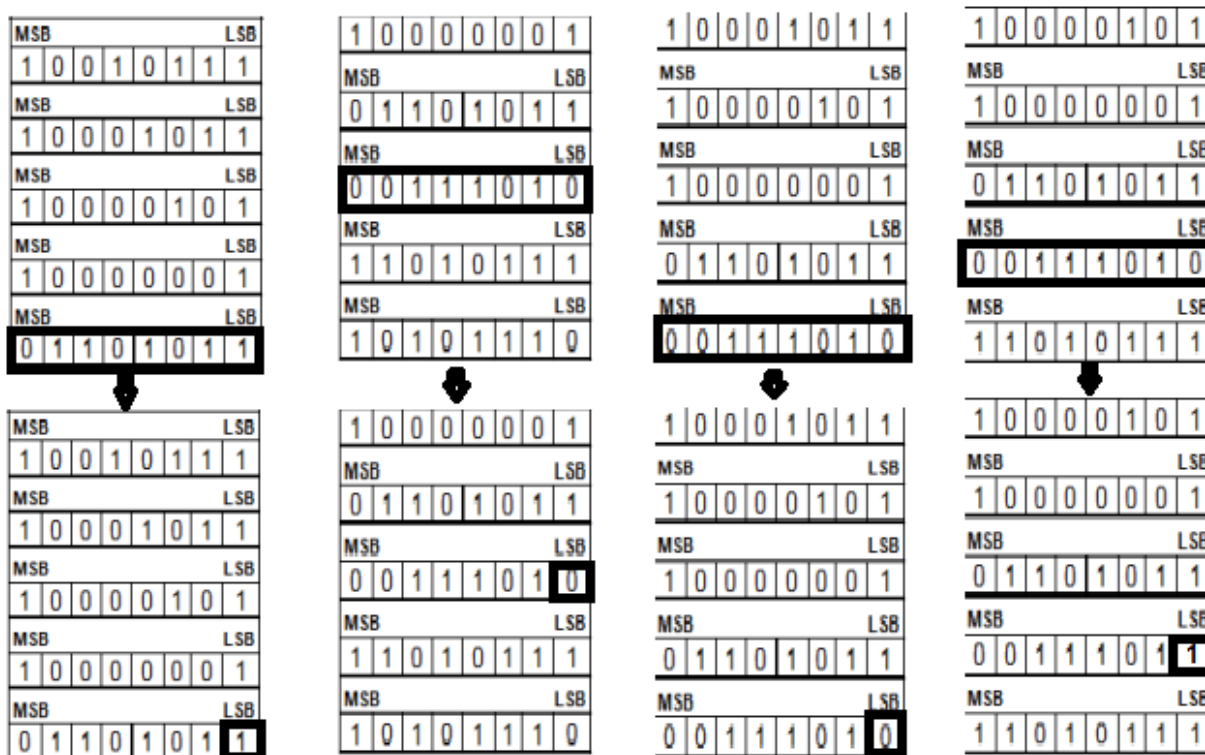


Figure 5.b. choose minimum values between five pixels

- **Sixth phase:** The layers are recombined and then the colored system is converted to the original colored system thus the criteria used to measure the efficiency of the algorithm are applied. Figure (6) show how to return the image to rig the final color space



Figure 6. convert Ybcr to Rgb

5. Result

When employing the proposed algorithm, it was based on varied text lengths and different nature types of images as a cover. The results of applying this technique on the lighting layer as a cover, while the other layers were employed to hide the key, are shown in the line charts below.

