ARTICLE

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.30; No.4.| 2022

# Review on Common Steganography Techniques

Noor Kadhim Ayoob [1*], Asraa Abdullah Hussein [2]

1College of Science for Women, University of Babylon, noor.kadhum@gmail.com, Babylon, Iraq,
2College of Science for Women, University of Babylon, esraa_zd@yahoo.com, Babylon, Iraq

*Corresponding author email: noor.kadhum@gmail.com

# مراجعة تقنيات إخفاء المعلومات الشائعة

نور كاظم أيوب , اسراء عبدالله حسين

| Received: | 30/1 /2022 | Accepted: | 16/10/2022 | Published: | 31/12 /2022 |
|---|---|---|---|---|---|

## ABSTRACT

Various authorities are keen to preserve the confidentiality of their information and protect it from competing or hostile parties who were also keen to access that information by all available means. Since the encryption of information is exposed as it produces incomprehensible texts that arouse suspicion, some tend to work in a way that removes suspicions by hiding the information in a medium like text or picture so that what is sent and circulated appears natural and free of signs or incomprehensible symbols as if not loaded with any additional information. This paper introduces a review the techniques used to hide data in images as one of the most common concealment techniques.

Keywords: Image, Steganography, DCT, LSB, PSNR.

## الخلاصة

تحرص الجهات المختلفة على الحفاظ على سرية معلوماتها وحمايتها من الأطراف المتنافسة أو المعادية التي حرصت أيضًا على الوصول إلى تلك المعلومات بكافة الوسائل المتاحة. بما أن تشفير المعلومات ينكشف لأنه ينتج نصوصًا غير مفهومة تثير الشك، يميل البعض إلى العمل بطريقة تزيل الشكوك عن طريق إخفاء المعلومات في وسيط مثل النص أو الصورة بحيث يبدو ما يتم إرساله وتداوله طبيعيًا وخاليًا من العلامات أو رموز غير مفهومة كما لو لم يتم تحميلها بأي معلومات إضافية. هذا البحث يقدم مراجعة للتقنيات المستخدمة لإخفاء البيانات في الصور باعتبارها واحدة من أكثر تقنيات الإخفاء شيوعًا.

الكلمات المفتاحية: الصورة، إخفاء المعلومات



ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com



## 1. Introduction

Humans sought to find different ways to preserve the confidentiality and integrity of data. Maintaining the confidentiality of the data during the transmission has critical importance especially military data, data belonging to economic and industrial organizations, and credit card numbers, as a result the need to secure information appeared [1].

Information security is the protection of certain information, whether digital or non-digital, from being examined, disclosed, or manipulated by unauthorized persons. Data is secured through encryption or concealment, each of which has its own methods [2]. Although concealment is very important, it is not as widespread as cryptography. Beginnings in information security science confuse cryptography with concealment, believing that both terms give the same meaning, while each term covers a particular science of information security [3].

There is a big difference between concealment and encryption of information. Encryption relies on changing data in a certain manner to become unreadable for this reason, the encrypted information is susceptible to traceability because it is obvious; the existence of encrypted information itself is valuable because it induces an intruder to try to decrypt it [4], thus raising the risk of its content being discovered. The concept of information concealment aims to conceal the fact that information exists from any unauthorized party to know or view it by including it in other data, such as pictures or sound, no apparent change or distortion of information was observed after the concealment.

## 2. Related Work

Priti Sehgal et al. [11] are introduced a method to hide secret data in images through three levels including (vegenere cipher, white space text steganography and LSB ) to increase the level of confidentiality and reliability. Cover images used in this method are RGB and system performance was evaluated using MSE and PSNR.

Pratik D. Shah et al. [12] suggested a method based on rearranging confidential data before hiding it using least significant bit. GA uses a concept flexible of chromosome that allows interruption of the chromosome in various ways to control the data rearrangement parameters.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com



Searching for the best parameter is the mission of GA in order to find or achieve high quality for masking images.

