# A Technique of Image Steganography using Parity Checker and LSBraille

Abdelmged A. A.
Computer Science Department
Minia university, Egypt

Al-Hussien Seddik Saad
Computer Science Department
Minia university, Egypt

Nada Hussien
Computer Science Department
Minia university, Egypt

## ABSTRACT
Today, internet made it easier to send the data more accurately and faster to the destination with the increasing unauthorized access of confidential data. So that, the issue nowadays reduces detection of information during transmission. To hide the secret information during transmission, there are two methods cryptography and steganography. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Steganography is a Greek origin word which means "hidden writing". In this paper, a new image steganography method is proposed. The proposed method hides the secret message inside the cover image by representing the secret message characters using Braille method of reading and writing for blind people. Which all pixels of the cover image can be used and message bit is stored in LSB of one of the three color components Blue (B) only; based on the parity of three LSBs of R, G, and B components of 24-bit color image. From the experimental results it's founded that the proposed method can hide a lot of data in single RGB image which a few pixels of image can be changed so that method can achieve higher value of (PSNR) and Maximum Hiding Capacity (MHC).

## Keywords
Steganography, Peak Signal-to-Noise Ratio (PSNR), Least Significant Bit (LSB), even odd Parity.

## 1. INTRODUCTION
There are a lot of devices transmissions on the network and there must be some important information that needs to be protected during transmission. So that it's becomes an important research issue. In fact, the problem is how to protect secret message from being stolen during transmission is a big problem and there are two ways to solve this problem. One way is encryption, which refers to the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully; but message make suspicion about the communication. The second way is steganography, which is selected as a point of research, and this is a technique which hides secret information into a cover media or carrier so that it becomes unnoticed and less attractive [1]. which it's hides the existence of message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message and no one can even guess about the communication going on between sender and receiver.

### 1.1 Basic Steganography system
The basic Steganography system consists of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message within a cover media, and is the most carefully constructed process of the two. Because needed no one from the third parity to notice there are secret message inside the cover media during transmission so that it must be taken into consideration in that process. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end[2]. In general, there are three inputs are required for the embedding process: Cover file (Carrier): It is defined as a file to embed the secret message inside it. It is also termed as innocent file or host file.

a) Payload (Secret Message): It is the secret massage that has to be embedded within the cover file. The payload can be in the form of text, audio, images, or video.
b) Stegokey: is a password that may be used to encode the secret information to provide an additional level of security. The next step is to pass these inputs through the stego-system encoder, which will be carefully engineered to embed the message within the cover media (image). The resulting output from the stego-system encoder is the stegogramme [3].
c) Stegogramme: is the final file obtained after embedding the secret message into a given cover media. It should have similar properties to that of the cover media (image), except it will contain the secret message.

### 1.2 LSB Technique
LSB method is the most popular method that hides the secret message inside the cover image. In LSB method the message is hid in the least significant bits (LSB's) of pixel values of an image. Which each image consists of a set of pixel values. Then each pixel is converted to equivalent binary and replace LSB of each pixel of image by the secret message after converter it to binary using ASCII format. For example, data bits 01100101 are tried to hide into an 8-bit color image. The binary equivalent of those pixels may be like this: -

00100101 11101011 11001010 00100011 11111000
11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become 00100100 11101011 11001011 00100010 11111000 11101111 11001110 11100111.

The problem with this technique is that it is very easy to attacks which it's most popular [1, 3].

### 1.3 Categories of Image Steganography
Image steganography techniques can be divided into two groups [3]. One of them is called spatial domain technique, which embed messages in the intensity of the pixels directly. Such as, least significant bit insertion methods. The second technique is called transform domain, in that type of technique images are first transformed and then the message is

embedded in the image, like DWT (Discrete Wavelet Transforms).

## 1.4 The Main Objectives of Steganography Techniques Are [4,3]:

- Capacity; the amount of information that can be hidden in the cover medium.
- Security; related to the eavesdropper's inability to extracted the hidden information.
- Imperceptibility; referred to no one can noticed difference between the cover and original signal.

