Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

Steganography Technique for Embedding a Variety of Binary Images inside a Grayscale Image

Huda Dheyauldeen Najeeb

Department of Public Relations,University of Al Iraqia, Baghdad, Iraq.Email: huda_iraq81@yahoo.com

ARTICLE INFO

Article history:
Received: 07 /05/2020
Rrevised form: dd /mm/year
Accepted : 13 /06/2020
Available online: 10 /07/2020

Keywords:

Binary Images, Grayscale images, Embedding , Least Significant Bit (LSB), Mean Square Error(MSE) and Peak Signal to Noise Ratio(PSNR).

ABSTRACT

Because of the rapid development and use of the Internet as a communication media emerged to need a high level of security during data transmission and one of these ways is "Steganography". This paper reviews the Least Signification Bit steganography used for embedding a variety of related binary images in a single grayscale image rather than traditional methods of embedding information which is embedded one image in another image (cover image). First three images represent the secret images which are used for hiding from unauthorized users while other images used for making more difficult and more secret watermark. In this paper, we have merged both methods of hiding and watermark. Instead of either creating a watermark or hiding secret data in a grayscale image, we can use both of them at the same image to take advantage of both the hiding and watermark properties at the same time. The findings of the research were the results as a new watermark composed of multiple related binary images and hidden secret multiple binary images inside.

https://doi.org/10.29304/ *jqcm.2020.12.2.694*

1. Introduction

Although encryption is a good way to protect information, but it is easy to detect and can be manipulated by an intruder. The need for more sophisticated, more confidential and data-intensive technology, especially with the emergence and evolution of the Internet, Seeing encrypted data is enough to push a hacker or an attacker to believe that important or sensitive data exists in random or encrypted text. He starts using cryptographic techniques to try

∗Corresponding author : ***Huda Dheyauldeen Najeeb***

Email addresses: *huda_iraq81@yahoo.com*

Communicated by : ***Alaa Hussein Hamadi***

to obtain their content. Even if he fails to do so, he may tamper with them, distort them or use some means. Available To prevent and reached its target[1,2].

Steganography is an effective way to protect sensitive data from unauthorized users which is a method of protection that makes incoming and outgoing data invisible by hiding certain messages within a particular cover[3]. The objective of the concealment process is not to raise any doubt about the existence of hidden data. Steganography includes four different types are: text files steganography, image steganography, video steganography and audio steganography [4].

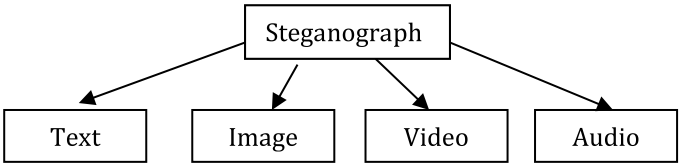


Fig. 1- Types of steganography

Image steganography which is a method or technique to hide data within a digital image, so as to hide the existence of any contact or exchange of information into a cover media and is not aware of this contact only the persons concerned.

Watermark is a new security field whose role is to verify the consistency of digital information spread through various means of transmission of information. The watermark can be created by adding text or an image to the original image for protecting moving images or the static digital image from theft or hacking.

Digital images are divided into the many types: binary Images, grayscale images, and color images. The images represented by one byte for each point with grayscale gradients are suitable for hiding, because when changes in values are less pronounced and less discriminated by the human eye.

In this paper, we have been proposed a new method for a combination between both hiding and watermark methods. Instead of either creating watermark or hiding secret data in a grayscale image, we can use both of them at the same image to take advantage of both the hiding and watermark properties at the same time. The watermark using to achieve the legitimacy, reliability, integrity of data and ownership marks, control determinants, content protection while the hiding aims to hide the data completely from unauthorized users .