Aya Jaradat et al. [13] built a steganography system based on hide confidential information in the best locations of image by using swarm optimization method and chaos theory. The goal of dividing the image into blocks is to improve steganography capacity so each block stores a number of secret bits.

The system proposed by the Zahraa Salah Dhaief et al. [14] consists of two parts: the first part includes encrypting the data based on a chaotic map cipher and then passing it to the second part in order to hide it in colored images using LSB technique with help XOR operation.

The researcher R. Varalakshmi [15] used a method of AI called Karhunen Loeve Transform to communicate the confidential data that you take as input and encrypt the images which contain the data to be hidden. DES algorithm using as a method for decoding encrypted image to retrieve the original confidential data.

Hassanain Raheem Kareem[16] The proposed system depends on generating a random key to choose locations in image for hiding, the length of which is the same as the secret data and then use the XOR process to hide data. The next stage of the system involves encrypting the image with the data hidden inside it by using 3DES algorithm to increase confidentiality and reliability.

Swati Bhargava[17] Have suggested a system includes as a first step apply LSB bits substitution on the cover image and then encrypt the confidential data using an RSA algorithm. Now hide the encrypted text in the encrypted image by discrete wavelet transform to getting the hidden image.

The idea of the system proposed by Mansoor Fateh[18] depends on dividing the series of bits of confidential data into groups of n bits and then select 2n− 1 location from cover image to hiding each group. The researchers Rusul Mohammed Neamah et al. [19] introduced a hiding system that includes as a first step encrypting secret data using the X-Nor process and then passing it to the next step to be hidden through the second bit test for RPG channels: if the remainder of the division bit on 3 is 0 (Choose the red channel), if the remainder is 1 (Choose the green channel) and if the remainder is 2( the chosen channel is blue).

Ahmed Toman Thahab [20] Suggested a hiding system in spatial field which the cover image is divided into non-overlapping blocks that are scattered within the image size using the method Burrows Wheeler transform. Confidential data is hidden based on its sequence in output

Burrows Wheele method. The hiding process relies on making exclusive-or between the most significant bit and the least significant bit.

Al-Hussien [21] Suggesting a system that includes hiding data in secret images using GA with wavelet method and then encrypt the generated image using filter bank cryptographic. The data passes as a final stage in hashing algorithm to increase the level of security and reliability.

The researchers Saad Ahmedet al. [22] presented an improved method for hiding confidential data in the significant bits of the cover image using the pixel value indicator method. The green channel here acts as a router to hide the data in 5 , 6 bits of the red and blue channels, if the green channel has an even number of 1's the blue channel is used for hiding otherwise the red channel is used. Summarize of related work show in table 1.

**Table 1: Summarize of related work**

| NO. of reference | year | methods | Quality measure |
|---|---|---|---|
| [11] | 2017 | White space text technique and LSB | MSE=9.333 PSNR=99.09 |
| [12] | 2021 | GA algorithm with flexible chromosome structure | PSNR=46.41 |
| [13] | 2021 | Chaotic Particle Swarm Optimization | PSNR=69.02 |
| [14] | 2020 | A chaotic map cipher and LSB Steganography | Time=1.337 |
| [15] | 2020 | Artificial Intelligence Technology | MSE=8.80E-04 PSNR=86.6468 |
| [16] | 2020 | Randomization depending on the random key | MSE=0.03602 PSNR=55.0016 |
| [17] | 2019 | LSB, DWT AND RSA | MSE=1.2050 PSNR=71.8331 Entropy =7.5819 |
| [18] | 2021 | LSB Matching Revisited | MSE=0.1416 PSNR=66.4486 |
| [19] | 2020 | Modified LSB algorithm | MSE=0.0336 PSNR=61.74 |
| [20] | 2019 | Burrows transform and dynamic bit embedding | PSNR=51.1412 NCC=0.999 |
| [21] | 2018 | Wavelet and genetic algorithm based steganography | PSNR(db)=11.2451 Entropy=7.9875 |
| [22] | 2018 | Green Channel as Pixel Value Indicator | MSE=0.1970 PSNR=55.185 |

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com



## 2- Digital steganography

Steganography is a method of concealing data within a medium that conceals information [3] without arousing suspicion so that only the persons concerned are aware of the concealment. Shorthand has appeared in many forms throughout history, from the concealment of secret information written on the head after its shaving and the growth of the hair again, to the concealment only after the shaving of the head, [7] to the use of secret ink in world wars, [2] to the advent of the information revolution and computer technology, and thus the use of digital media to conceal information.