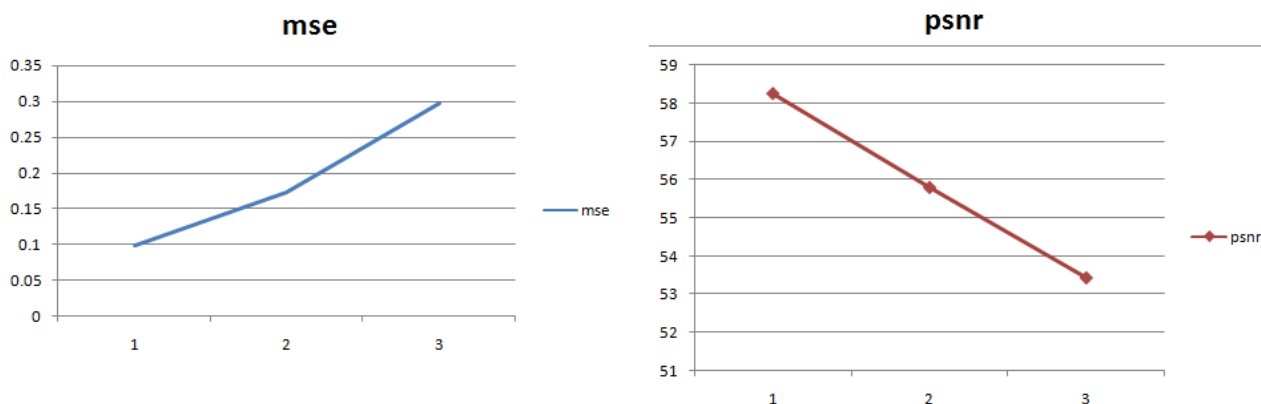


Figure 7.a. result when the size of image 400*400

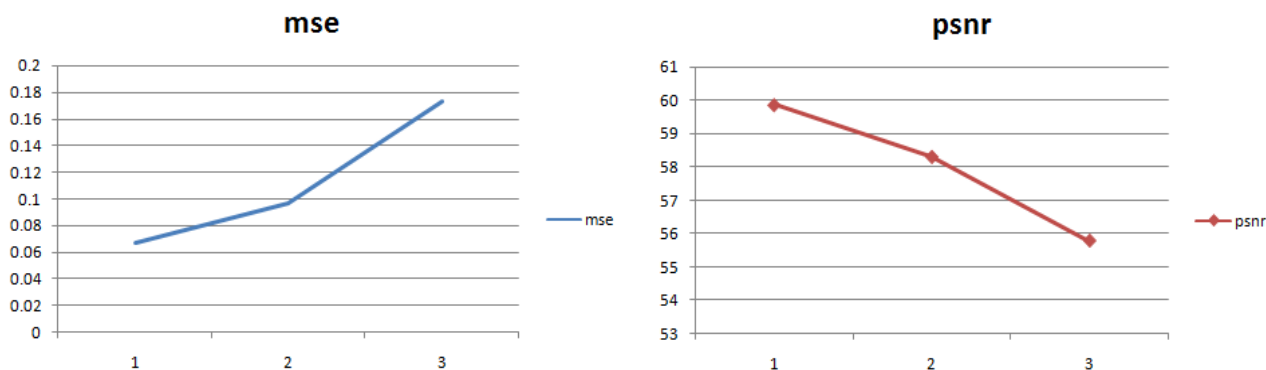


Figure 7.b. result when the size of image 700*700

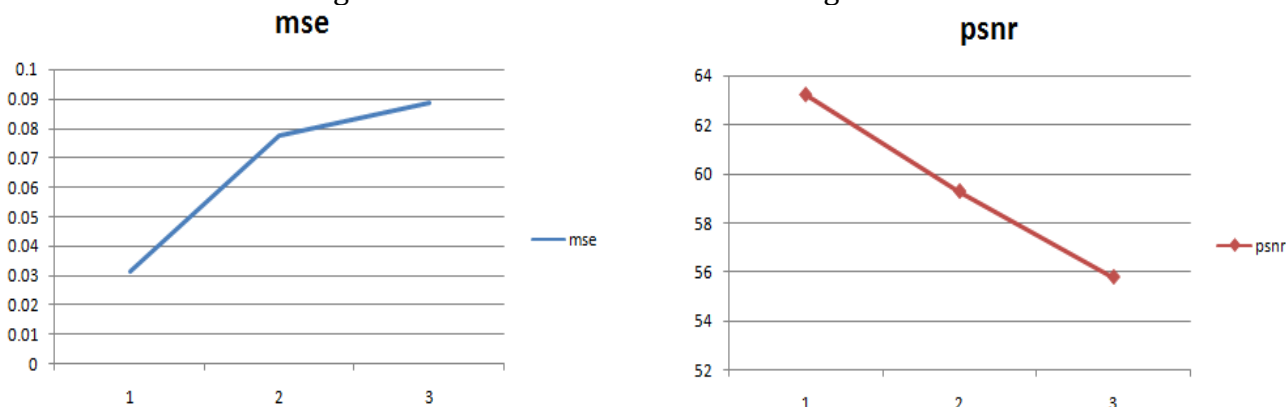


Figure 7.c. result when the size of image 1200*1200

when noted the line charts that the algorithm is applied to images of different nature, as well as texts of different lengths were included. It was

also noted that texts with shorter lengths were better than texts with larger lengths and vice versa, as the larger the image used in the

embedding process, the better the output from embedding in a small image.