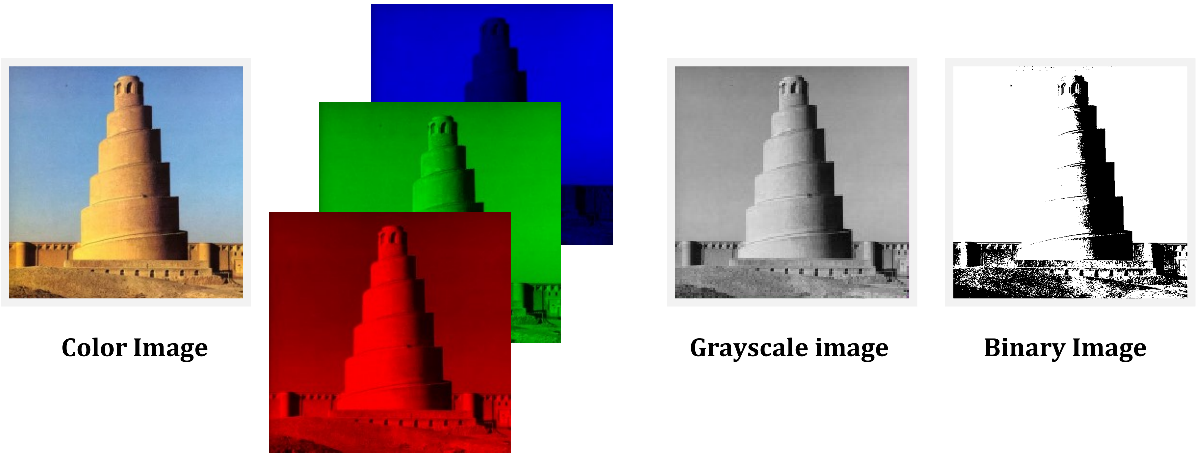
2. Related Works

Over the past years, information security has become the focus of many researchers who are trying to find new solutions, technologies and ideas that ensure the safe transfer of information through the network, especially the Internet, without interference. As a result, there are many techniques and methods currently used in information security. In this article we will highlight some ways to protect information. Vijay [5] proposed a new algorithm of steganographic which is based on logical process for embedding MSB of secret image in to LSB of cover image which resulted in a significant improvement with lower computational complexity. Kamlesh, et al. [6] presented a new schema for hiding secret image inside the image which contains two algorithms. The first algorithm for encrypting the secret image through the Triple-DES algorithm. Second algorithm for hiding the encrypted image in the original image through the LSB algorithm. This schema has been compared with the previous schema. The result of Kamlesh's schema is more secure than Vijay's schema. Mahdi, et al. [7]. designed proposed system is to hide image in image by using discrete cosine transformation method (DCT) and discrete wavelet transformation method (DWT) and Least Significant Bit (LSB). The system will embed the (input) secret image color inside a cover image color the secret image apply it discrete cosine transformation method (DCT) and the cover image is decomposing into four parts (LL, LH, HL, HH) by using discrete wavelet transformation method (DWT) and the secret image hidden in the part (HH) in segment Least Significant Bit (LSB) of cover image, and produce (output) stego image. And uses the stego key for extraction the data hidden (secret image) from stego cover through use the process embedding inverse. Manikandan, et al.[8] proposed a new approach for hiding a secret image in the image by using the Least Significant Bit (LSB). This approach splits the secret image into several blocks and converts them to cipher image through applying pixel transformation and embedded them in the original image by LSB to create stego image which will be sent in the insecure channel. Huda [9]suggested a new technique of watermark image which used Bit Plane Slicing for embedding Cubic-spline interpolation inside the grayscale image. The researcher enabled to embed two Cubic-spline interpolations in the image. Hewa [10] presented a new method for making a watermark image that depended on properties of the Mojette Phantoms and the Mojette Transform. His result gets a difficult watermark through hiding special information in the original image. Most of the offered works that are relevant to our research did not embed several images, it was embedded one image inside another image and did not merge both methods of hiding and watermark, but in this paper, both of them are successfully embedded inside a single image.

3.Types of images

Digital images are divided into the following types:

- Binary Images is the simplest types of images are black and white or symbolized by zero or one. The binary image can be referred to as 1bit per pixel.
- Grayscale images are the second type of digital images that contain light information only. No color information. Grayscale images with Monochrome or One Color Image are included. They contain only brightness information , each image contains 8 Bit / Pixel (1Byte) to represent each element in it, that is, it allows 256 levels of illumination from 0 (black) to 255 (white)[11].
- Color images: A group of colors that are recognized by the human eye and are simply produced by adding percentages of basic colors (red, green and blue). These colors are known as basic colors. All colors can be formed by combining these three colors. Each color represents by (1Byte), therefore the color image is represented by (3 Byte) .This explains why the size of color images is bigger compared to the previous[12].



Color Image **Grayscale image** **Binary Image**

Fig. 2- Types of images

4.Techniques used to hide data inside images:

4.1. Least Significant Bit Insertion(LSB)

One of the most technologies which are important, more famous and easy to implement. The LSB is a simple and common method which used with steganography for embedding secret data (hiding) in to the least significant bits of the pixel values in a Cover image[13,14].

Suppose the first eight pixels of the Cover image are:

11010010 00100111 11101001 11101000 10000001 01010111 11101001 01000011
11001000 01001010 10010111 11101001 00100110 00010101 00100110 00100111

After hiding the message "Hi" whose binary value is 01001000 01101001, by LSB the values of these pixels become:

11010010 00100111 11101000 11101000 10000001 01010110 11101000 01000010

11001000 01001011 10010111 11101000 00100111 00010100 00100110 00100111.

4.2. *Masking and Filtering*

The hide process is performed by filtering and blocking similar to the watermark. A watermark is not hide process but rather an extension of image information and includes a feature of the cover file which is used to guarantee property rights[14,16].

5.Calculation of quality measures Method:

Assessing the performance of a particular method based on human vision is ambiguous and inaccurate because it depends on the person's experience and vision system has but is reliable to prove the success or failure of the method, so it is supported objective evaluation methods for leading the quality of the method used.

There are several methods used for measuring the quality, some of these are:

a) Mean Square Error and Peak Signal to Noise Ratio

PSNR is the most widely used objective image quality metric. it defines simply through MSE which must be as small as possible between the reconstructed image and the original image with maintaining the quality of reconstructed image which would be near to the original image. Given Image X which is n×m monochrome with noisy approximation Y. Is defined as follows:

$$\mathrm{MSE} = \frac{1}{nm}\sum_{i=o}^{n-1}\sum_{j=0}^{m-1}[X(i,j) - Y(i,j)]^2$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right)$$

Where MAX is the maximum possible pixel value of the image. Get it from this equation 2B-1, where B is the value of bits.[9]

b) Structured Similarity Index (SSIM).

$$\mathrm{SSIM}\ (x, y) = \frac{(2\,\mu_x\,\mu_y + C_1)\,(2\,\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_x^2 + C_1)\,(\sigma_x^2 + \sigma_x^2 + C_2)}$$

$$C_1 = (k_1 * L)^2\ ,\ C_2 = (k_2 * L)^2$$

Where μ_x is the mean of x
μ_y is the mean of y
σ_x is the variance of x
σ_y is the variance of y
σ_{xy} is the covariance of x and y
L is the maximum gray level
k_1 and k_2 are 0.1 and 0.3 respectively by default [17].