## 1.5 Performance of Image Steganography

The performance for image steganography can be measured by peak-signal-to noise ratio (PSNR), which measured the similarity between the stego-image and the cover image, represented by equation in [5]

$$\text{PSNR} = 10\log_{10}(\text{R}^2/\text{MSE}) \quad \text{..... (1)}$$

Where MSE denotes the mean square error, it's measure the difference between the stego image the cover image, represented by equation

$$\text{MSE} = \frac{\sum_{\text{M,N}}[\text{I}_1(\text{m,n}) - \text{I}_2(\text{m,n})]^2}{\text{M} * \text{N}} \quad \text{..... (2)}$$

This paper is organized as follows; previous work will be discussed in section 2, the proposed method will be discussed in details in section 3, experimental results will be given in section 4. Finally, section 5 concludes the paper.

# 2. PREVIOUS WORK

In [6], The proposed method used the Braille method representations of the characters where each character is represented by only six dots using the six – dots matrix that called (Braille Cell). The method starts by representing these characters (dots) as binary digits, each of which consists of 6 bits only instead of eight bits as in original LSB embedding method that uses the binary representation from the ASCII table. Therefore, by using this representation, two pixels are saved from each secret byte embedding process or more than one-fourth of the maximum hiding capacity for each cover image. Therefore, the maximum hiding capacity (MHC) has been increased and the PSNR of the LSB embedding technique has been enhanced.

In [7], a new approach for hiding message in digital image in spatial domain has been presented. In the proposed method, all pixels of the cover image can be used which has been determined if the parity is even or odd by using the LSB of the three color components of each pixel but message bit is stored in LSB of one of the three color components, Red(R), Green (G), Blue (B) in alternate fashion based on the parity of three LSBs of R, G, B components of 24-bit color image.

In[8], this paper has been presented a novel algorithm for image steganography based on effective channel selection technique is used in order to hide secret data in cover-image .Proposed work is concentrated on 8 bits of a pixel (8 bits of blue component of a randomly selected pixel in a 24 bit image), resulting better quality of image. Proposed technique has also used contrast sensitivity function (CSF) and just noticeable difference (JND) Model.

In [9], The proposed method work by adding an Alpha channel to the image whose pixels are 255 , then searching for the MPKDigits of the character and if found, the index will be embedded in the corresponding Alpha pixel by using Least Significant Bit (LSB) Method else, new search space will be encountered. The new proposed method converts the whole cover image into a search space for the whole secret message. So, instead of embedding the secret character itself which can varies from (0 to 127); in case of secret text or (0to 255); in case of secret image, the secret character index which varies from 1 to 6 will be embedded; which are the indices of the search space. This means that the secret characters varies from (001)2 to (110)2 not from (00000000)2 to (11111111)2 which means smaller number of modified pixels and higher PSNR values plus higher Maximum Hiding Capacity (MHC).

In [10], this paper presented the analysis of various image steganography techniques in spatial domain on the basis of Relative Entropy metric (LSB Technique- Parity Checker Method- Inverted Pattern Approach). The lower the value of the Relative entropy the better will be the quality of the stego image. And found that parity checker method given by Rajkumar et. al provide least value of relative entropy among the investigated techniques.

# 3. PROPOSED TECHNIQUE

The proposed method will concern the spatial domain of the cover image. And must know in that method the secret message and the cover image are considered as an input. The principal of this method using Braille method [6] which each byte in the secret message is represented by 6-bits only instead of 8-bits by using ASCII encoding format. And embedded the secret message in the blue layer according to type of parity checker method. The concept of even and odd parity by using the parity checker has been used by Rajkumar et al. As it is already known that even parity means that the pixel value contains even number of 1's and odd parity means that the pixel value contains odd number of 1's, and determine that by collecting the bits of LSB of each pixel (Red, Green, and Blue) and makes a group of three bits. Now the sequence of these three bits may have either even number of 1's or odd number of 1's,if it's even parity that's mean the pixel value contains even number of 1's and odd parity means that the pixel value contains odd number of 1's [10].

After identifying the parity, the embedding in the proposed algorithm depends on the message bit and the parity generated by the LSB of each color components.

