# Enhancing the Security of SMMWB Image Steganography Technique by using the Linked List Structure (Cover Package Method)

Abdelmgeid Amin Ali
Professor, Department of Computer Science, Faculty of Science, Minia University, Egypt

Bahgat Abdelhamid Abdellateef
Lecturer, Department of Computer Science, Faculty of Science, Minia University, Egypt

Al – Hussien Seddik Saad
Assistant Lecturer, Dept. of Computer Science, Faculty of Science, Minia University, Egypt

## ABSTRACT
The rapid development of data transfer through the internet made it easier to send and receive gigabytes of data accurately. One of the most important factors of information technology and communication is the security of the information. For security purposes, the concept of steganography has been used. Steganography is a covert communication in which the existence of the message is not known to anyone other than the sender and the receiver. The secrecy is gained by hiding information in other information or carriers like audio, video, digital images etc., but digital images are the most popular carriers, that's because a lot of reasons such as their frequency on the internet. In fact, there exists a large variety of image steganography techniques some are more complex than others and all of them have respective strong and weak points, because of these weak points this work has been proposed. This paper contains a new proposed method which can be applied on any previously proposed image steganography technique as a pre-processing step to be added before the embedding steps to make the technique achieves its goals and strengthen its weak points, this method is the "Cover Package" which briefly means instead of using only one cover image to hide the secret message, a lot of cover images or a package of cover images can be used.

## General Terms
Image Steganography, Security, Data Hiding

## Keywords
Spatial Domain Image Steganography, Peak Signal-to-Noise Ratio (PSNR), Maximum Hiding Capacity (MHC).

## 1. INTRODUCTION
In this modern era, computers and the internet are major communication media that connect different parts of the world as one global virtual world. As a result, people can easily exchange information and distance is no longer a barrier to communication. However, the safety and security of long-distance communication remains an issue. This is particularly important in the case of confidential data. The need to solve this problem has led to the use of data hiding [1]. Data hiding is a challenging issue, steganography is considered one of the branches of data hiding [2] which is the art of hiding secret data within the cover file [3]. Steganography is a powerful security tool that provides a high level of security. The word "steganography" is of Greek origin and means "Hidden writing" [4]. It is one of the methods used for the hidden exchange of information and it can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. In this way, if successfully is achieved, the message does not attract attention from eavesdroppers and attackers [1, 5].

In fact, there are two methods for concealing secret message, steganography and cryptography. Steganography and cryptography are counter parts in digital security [4]. The goal of cryptography is to secure communications by changing the data into a form that an eavesdropper cannot understand which called the cipher text, while steganography techniques on the other hand, tend to hide the existence of the message itself which makes it difficult for an observer to figure out where the message is. In some cases, sending encrypted information may draw attention, while invisible information won't [1].

So, the similarity between steganography and cryptography is that, both are used to conceal information but the difference is that the steganography does not reveal any suspicious about the hidden information to the user. Therefore the attackers will not try to decrypt information [6].

The use of steganography dates back to ancient times where it was used by Romans and ancient Egyptians. The interest in modern digital steganography started by Simmons in 1983 [3] when he presented the problems of two prisoners wishing to escape and being watched by the warden that blocks any suspicious data communication between them and passes only normal looking one [7].

The main terminologies used in the steganography are the cover file (carrier), payload (secret message), stego file, hiding capacity and stego key [8, 9].

- Cover file (Carrier): It is defined as the original file into which the required secret message will be embedded. It is also termed as *innocent file* or *host file*. The secret message should be embedded in such a manner that there are no significant changes in the properties of the cover file [10].
- Payload (Secret Message): It is the massage that has to be embedded within the cover file in a given steganography model. The payload can be in the form of text, audio, images, or video.
- Stego file (stego-object): It is the final file obtained after embedding the payload into a given cover file.

It should have similar properties to that of the cover file.

- Hiding Capacity: The size of information that can be hidden relative to the size of the cover without deteriorating the quality of the cover file.
- Stego key: Is a password that may be used to encode the secret message to provide an additional level of security [11].

So, the basic model of steganography system will be as shown in Fig. 1 [12].