The value of SSIM is between -1 and 1.

6.Proposed Method

The proposed work is embedding multiple related binary images in one grayscale bitmap images to get a new image which is considered a new way for merging both hiding and watermark methods.

In this work, first, we take a grayscale image and convert it to an 8-bit stream, then embed a bitmap image in each bit of it to get a new image (Stego image) which is embedded 8 binary images. Three binary images from them use for hiding secret images which can be retrieved from Stego image while other images used for creating a watermark.

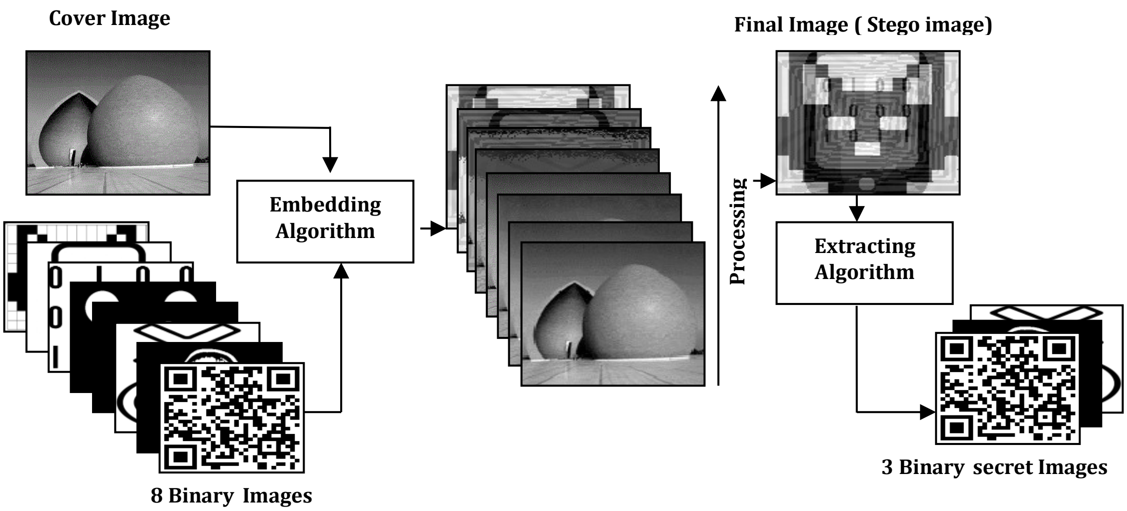


Fig. 3- Proposed System

Algorithm (1) : Embedding 8 binary images in grayscale bitmap image

Input : Cover image and 8 Binary images.
Output : Final(Stego) image.

```
Convert Cover image to 8-bit stream.
Normalize all this images.
For i ←1 to Cover image size
    For j ←1 to binary image1 size.
        Stego1(i,j) = CoverImage(bitNo1)
        Calculate MSE and PSNR between Cover and Stego1 image.
    For j ←1 to binary image2 size.
        Stego2(i,j) = CoverImage(bitNo2)
        Calculate MSE and PSNR between Cover and Stego2 image.
    For j ←1 to binary image3 size.
        Stego3(i,j) = CoverImage(bitNo3)
        Calculate MSE and PSNR between Cover and Stego3 image.
    For j ←1 to binary image4 size.
        Stego4(i,j) = CoverImage(bitNo4)
        Calculate MSE and PSNR between Cover and Stego4 image.
    For j ←1 to binary image5 size.
        Stego5(i,j) = CoverImage(bitNo5)
        Calculate MSE and PSNR between Cover and Stego5 image.
    For j ←1 to binary image6 size.
        Stego6(i,j) = CoverImage(bitNo6)
        Calculate MSE and PSNR between Cover and Stego6 image.
    For j ←1 to binary image7 size.
        Stego5(i,j) = CoverImage(bitNo7)
        Calculate MSE and PSNR between Cover and Stego7 image.
    For j ←1 to binary image8 size.
        Stego6(i,j) = CoverImage(bitNo8)
        Calculate MSE and PSNR between Cover and Stego8 image.
Convert the result to the decimal value that will generate a Final image.
```

Algorithm (2) : Extracting 3 Binary secret images from Stego image

Input : Stego image.
Output : 3 Binary secret images.

```
Convert Stego image to 8-bit stream.
For i ← 1 to  Stego image size.
        Secret1(i,j) = StegoImage(bitNo1)
        Secret2(i,j) = StegoImage(bitNo2)
        Secret3(i,j) = StegoImage(bitNo3)
Convert the result to decimal value for getting Secret images.
Return the secret images.
```

7.Results and Discussion

This work has been implemented in MATLAB 2013a. We used grayscale image "Baby" as the cover image, then convert it to 8-bit stream .In figure.3 we can see that a grayscale image "Baby" is considered as a combination of eight bit-planes where each bit-plane can be represented by a binary matrix. Plane 1 contains the lowest order bit of all the pixels in the image, while plane 8 contains the highest order bit of all the pixels in the image[18].