## 2.1 Embedding Process

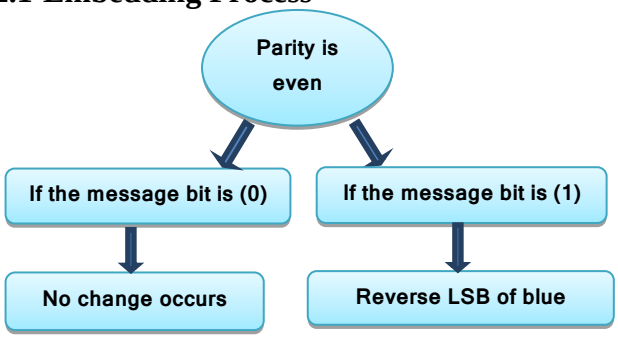


**Fig 1: Embedding process if the parity is even**

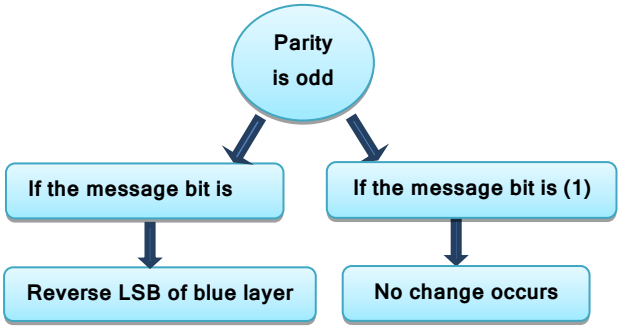


**Fig 2: Embedding process if the parity is odd**

In the embedding process if the parity is even and sender wants to embed (0) then, no change can be occurring, but when embedding (1) then changed the LSB of Blue layer i.e. 1changed to 0, and reverse as shown in Figure 1. But if the parity is odd and sender wants to embedded (1) then, no change can be occurring, but if wants to embedded (0) then changed the LSB of Blue i.e. 1changed to 0 and reverse, as Shown in Figure 2.

### *2.1.1 Embedding Algorithm*

1. Get the message to be embedded
2. Convert the message to 6 binary number using LSBraille method instead of 8 by using ASCII code format [1].
3. Calculate the size of the message (no. of character or byte)
4. Let N=length of resultant message in bits after using LSBraille method.
5. Select a cover image.
6. Then make loop from I=1: N.
7. Represent the cover image into three layers (R-G-B).
8. Convert each layer to binary number (8-bits) and take the LSB of each pixel of the three layers (R-G-B).
9. Collect three LSBs say (R)LSB, (G)LSB, (B)LSB for R, G, B color components of Ith pixel
10. Determine the parity of (R)LSB, (G)LSB, (B)LSB (Even or Odd)
11. Get message bit (0 or 1)
12. If message bit is 0 and parity is even, do nothing
13. If message bit is 0 and parity is odd, reverse the value of the LSB(BLSB)
14. If message bit is 1 and parity is even, reverse the value of the LSB(BLSB)
15. If message bit is 1 and parity is odd, do nothing
16. I= I+1
17. Then collect the three layers and return the image which it's called stego image after embedding the message.
18. END.

### *2.1.1.1 Extracting Process*

The extraction process can mean reverse the embedding process that's mean that collect the components of the LSBs of the three pixels of each layer and determine the parity if it's odd or even .if the parity is even and LSB of Blue layer is 0 then no change occurs and return 0 but if the LSB of the Blue layer is 1 then return 0.but if the parity is odd and LSB of Blue layer is 1 then no change occurs and return 1 but if the LSB of the Blue layer is 0 then return 1.that's mean that if the parity is even return 0,if the parity is odd return 1 as shown in Figure 3.