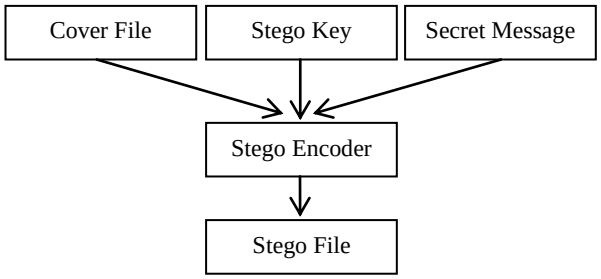


**Fig. 1: Basic model of steganography system**

In fact, there are two basic types of steganography, linguistic and technical steganography, see Fig. 2 [13].

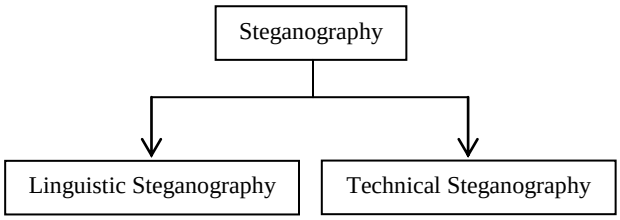


**Fig. 2: Types of steganography**

Linguistic steganography is an art of concealing secret messages. More specifically, it takes advantage of the properties of natural language, such as the linguistic structure to hide messages. Linguistic steganography can be described quite simply as any form of steganography that uses language in the cover.

While technical steganography is a little broader in scope because it does not necessarily deal with the written word even though it communicates information. Technical steganography is the method of steganography where a tool, device, or method is used to conceal the message. In reality, linguistic steganography could be considered technical steganography because it is a method. Technical steganography can be classified into: image, audio, video and text steganography [11] as shown in Fig. 3.

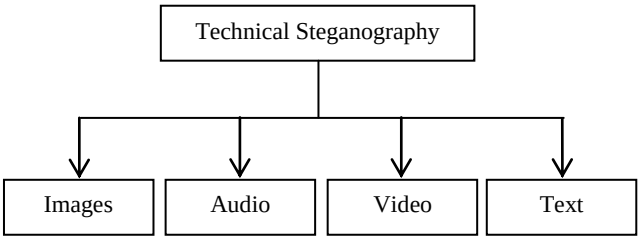


**Fig. 3: Technical steganography classification**

One of the most common types of cover objects used in modern digital steganography is digital image files [3]. These types of files are easy for any computer user to obtain or produce, and are prevalent enough in the world of computers that their presence alone does not warrant suspicion and that it would be impractical to check every such file for hidden messages. In particular, the presence of these types of files on the Internet - which is, by its far reaching and inherently anonymous nature, a common method for transmitting hidden communications - makes them a popular choice for steganographers [11].

As known, there are a number of steganography techniques that hide secret message in an image file; these techniques can be classified according to the format of the cover image or the method of hiding. There are two popular types of image steganography techniques; spatial domain techniques and transform domain techniques [3].

In spatial domain techniques, the processing is applied on the image pixel values directly, such as, Least Significant Bit Insertion (LSB) techniques [14] and Pallet based techniques.

In transform domain techniques, the first step is to transform the cover image into different domain. Then the transformed coefficients are processed to hide the secret information. Finally, these changed coefficients are transformed back into spatial domain to get the stego image.

Steganography techniques that use DCT (Discrete Cosine Transforms), DWT (Discrete Wavelet Transforms), IWT (Inverse Wavelet Transforms), or DFT (Discrete Fourier Transforms) come under this category [15, 2].

An important note is that, there are some goals to be considered when designing an image steganography system:-

1) *Capacity*: It is the amount of information that can be hidden relative to the size of the cover image without deteriorating the quality of it.
2) *Invisibility*: It is the ability to be unnoticed by the human vision system (HVS).
3) *Security*: Means even if an attacker realizes the existence of the information in the stego image it should be impossible for him to detect the information.
4) *Robustness*: It is the ability of the stego image to withstand manipulations such as filtering, cropping, rotation, compression etc. [2].

So, how the performance of an image steganography technique can be measured?, it can be measured using several properties. The most important property is the undetectability (invisibility) of the data, which shows how difficult it is to determine the existence of a hidden message in the stego image and this can be measured by calculating the PSNR (Peak Signal to Noise Ratio) value. Other associated measure is the embedding capacity or MHC (Maximum Hiding Capacity), which is the maximum information that can safely embedded in a cover image without having statistically detectable objects and can be retrieved correctly [15, 1].

In fact, for hiding secret information in images, there exist a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used [16, 1, 17] but, in almost all proposed techniques for image steganography whether spatial or transform, the key problem is how to increase the size of the secret message without causing noticeable distortion in the cover object. These techniques try to achieve the high hiding capacity of the cover

according to its local characteristics [3] or by modifying the secret message itself as in the method proposed in [12].