Eight related binary images of personal information (Name, Work, Code, Horoscope, Scary animal, Play, Country, Phone) embedded in each bit of Baby image respectively.

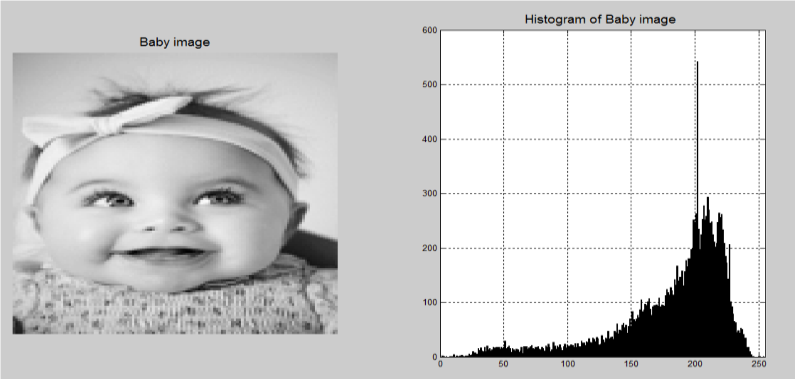


Fig. 4- Baby image with its histogram

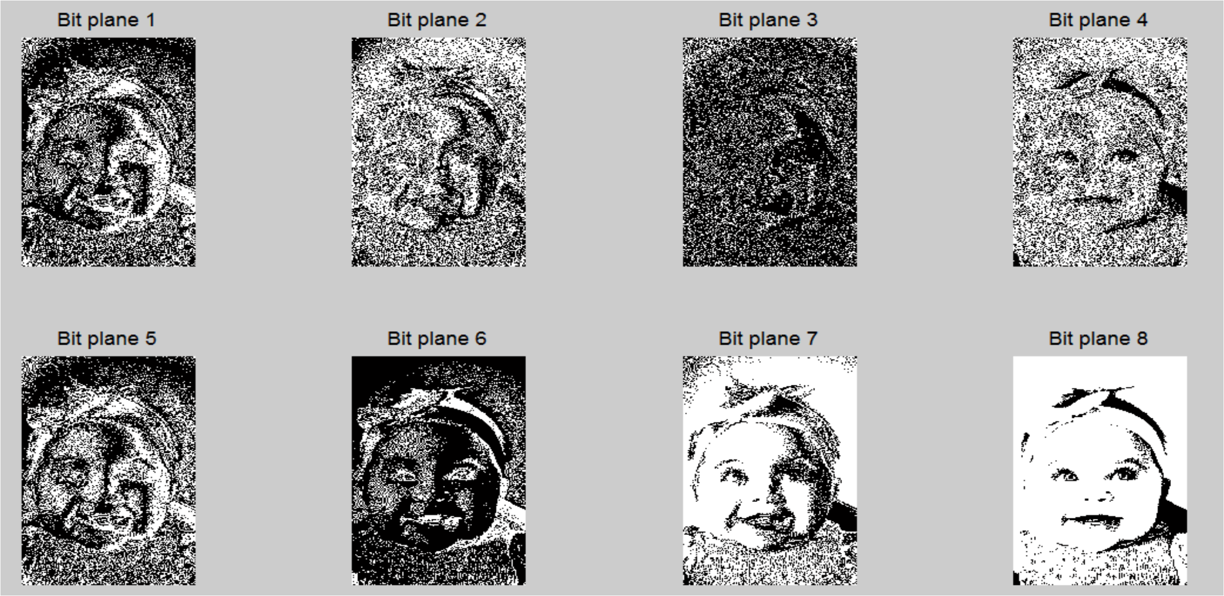


Fig. 5- a grayscale image "baby"