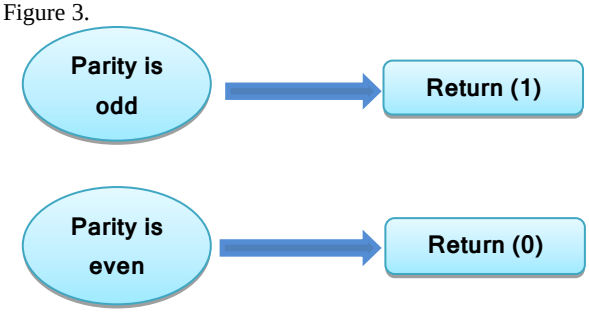


**Fig 3: Extraction process**

### *3.1.1.2 Extracting Algorithm*

1. Get stego image.
2. Take the size of the message
3. Let the size of the message is p
4. Then make loop from I=1: P*6
5. Represented pixel in the stego image by three layers (R-G-B)
6. Collect three LSBs say (R) LSB, (G) LSB, and (B) LSB for R, G, and B color components of Ith pixel
7. Determine the parity of RLSB, GLSB, BLSB (Even or Odd)
8. If the parity is even store the 0 as the message bit else store 1 as the message bit.
9. I = I+1
10. After having a set of binary number like that for example (10101010101010101010101010010101001010100101001010 010100100)
11. Recall the function that convert a set of binary to character according to LSBraille and return the secret message.
12. END.

## 4. EXPERIMENTAL RESULTS

To determine the performance of the proposed technique, first of all steganographic technique applied a test to a set of images, to measure the quality of the image parameters such as Peak Signal to Noise Ratio (PSNR). The proposed algorithm was implemented in MATLAB (R2015a) running on Windows 10 operating system. In this section, the proposed method will be implemented and evaluated by comparing it with different methods, as well as, using different messages, different cover image and different size of the message.

**Table 1. Comparison between PSNR of 3-Methods and proposed**

| Cover images | Message Capacity | PSNR | | | |
|---|---|---|---|---|---|
| | | DWT | Method [12] | Parity checker | proposed method |
| Lena | 1000 | 60.3033 | 63.0432 | 65.0202 | 66.2011 |
| Baboon | 1000 | 60.2393 | 63.0220 | 65.0789 | 66.3276 |
| Pepper | 1000 | 60.1 | 63.0535 | 65.0440 | 66.2567 |

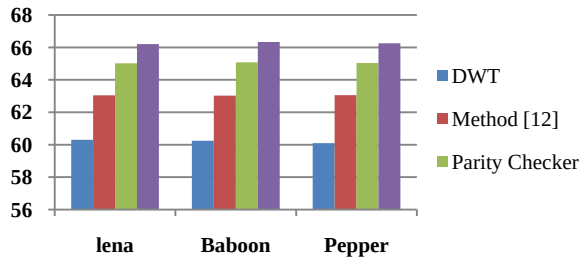


**Fig 4: comparison between PSNR values of Table (1)**

Table 1 and Figure 4 show the comparison between the proposed method with DWT method [11], method [12] ,parity checker [10]by using 1000 characters (bytes) secret message and 265 x 265 cover images (Lena, baboon, pepper) and it was founded that the proposed method has more PSNR values than DWT method , method [12] and parity checker method which means the stego image quality of the proposed method will be higher than the stego image quality of the DWT method, method [12], parity checker method. So, the proposed method succeeded in obtaining more capacity for the same cover image when LSBraille is used so the value of PSNR is increased too.as shown on Figure (4).

**Table 2. Comparison between PSNR of 3-Methods and proposed method**

| Cover images | Message Capacity | PSNR | | | |
|---|---|---|---|---|---|
| | | SLDIP | MSLDIP | Method [9] | proposed method |
| Lena | 6656 | 44.9886 | 48.7596 | 48.823719 | 58.0829 |
| Boat | 6656 | 44.9953 | 48.6661 | 48.894425 | 58.1030 |
| Baboon | 6656 | 44.9953 | 48.6638 | 48.684503 | 58.0530 |

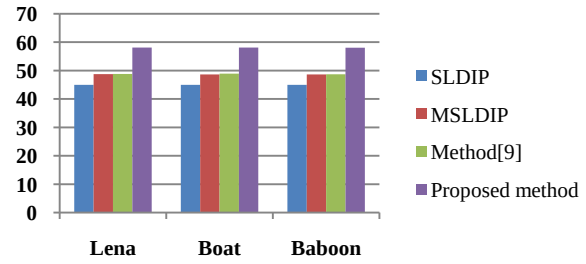


**Fig 5: comparison between PSNR values of Table (2)**

Table 2 and Figure 5 show the comparison between the proposed method with SLDIP[1],MSLDIP[1]and method [9] by using 6656 characters (bytes) secret message and 265 x 265 cover images (Lena, boat, baboon) and the result of proposed method has more PSNR values than other methods which means that the stego image quality of the proposed method will be higher.