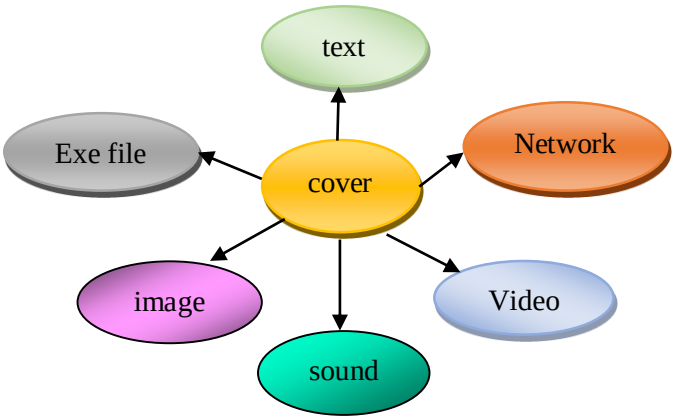


**Figure 1: illustrates the general method of data reduction.**

### 2.1 Digital media Hidden Information:

- *Hiding in exe files*: data by adding the message to the back of an executable file that plays the role of cover. Adding a message to the executable does not affect the work of the executable.
- *Hiding within video*: the information is hidden in Mp4, MPEG, and AVI or other video formats. A video is at the end of a group of images thus data can be hidden in each of the images in a way that does not attract attention.
- *Covering message by text file*: the message can first be encrypted with an encryption algorithm to give it more immunity before hiding it in a medium, such as changing the font color to be the same as the background color, so that the message will not look until after the font color has changed.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com



- *Concealing a message in an image* can be done by using the least valuable bits of image bytes, so that the image that is produced after the cloaking is not so different from the original as to be seen with the naked eye. This technique is also used in audio files.
- *Networks steganography*, which first appeared in 2003 by the researcher Christoph Schiborsky and uses key protocol controls and core functions, making it difficult to detect, includes a number of techniques, including Voice-over-IP (overshoot) message concealment and LAN (overshoot) transmission, with a practical application of WLAN: Hidden Communication System for Corrupted Networks.

As seen in figure 2, the key elements of this system are:

- The message: the original information that is to be kept and concealed by those concerned [6]
- The cover - The transmitting medium - as a mask - to conceal the confidential message [7].
- Hidden algorithm: The algorithm used by the sender to encapsulate and hide a message in a cover is matched by a corresponding algorithm used to extract the hidden message from the recipient.
- Shorthand message: The message that comes from encapsulating a secret message in a cover using a cloak-out algorithm will be sent to the other party [8].
-

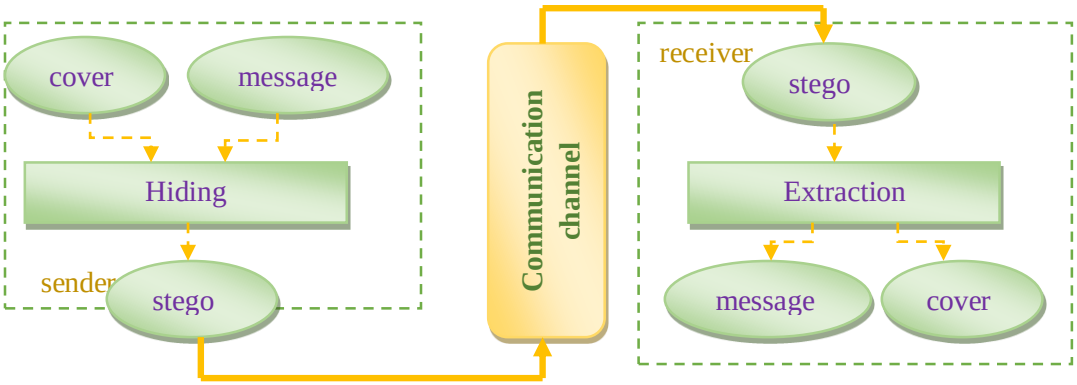


**Figure 2: The structure of steganography system**

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com



## 3- Image and steganography

digital images can be viewed as array of pixels. The methods of using image for concealment fall into two categories:

**1) Using of Frequency/ Transformation:** This type of concealment depends on making image conversions (DCT, DFT, Wavelet) to prepare for the concealment phase [5]. These transformations convert the cover from spatial to spectral domain.

### I. DCT (Discrete Cosine Transformation)

The image is divided into spectral regions by taking into account the importance of visual information [23]. The most important visual information is concentrained at the low frequency part [24]. Conversely, high frequency part contains the less visual information, so that it is deleted when the data is compressed [25]. The message is hidden in the least significant bits of the discrete cosine coefficient of middle frequency region [23]. For N* N cover, the DCT coefficients are obtained by applying the following equation:

$$\text{DCT(i, j)} = \frac{1}{\sqrt{2N}} \text{C(i) C(j)} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \text{cover (x, y)} \left[\cos \frac{(2x+1)i\pi}{2N}\right] \left[\cos \frac{(2y+1)i\pi}{2N}\right]$$

Where:

$$\text{C(x)} = \begin{cases} \frac{1}{\sqrt{2}} & if \ x = 0 \\ 1 & if \ x > 0 \end{cases}$$

### II. DWT(discrete wavelet transform)

Using DWT, we can recover the image with higher quality compared with DCT. Typically, the embedding process is referred to as encoding while decoding means extracting hidden data from cover[23]. The 2D image is partioned into four non-overlapping bands [24] as shown in Figure 3:

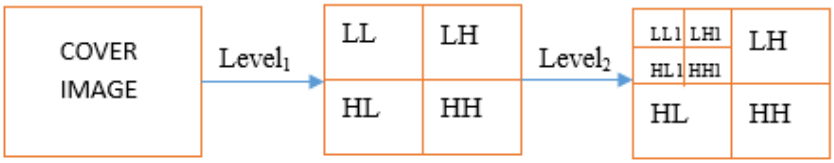


Figure 3: 2- levels DWT

The low-low (LL) band is divided into sub-bands and this process is continued as far as possible (based on image resolution). Hiding data in low frequency sub-bands ($LL_x$) may perceive by the human eye because they hold much of signal energy. In contrast, hiding information in $HH_x$ can be done without being noted by human eye since they contain information about edge and

texture [24] so it is the best choice for hiding. The DWT is strong method for hiding which characterized by high-quality stego image. However, it is expensively computation and takes long time for compressing [25].

**2) Spatial encapsulation**: data are hidden directly in pixels of the image. There are some choices to hide data in spatial domain.

**I. Hidden using LSB (Least Significant Bit)**

The well-known LSB based on replacing the less significant bits with the ones to be hidden. The least significant bit has less effect on the image. This method can be applied to gray and color images. The pixel in the gray image is converted into the equivalent binary form and the secret bit is placed instead of the least important bit then the pixel is reconverted from the binary to get the new pixel value, pixel after hiding. The pixel in colors images is a combination of three component: red, green, and blue [26]. LSB can be applied to any one or even all three colors. This method is easy to implement, but as expected, it is weak even against the simplest types of attack and the hidden data can be lost if the protective image is attacked.

**II. Histogram shifting**

This method hides the data in the image's histogram. A number of peak points (P) and zero points (Z) are determined in the histogram and then the values between them are shifted by one location towards ZP and thus create an empty gap near the PP that is exploited in the masking process [27]:

- If image pixel value = P and secret bit = 1, adjust pixel value to fill blank gap near P.
- If the secret bit value = 0, do not change the pixel value.

In order for the retrieval process to proceed properly and smoothly, the P and Z locations are also stored.