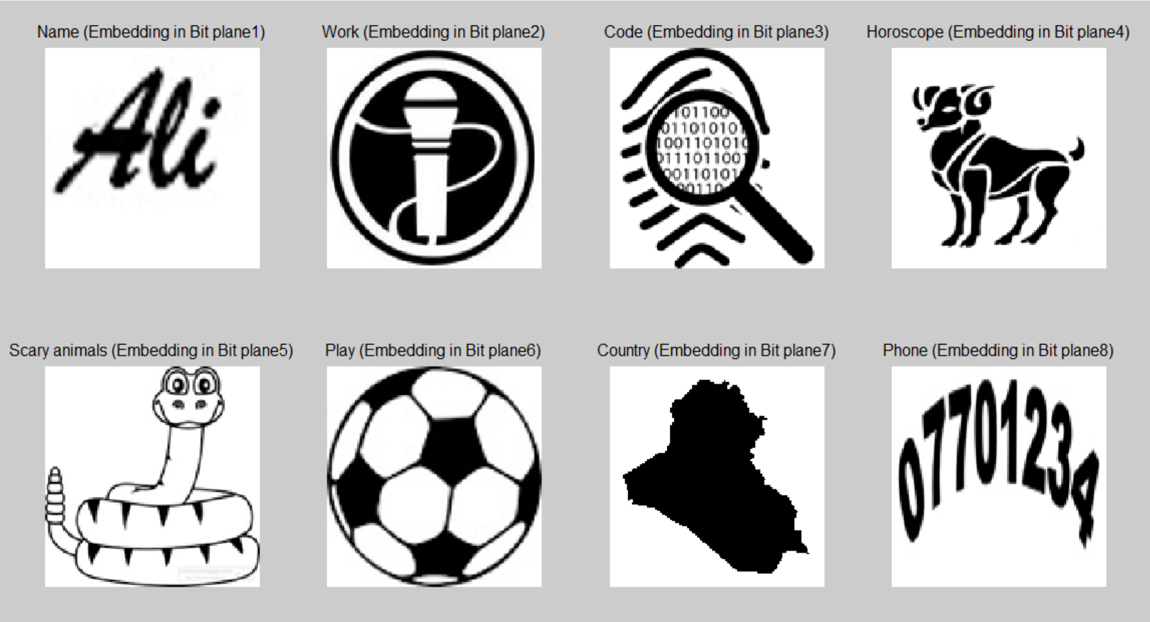
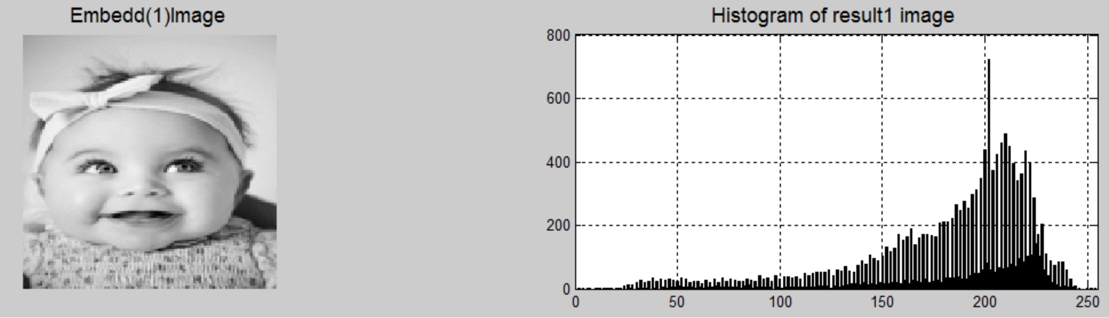
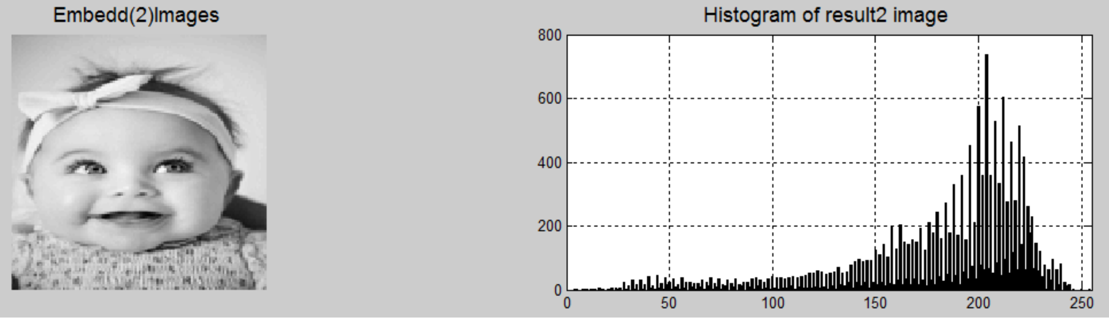
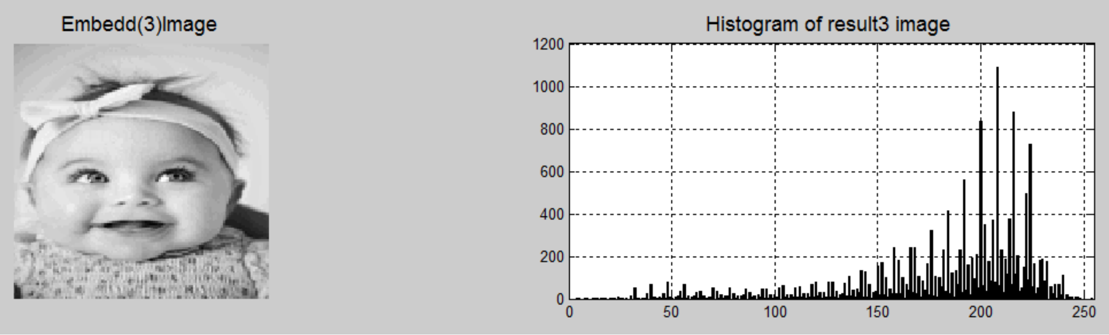

Name (Embedding in Bit plane1)
Work (Embedding in Bit plane2)
Code (Embedding in Bit plane3)
Horoscope (Embedding in Bit plane4)
Scary animals (Embedding in Bit plane5)
Play (Embedding in Bit plane6)
Country (Embedding in Bit plane7)
Phone (Embedding in Bit plane8)
Ali
07701234