In this paper, a method has been proposed that can be applied on any previous image steganography technique to solve the problem of achieving image steganography system goals; invisibility, capacity, security and robustness. This method is called "Cover Package", which means using more than one cover image to embed the secret message within them. The rest of this paper is organized as follows. In section 2, some previous methods that have been proposed to enhance image steganography techniques will be briefly explained. In section 3, the proposed method will be discussed in details. Section 4 contains results and discussion of the proposed method and finally section 5 concludes the paper.

## 2. LITERATURE SURVEY

A lot of methods have been proposed to enhance the previously proposed image steganography techniques. These methods such as compressing the secret message itself to shrink the size of it before embedding, as method in [18], to encode the secret message using new encoding techniques as in [12] or to represent the secret message using smaller number of bits as in [9].

In [12] authors proposed a new encoding technique that is called Mobile Phone Keypad encoding (MPK) for secret message that represent each character in the secret message by two digits only not three digits as ASCII encoding, and they constructed a full characters' table that contains small letters (a ... z), capital letters (A ... Z), digits (0 ... 9) and special characters (@, -, +, ... ) and this proposed MPK encoding technique saved one third of the required space for embedding which in turn enhanced the Maximum Hiding Capacity (MHC) of the cover image, as a result of this the PSNR values have been enhanced too.

Also, in [9] the authors proposed a method that hides the secret message inside the cover image by representing the secret message characters by using Braille method of reading and writing for blind people that can save approximately one-fourth of the required space for embedding. The proposed method was using the Braille method representations of the characters as each character was represented by only 6 dots using the 6 – dots matrix which called (Braille Cell). The method starts by representing these characters (dots) as binary digits each of which consists of 6 bits only, not 8 bits as in original LSB embedding method which uses the binary representation from the ASCII table. So, by using this representation one - fourth of the MHC for each cover image can be saved, and that increased the MHC and enhanced the PSNR.

Moreover, in [18], the authors proposed a method that takes the cover image, secret message and secret key, then transfers the secret message into text file, then convert the text file into a zip text file (Compressed File) and convert zip text file to binary codes. Finally the message is embedded by using 2 LSBs which means using the original LSB but with last 2 LSBs not LSB – 1. The author here used the zip file for securing and compressing the secret message.

## 3. PROPOSED METHOD

The rapid development of data transfer through the internet made it easier to send, receive, download and upload gigabytes of data in short periods of time. So, how the proposed "cover package" method will be applied on any previously proposed image steganography technique to enhance its performance and make it achieves the four required goals? While thinking of a way to enhance the hiding capacity and the image quality or PSNR of the stego image, it has been found that, multiple cover images can be used at the same time, in which some of them contains part of the secret message and will be called real cover images which will form the "cover package" and the others will be "fake cover images" or empty, and the whole folder will be sent over the internet to the recipient or uploaded on any social network such as Facebook, Twitter or MySpace. But actually some problems have been faced such as, how can real cover images be distinguished from fake images? how can the parts of the secret message be retrieved from the real cover images? And what are the orders of these parts to form the right secret message? So, a try has been made to find a way to solve these problems, this try was by using the "linked lists" more specifically, the structure of it.

The linked list is the simplest form of a linked structure, it can be defined as a data structure in which each element contains a pointer to the next element, thus forming a linear list. It consists of a chain of data locations called nodes, each of which holds two pieces of information, data and a link to the next node, and at the end there exist a Null node which defines the end of the linked list as shown in Fig. 4 [19].

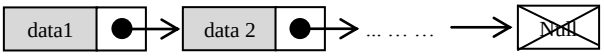


**Fig. 4: The structure of the Linked List**

First of all, the proposed method will start by selecting a folder contains a lot of cover images, then the method will randomly select the real cover images to form the cover package which corresponding to nodes in the linked list and then embed two pieces of information; data and next, in each real cover image in such a way that the data part will consists of following:-

- Current image number.
- Part of the secret message

While the next part will contains:-

- The number of the next real cover image.

The real cover image structure will be converted into the structure of the node and the number of the current image plus a piece of the secret message will be embedded in the data part of the image using any previous image steganography technique then the number of next real cover image will be randomly chosen and embedded in the next part, then the next real cover image will be selected and converted and so on.