**III. Pixel value differencing (PVD)**

One of the steganography spatial algorithms for gray images proposed by Wu and Tsai . It showed high performance in terms of resisting hidden information detection attacks also providing a good storage payload. The amount of secret bits that can be hidden in this way depends on the difference between adjacent pixels [28]:

Step1: The cover image is divided into non-overlapping blocks of two pixels, and then the difference between the pixels for each block is calculated $d= (pi – pi+1)$ .

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Step2: Determining the number of bits to be hidden based on the difference value and a predefined range table n=[log2(u-l+1)]

where (u , l) represent upper and lower bound from range table.

Step 3: Update the difference value by converting n secret bits stream into a decimal value m

D' = m+ l , then pi and pi+1 update by :

Pi=[pi-(d'-d)/2] , pi+1=[pi+1 +(d'-d)/2]

Step 4 : repeat steps from 1 to 3 until entire secret bits stream are hidden.

IV. Random pixel embedding method

The principle work of this method depends on randomly hiding for confidential data in image pixel locations in order to increase confidentiality and security. The locations are generated randomly through the use of special methods and algorithms for this purpose [29].

## 4- Quality measures

There are a number of ways to measure the effectiveness of a cloaking method:

a) Mean Square Error (MSE). Since we talk about an error, it is natural to want to minimize the error, in other words, the lower the error, the better the processing quality, which is an indication of the technique used to hide the information in the image. The MSE is calculated by the equation [5]

$$\mathrm{MSE}=\frac{1}{M\times N}\sum_{i=1}^{N}\sum_{j=1}^{M}\left[I(i,j)-I'(i,j)\right]^2$$

b) Peak Signal to Noise Ratio (PSNR). The ratio between the maximum possible energy of a signal and the ability of noise that negatively affects the accuracy of its representation. This measure is inversely related to the MSE, so the higher the PSNR, the more efficient the treatment method:

$$\mathrm{PSNR}=10\times\lg\left(\frac{255^2}{\mathrm{MSE}}\right)$$

c) average difference

The average difference between the cover before and after hiding can be provided by using the following formula:

$$AD=\frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}Ca(i,j)-Cb(i,j)$$

d) SSIM

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

The previous measures are evaluating quality based on error which does not consider the correlation. SSIM is used to compare the structure of the cover before and after hiding using the equation [26]:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_1^2 + \mu_2^2 + c_1)(\sigma_1^2 + \sigma_2^2 + c_2)}$$

When the resulted image is identical to original cover, the SSIM is equal to 1.

## Conclusion

It has become indispensable for the services provided by the Internet and the development of technology in terms of sending and receiving many information in various areas of life and at the same time there are dangers and fears of losing or hacking information by unauthorized persons. This paper presented a review that includes a simple definition of hiding as a means used to preserve data also display the most important hiding algorithms in the two fields spatial and transformation. A number of methods have been demonstrated to measure the efficiency of hiding algorithms.

## Conflict of interests.

There are non-conflicts of interest.

## References

1. Gandharba Swain," Digital image steganography using variable length group of bits substitution", Procedia Computer Science, 85, 2016 .
2. Suhaila Mohammed et al.," Block-based Image Steganography for Text Hiding Using YUV Color Model and Secret Key Cryptography Methods ", Australian Journal of Basic and Applied Sciences, 11(7) May 2017.
3. Gourav Tiwari et al., "Secret Information Transmission within Color Image using Wavelet Transformation", International Journal of Computer Science and Information Technologies, Vol. 8, No. (3) , 2017.
4. Shiv Prasad et al., "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing", Royal Society, March 23, 2018.
5. Nasseer M. Basheer et al., " Proposed Method of Text Hiding in Image Edges", International Journal of Computer Applications , Vol.( 126), No.(11), 2015.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