Fig. 6- Eight related binary images of personal information







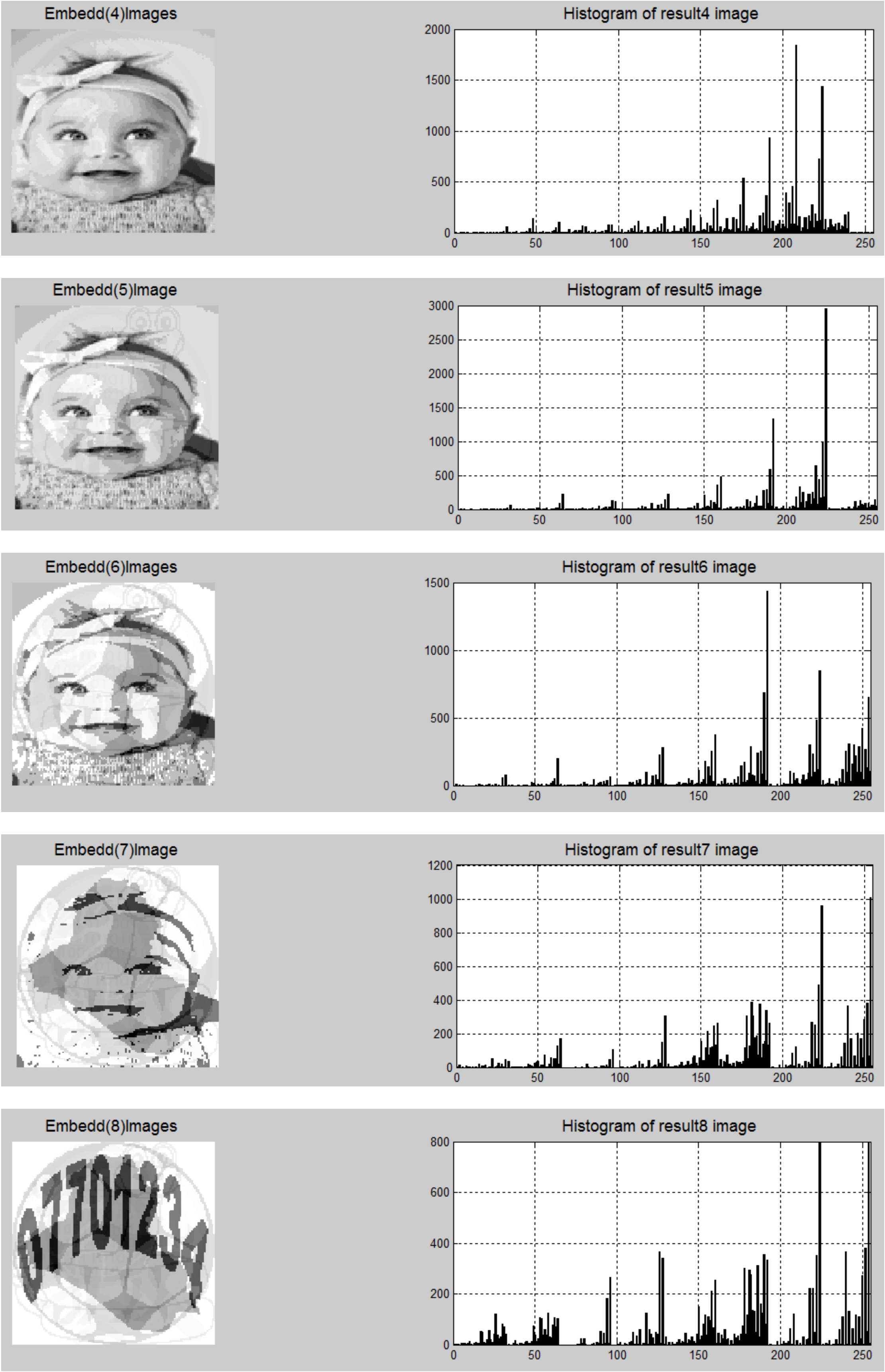


Fig. 7- Embedding eight related binary images of personal information a grayscale image "baby"

From figure .7, We can analyze the result into three categorized:

First categorized: First three related binary images have been embedded successfully in grayscale bitmap image in bits (1,2,3). We cannot recognize between the input image (cover image) and output image (stego image) by eye. The PSNR and MSE value is calculated to determine image quality before and after the data embedding. This categorized used for hiding a secret image from unauthorized users. Figure.8 shows that the secret image was extracted successfully from stego image.

Second categorized: From bit 4 can be used in making more difficult and more secret watermark which contains a variety of related binary images.

Third categorized: The Baby grayscale bitmap image has converted into 8 binary images.

Table 1: MSE and PSNR obtained different between the original image (Baby) and the final image .