**Table 3. Comparison between PSNR of Jpeg-Jsteg, Method [9] and proposed method**

| Cover images | Message Capacity | PSNR | | |
|---|---|---|---|---|
| | | Jpeg-Jsteg | Method [9] | proposed method |
| Lena | 4382 | 37.77 | 50.717675 | 59.8805 |
| Baboon | 6026 | 36.49 | 49.117879 | 58.4644 |
| Pepper | 4403 | 37.77 | 50.763116 | 59.8795 |

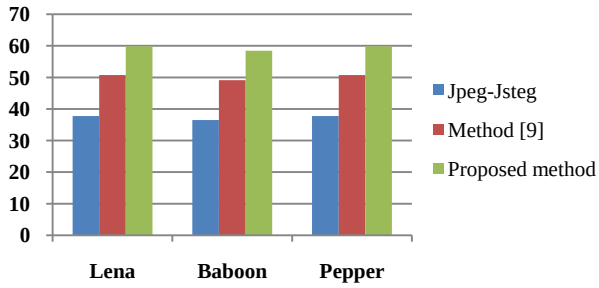


**Fig 6: comparison between PSNR values of Table (3)**

Table 3 and Figure 6 show the comparison between the proposed method with Jpeg-Jsteg [13]and method [9] by using different size (bytes) secret message and 265 x 265 cover Images (Lena, peppers, and baboon) and founded that the proposed method has more PSNR values than other methods which mean that the stego image quality of the proposed method will be higher.

**Table 4. Comparison between PSNR of 3-Methods and proposed method**

| Cover images | Message Capacity | PSNR | | | |
|---|---|---|---|---|---|
| | | SLDIP | MSLDIP | Method [9] | proposed method |
| Boat | 6656 | 44.9886 | 48.7596 | 48.823719 | 58.0829 |
| Bird | 6656 | 44.9953 | 48.6661 | 48.894425 | 58.1030 |
| Flinstone | 6656 | 44.9953 | 48.6638 | 48.684503 | 58.0530 |

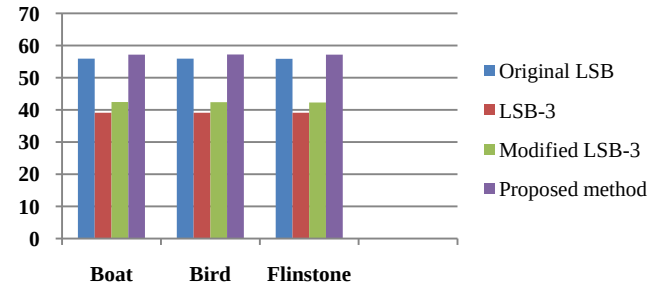


**Fig 7: comparison between PSNR values of Table (4)**

Moreover, Table 4 and Figure 7 show the comparison between the proposed method with Original LSB, LSB-3 and Modified LSB – 3 method [14] by using 8,192 characters (bytes) secret message and 265 x 265 cover images (boat, bird, flinstone) and the result of proposed method has more PSNR values than Modified LSB – 3 method and other methods which means that the stego image quality of the proposed method will be also higher.

**Table 5. Comparison between PSNR of SMMWB, Method [15] and proposed method**

| Cover images | Message Capacity | PSNR | | |
|---|---|---|---|---|
| | | SMMWB | Method [15] | proposed method |
| Lena | 10000 | 62.50107 | 38.38 | 62.6201 |
| Pepper | 10000 | 62.29195 | 37.78 | 62.3338 |

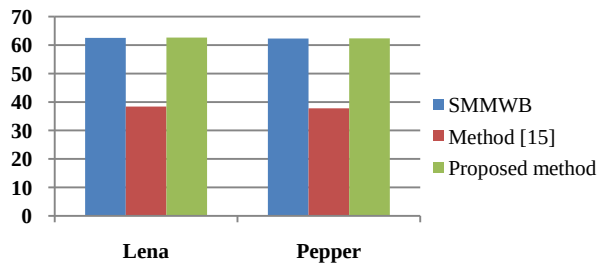


**Fig 8: comparison between PSNR values of Table (5)**

Table 5 and Figure 8 show the comparison between the proposed method with method [15]and SMMWB method [2]by hiding 10,000 secret bits in 512 x 512 cover images (Lena, Pepper) respectively, and also, it has been found that the proposed method has more PSNR values than method [15] and SMMWB method.