6. Vidhya P.Ma et al., " A Method for Text Steganography Using Malayalam Text ", International Conference on Information and Communication Technologies, Procedia Computer Science 46, 2015).
7. A.A. Mohamed," An improved algorithm for information hiding based on features of Arabic text: A Unicode approach", Egyptian Informatics Journal 15, 2014.
8. Harpreet Kaur1 et al., " A Survey on different techniques of steganography ", MATEC Web of Conferences 57, 2016.
9. Qasim Mohammed Hussein et al.," The efficiency of Color Models layers at Color Images as Cover in text hiding ", Tikrit Journal of Pure Science ,21 (1), 2016.
10. Poonam Yadav et al., "A Overview of various Steganographic Domains and its applications", International Journal of Engineering Trends and Technology (IJETT), Vol. (52), No. ( 3), 2017.
11. Priti Sehgal et al. "Hiding Encrypted Text Using Text And Image Steganography: A Dual Steganographic Technique", International Journal Of Electrical, Electronics And Data Communication, Volume-5, Issue-7, Jul.-2017.
12. Pratik D. Shah et al. ," Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure", Engineering Science and Technology, an International Journal, Volume 24, Issue 3, June 2021.
13. Aya Jaradat et al.," A High-Capacity Image Steganography Method Using Chaotic Particle Swarm Optimization", Security and Communication Networks Volume 2021, Article ID 6679284, 11 page.
14. Zahraa Salah Dhaief et al.," Hiding Encrypted Text in Image using Least Significant Bit image Steganography Technique", International Journal of Engineering Research and Advanced Technology, Volume.6, Issue 8 August -2020.
15. Dr. R. Varalakshmi," Digital Steganography For Preventing Cybercrime Using Artificial Intelligence Technology", Journal of Critical Reviews ,Volume 7, Issue 6, 2020.
16. Hassanain Raheem Kareemet al.," Hiding encrypted text in image steganography", Periodicals of Engineering and Natural Sciences, Vol. 8, No. 2, June 2020.
17. Swati Bhargava et al. , "Hide Image And Text Using Lsb, Dwt And Rsa Based On Image Steganography", Ictact Journal On Image And Video Processing, February 2019, Volume: 09, Issue: 03.
18. Mansoor Fateh et al.," A New Method of Coding for Steganography Based on LSB Matching Revisited", Security and Communication Networks Volume 2021, Article ID 6610678.
19. Rusul Mohammed Neamah et al., "Hide text depending on the three channels of pixels in color images using the modified LSB algorithm", International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 1, February 2020.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

20. Ahmed Toman Thahab, "A secure image steganography based on burrows wheeler transform and dynamic bit embedding", International Journal of Electrical and Computer Engineering (IJECE) Vol. 9, No. 1, February 2019.
21. Al-Hussien et al.," A Hybrid Text – Image Security Technique", Journal of Theoretical and Applied Information Technology 15th May 2018. Vol.96. No 09.
22. Saad Ahmed et al.," Data Hiding Using Green Channel as Pixel Value Indicator", International Journal of Image Processing (IJIP), Volume (12) : Issue (3) : 2018.
23. Ms. Shubhangi Hiwe et al., "An Analysis of Image Steganography Methods", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014.
24. Jay Desai et al., "Comparison between DCT and DWT Steganography Algorithms", International Journal of Advanced Information Science and Technology (IJAIST),Vol.24, No.24, April 2014.
25. Nicky saxena," Image steganography using DCT and DWT", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 7 issue 1 May 2016.
26. Mohammed Mahdi Hashim et al.," Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats", International Journal of Engineering & Technology, 7 (4) (2018) .
27. Alaa Fkirin et al.," Steganography Literature Survey, Classification and Comparative Study", Communications on Applied Electronics (CAE) – ISSN : 2394-4714 Foundation of Computer Science FCS, New York, USA Volume 5 – No.10, September 2016.
28. Aditya Kumar Sahu et al.," A Review on LSB Substitution and PVD Based Image Steganography Techniques", Indonesian Journal of Electrical Engineering and Computer Science Vol. 2, No. 3, June 2016.
29. Mehdi Hussain et al.," Image Steganography in Spatial Domain: A Survey", 2018 Elsevier.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com