The number of bit plane which will be hide in	MSE	PSNR
1	0.49036	**51.2257**
2	2.6547	**43.8907**
3	12.498	**37.1624**
4	24.018	**34.3254**
5	53.596	**30.8391**
6	95.181	**28.3453**
7	251.99	**24.1169**
8	624.06	**20.1785**

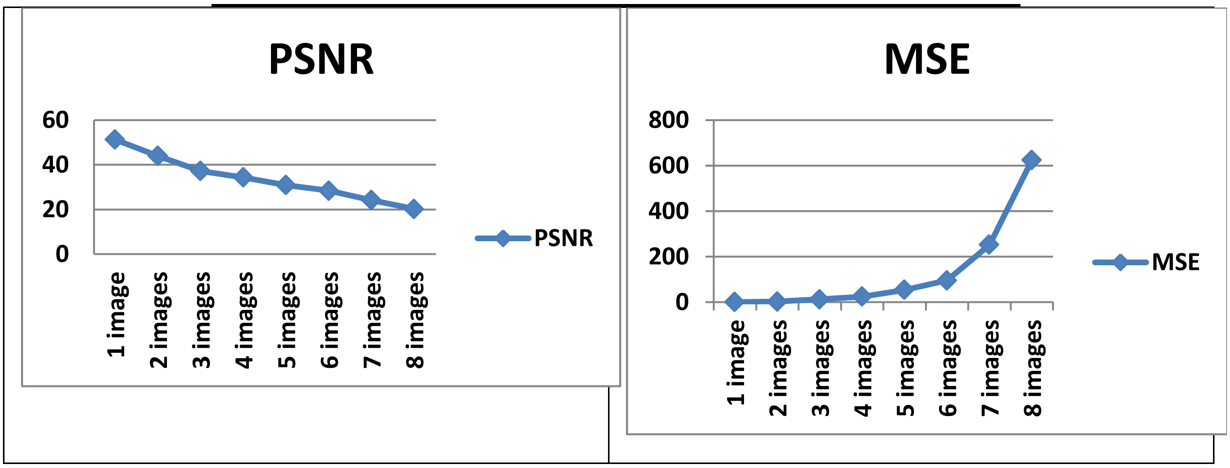
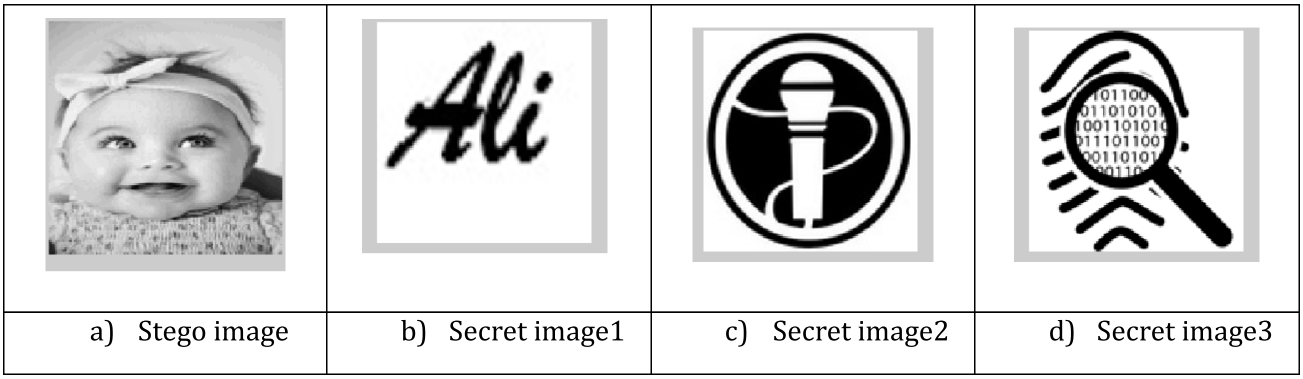


Chart .1- MSE and PSNR obtained different between the original image (Baby) and the final image .



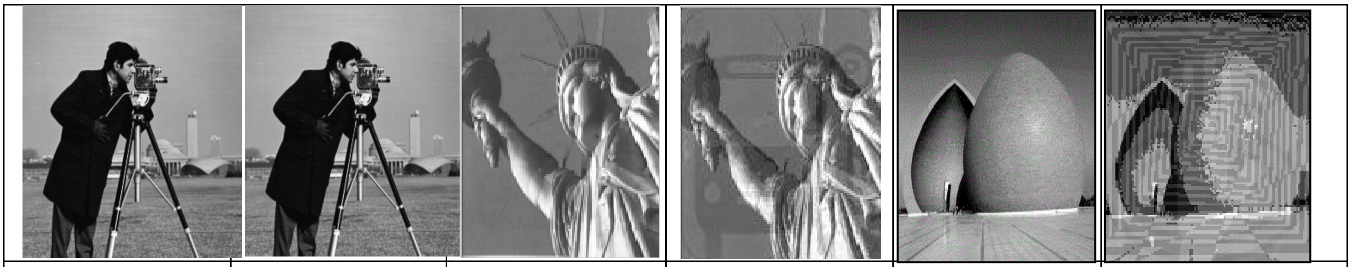
a) Stego image b) Secret image1 c) Secret image2 d) Secret image3

Fig. 8- Extracting three related binary images of personal information from Stego image

This work is implemented successfully, thus we can:

- Create a watermark only by embedding one or more images (from bit 4 to bit 8).

- Hide one, two, or three secret images (from bit 1 to bit 3).
- Combine the two previous ways.



a) Original image

b) Stego image hiding two secret images.

c) Original image

d) Creating watermark from embedding one image.

e) Original image

f) Creating watermark from embedding three images as well as hiding three secret images.

Fig. 9- Result of algorithm when applied in several images.