6. Conclusion

Relying on less popular color schemes than the original red, green and blue color system will be secure because these color systems are less defined in the properties of this color. furthermore, the image will be returned to the original color system and therefore it is difficult to infer that the image was originally hidden in another color system.

Important criteria were relied on to measure the efficiency of the algorithm, and the application proved that relying on a large image is better than relying on images of small sizes, because the space that will be available to include the data is large and the results in the process of including short texts are better than embedding large texts. In addition, the process of encrypting the text before hiding it will give higher security to the data because the intruder, even if he was able to obtain the image and discover the method of embedding and then access the text, there will be protection for this text, because the text has been encrypted, especially the key used in the embedding process has been hidden, which it gives strength to the algorithm.

7. References

1. P. Roy and A. Nath, "New Steganography approach using encrypted secret message inside Audio and Video media," 2014.
2. K. Muhammad, J. Ahmad, H. Farman, and M. J. a. p. a. Zubair, "A novel image steganographic approach for hiding text in color images using HSI color model," 2015.
3. A. M. Al-Shatnawi, "A new method in image steganography with improved image quality," *Applied Mathematical Sciences*, vol. 6, no. 79, pp. 3907-3915, 2012.
4. A. Kumar and S. Khurana, "Steganalysis Technique on Gray scale Image by Varying Message Length using Adaptive Histogram Equalization Attack," *International Journal of Computer Applications*, vol. 90, no. 14, 2014.
5. A. Singh and S. Malik, "Securing data by using cryptography with steganography," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 5, 2013.
6. C. Patvardhan, P. Kumar, C. J. M. T. Vasantha Lakshmi, and Applications, "Effective color image watermarking scheme using YCbCr color space and QR code," vol. 77, no. 10, pp. 12655-12677, 2018.
7. A. Dixit and R. Dixit, "A review on digital image watermarking techniques," *International Journal of Image, Graphics and Signal Processing*, vol. 9, no. 4, p. 56, 2017.
8. A. s Abdullah, "Saturation Component In HSB Color Space With Image Processing Methods To Enhanced Image Segmentation," in *IOP Conference Series. Materials Science and Engineering*, 2020, vol. 928: IOP Publishing.
9. D. Hema and D. S. Kannan, "Interactive color image segmentation using HSV color space," *Science and Technology Journal*, 2020.
10. 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
11. Qasim Mohammed Hussein, Hiding Message In Color Image Using Auto Key Generator, 3rd International Conference On Advanced Computer Science Applications And Technologies. 2014
12. Qasim Mohammed Hussein, Ahmed Saadi Abdullah, Nada Qasim Mohammed," The Efficiency Of Color Models Layers At Color Images As Cover In Text Hiding", *Tikrit Journal Of Pure Science* , Vol. 21, No. 1, Pp. 130-139, 2016
13. Nagham S. Al-Lella , Khalil I. Alsaif ." Data Hiding In Contourlet Coefficients Based On Their Energy", *J. Of University Of*

- Anbar For Pure Science : Vol.6:No.2 : 2012.
14. Ahmed saadi Abdullah¹ and Qasim Mohammed Hussein," Using Digital Image as a Cover of Information Hiding: Review Paper",IOP Conference Series: Materials Science and Engineering,2020.
 15. Ahmed S. Abdullah," Using Cucumber Plants Leaves A Cover To Hiding Encryption Text
16.",IOP Conference Series. Materials Science and Engineering; Bristol
 17. M. Waleed, A. S. Abdullah, and S. R. Ahmed, "Classification of Vegetative pests for cucumber plants using artificial neural networks," 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), Sep. 2020.

Acknowledgment

We are thankful and highly appreciate the staff of the Computer and Informatics Center at Tikrit University for their cooperation and contribution to accomplishing and considering this study.