Finally, as shown in tables (1, 2, 3, 4, and 5), after the comparisons have been done among proposed method and other methods by using different secret message size and different cover image (boat, bird, flinstone, Lena, peppers, baboon). It was observed that proposed method has more PSNR values than other methods which means the stego image quality of the proposed method will be higher than the quality of other methods.

## 5. CONCLUSIONS

In this paper a new technique has been proposed by represented the message using LSBraille and the message has been embedded using parity checker, as shown in comparison tables, after doing the same experiments using the different methods, the PSNR values of the proposed method were higher than other methods. This means that the proposed method is succeeded to improve the PSNR value (stego image quality). In that work, a new technique of image steganography has been provided based on modified LSB approach. The proposed algorithm is based on the parity of LSBs of three color components (R, G, B). The main goal of the proposed technique is to improve the value of PSNR and increase the size of the message to be embedded with the image and also make it difficult to the unauthorized person to determine the presence of secret message. In the future, the security of the message will be improved and the value of (PSNR) will be increased.

## 6. REFERENCES

[1] Radwan, A. A., & Swilem, A. seddik AH," A high capacity SLDIP (substitute last digit in pixel) method. In fifth international conference on intelligent computing and information systems (ICICIS 2011) (Vol. 30).

[2] Abdelmgeid A.A., and Al - Hussien S. S., "Enhancing SMM Image Steganography Method by using LSBraille Image Steganography Method (SMMWB; Secret Message Matching With Braille)." International Journal of Computer Applications Vol. 70, No. 8, May 2013.

[3] Deepa S., Umarani R., " A Study on Digital Image Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 1, January 2013.

[4] Abdelmgeid A. A., Al - Hussien S. S., " New Text Steganography Technique by using Mixed-Case Font ", International Journal of Computer Applications, Vol 62, No.3, January 2013.

[5] Rajani and Muhammed T. K. "Data Hiding In Digital Image Processing Using Steganography: A Review." International Journal of Engineering Development and Research. Vol. 2, No. 3, Sept 2014.

[6] Abdelmgeid A. A., Al – Hussien S. S., " Image Steganography Technique By Using Braille Method of Blind People (LSBraille) ", International Journal of Image Processing (IJIP), Vol 7, Issue 1, 2013.

[7] Tahir A. and Amit D." A Novel Approach of LSB Based Steganography Using Parity Checker" International Journal of Advanced Research in Computer Science and Software Engineering, Vol 5, Issue 1, January 2015.

[8] Vijaypal D., Ramesh C. P., Yash V. S. "A Novel Algorithm for Image Steganography Based on Effective Channel Selection Technique" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.

[9] Abdelmgeid A. A., Al – Hussien S. S., " New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM) ", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 3, Issue 2, Jun 2013.

[10] Kamal D. "Relative Antropy Based Analysis of Image Steganography Techniques". International Journal of P2P Network Trends and Technology (IJPTT).Vol 1, Issue 3 - 2011.

[11] Arun R. , Nitin S. , Eep K. "Image steganography method based on kohonen neural network." International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012.

[12] Marwa M. E., Abdelmgeid A. A., Fatma A. O. "A Modified Image Steganography Method based on LSB Technique." International Journal of Computer Applications,Vol. 125, No. 5, September 2015.

[13] S. K. Muttoo , Sushil K. "Data Hiding In JPEG Images",BVICAM'S International Journal of Information Technology Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi, Vol. 1, No. 1 January – June, 2009.

[14] A. I. Abdul-Sada. "Hiding Data Using LSB-3". J. Basrah Researches (Sciences), vol. 33, No. 4, DEC. 2007.

[15] Sara N., Amir M. E., Mohammad S. M., " Secure Information Transmission using Steganography and Morphological Associative Memory ", International Journal of Computer Applications, Vol 61, No 7, January 2013.