Table 3: Comparable Our Result with Related Work

Year	Name of researcher	Method	Result
2012	Vijay and others	Most Significant Bit (MSB) and Least Significant Bit (LSB)	Hiding one secret image in the original image.
2014	Kamlesh and others	Triple DES algorithm and Least Significant Bit (LSB)	Hiding one secret image in the original image.
2014	Mahdi and others	discrete cosine transformation method (DCT) and discrete wavelet transformation method (DWT) and Least Significant Bit (LSB)	Hiding one secret image in the original image.
2019	Manikandan and others	Least Significant Bit (LSB)	Hiding one secret image in the original image.
2019	Huda	Bit Plane Slicing	Creating watermark through hiding one or two Cubic-spline Interpolation in the original image**.**
2020	Majeed	Mojette Transform	Creating watermark through hiding special information in the original image**.**
2020	Our proposal	Least Significant Bit (LSB)	1) Creating a difficult watermark through embedding one or more related binary images in the original image**.** 2) Hiding one or more secret images in the original image. 3) Using both methods (hiding and watermark)

8. Conclusion

Steganography is the art of writing hidden messages while watermark is a shadow image with changing in darkness/lightness of the image. In this work, we have merged both methods of hiding and watermark to take advantage of both the hiding and watermark properties at the same time through emedding various binary images which embedded in any bit in Tiff or Jpg grayscale bitmap image when the values of bit equal 4 or more MSE becomes bigger while PNSR becomes smaller. Finally, we conclude that the proposed approach gives a new technique for a combination between both hiding and watermark methods. We can get an image which is hiding multiple sensitive binary images and at the same time create a difficult watermark which is created from multiple related binary images.

References

[1] C. Chin,C. Jun, and C. Yu," Spatial Domain Image Hiding Scheme Using Pixel-Values Differencing", *Fundamenta Informaticae*, vol.70, (2006), pp.171–184.

[2] P. Kusuma, and A. Archana, " Techniques and analysis for Image Watermarking using Inverted Bit planes and coding", *International Journal of Electrical, Electronics and Computer Systems (IJEECS)*, vol.4, (2016) , pp. 80- 86, doi: 10.17148/ IJEECS.2016.51288.

[3] D. Abhay, and B. Sanjay ," A Review on Image Steganography Techniques", *International Journal of Advanced Research in Computer and Communication Engineering*, vol.4, (2015) , pp. 24-26, doi: 10.5120/ijca2015905280

[4] N. Reyadh ,S. Ahmed , and A. Sadeq ," Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation", *International Journal of Computer Science and Network Security*, vol.15, (2016) , pp. 16-18.

[5] K. Vijay, and S. Vishal, " A Steganography Algorithm for Hiding Image In Image By Improved Lsb Substitution By Minimize Detection", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.36, (2012), pp. 1-12.

[6] K. Lakhwani, and K. Kumari," KVL Algorithm: Improved Security & PSNR for Hiding Image In Image Using Steganography ", *International Journal of Computational Engineering Research*, vol.3, (2014), pp. 1-6

[7] A. Mahdi, A. Khidhir, and M. Hussein, " Image in Image Steganography based on DCT", *Iraqi Journal of Science*, vol.55, (2014), pp. 1675-1684.

[8] G. Manikandan, R. Bala, E. Preethivi, K. Sekar, R. Manikandan, and J. Prassanna, " An Approach with Steganography and Scrambling Mechanism for Hiding Image over Images ", *International Journal on Emerging Technologies*, vol.10, (2019), pp. 64-67.

[9] D. Huda, "New Techniques of Watermark Images using Bit Plane Slicing and Cubic-spline Interpolation", *Ibn AL-Haitham Journal for Pure and Applied Science*, vol. 23, (2019), pp. 192-200.

[10] H. Majeed, "Watermarking Image Depending on Mojette Transform for Hiding Information ", *International Journal Of Computer Sciences And Engineering*, vol.8, (2020), pp. 8-12, doi: 10.26438/ijcse/v8i1.812

[11] S. Mamoun , "Colored Image-In-Image Hiding", *International Conference CAD Systems in Microelectronics IEEE Xplore* ,(2008).

[12] R. Deepesh, and B. Vijaya , "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", *International Journal of Computer Applications*, vol. 64,(2013), pp.15-26,doi: 10.5120/10749-5625.

[13] D. Huda, and T. Israa ," A proposal of Multimedia Steganography Algorithm based on Improved Least Significant Bit (LSB) Method", *Iraqi Journal of Science*, vol.58,(2017), pp. 2188-2199, doi: 10.24996/ ijs.2017.58.4B.22.

[14] J. Mekha ," Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality", *International Journal of Science and Research*, vol.3, (2014), pp. 2281-2284.

[15] H. Faheem, and U. Rizwan," Embedding Multiple Images in an Image Using Bit Plane Slicing" , *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.3, (2013), pp. 327-335.

[16] A. Mahdi, A. Khidhir, and M. Hussein," Image in Image Steganography Based on DCT", *Iraqi Journal of Science*, vol.55, (2014), pp. 1675-1684.

[17] G. Kieran ," Structural Similarity Index SSIMplified", *Occasional Texts in the Pursuit of Clarity and Simplicity in Research*, vol.1, (2015).

[18] D. Mayukh, " An Effective Method to Hide Texts Using Bit Plane Extraction" , *Journal of Computer Engineering*, vol.17, (2015), pp. 17-23.