After embedding the whole secret message in randomly chosen real cover images, the selected folder will contains real cover images that form the cover package which contains real secret message and fake cover images which exist in the folder but contains no secret data.

So, every real cover image will contains part of secret data and will call the next cover image till reaching the next to be Null. Finally, the cover package, will looks like the linked list's structure as shown in Fig. 5.

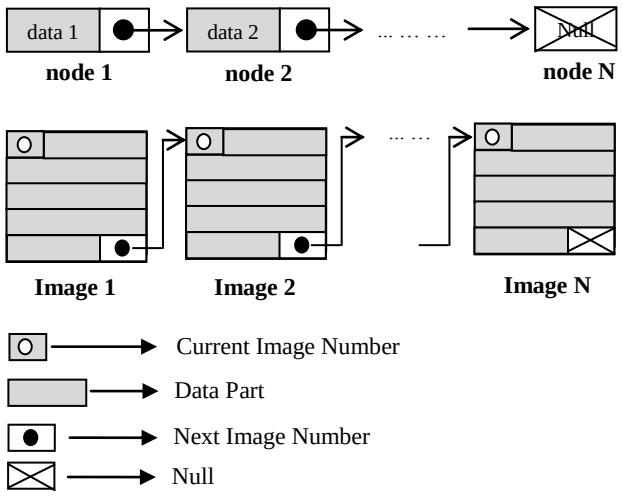


**Fig. 5: The structure of Cover Package method**

## 4. RESULTS AND DISCUSSION

In this section, the results obtained after applying the new proposed cover package method on previous image steganography techniques will be discussed.

The evaluation procedure has been started by selecting six different color test images (Peppers, Lena, Boat, Baboon, Airplane and Flinstone) with dimension (512 x 512) as shown in Fig. 6 in a folder, each of which with four different characteristics. So, the folder will contains 24 cover images.

**Fig. 6: Test images**

Then some previously proposed methods have been selected such as original LSB method, LSBraille method [9], SMM method [13] and SMMWB method [15] to apply the proposed cover package method on and a large secret message has been used to be embedded.

From the results, it has been found that the new maximum hiding capacities (MHCs) of these methods and other methods were enhanced or became unlimited because of the unlimited number of cover images with different dimensions that can be used instead of using only one image with a fixed dimension.

So, the capacity issue has been solved or the problem of "cover image is not enough to hold the secret message" is disappeared forever. This means that the first goal or the capacity goal has been achieved by applying the new proposed cover package method.

The second goal is the invisibility or the PSNR. The PSNR values were enhanced that's because the embedding algorithm didn't use the full maximum hiding capacity of each selected cover images, instead, it spreads out the whole message within a large number of real cover images (cover package). So, the number of modified pixels in each real cover image will be small which leads to a very high PSNR values or a very high stego images quality. This means that the second goal or the invisibility goal has been achieved also.

The third goal is the security, which means even if an attacker realizes the existence of the information, it should be impossible to detect it. By applying the cover package method on these methods, the security enhanced a lot, that's because the folder can contains hundreds of cover images and the data will be embedded in random number of random cover images selected by the algorithm from the folder which will cause to form the real cover images (cover package) and fake cover images.

For more security, instead of sending the whole folder it can be spread out over social networks such as Facebook, Twitter or MySpace as they contains millions of images; it will be more secure and impossible to search among millions of images. So, it can be said that the security goal has been achieved also.

The fourth goal and the final one is the robustness, which is the ability to withstand manipulations such as filtering, cropping, etc. In fact, when cover package applied, the robustness was enhanced that's because if one or more images cropped, filtered or compressed not the whole message will be damaged or removed but just small part of it.

Finally, in order to prove the efficiency of the proposed method, 10 different images have been collected in a folder and the proposed cover package method has been applied on previously proposed SMMWB image steganography method to compare between results before and after applying the cover package method on. The results that obtained are recorded and can be summarized in the following tables:-

**Table 1. PSNR value of embedding 18,224 bytes of secret message using the original SMMWB method**

| Cover images (512 x 512) | Message Capacity (Bytes) | PSNR (dB) |
|---|---|---|
| | | SMMWB method |
| Lena | 18,224 | 50.622882 |

In table 1, the original SMMWB image steganography method has been tested on Lena image with dimensions 512 x 512 to hold a secret message with size 18,224 bytes and the PSNR value obtained was 50.622882.

Now, the efficiency of the cover package will be tested by applying it on the original SMMWB to become SMMWB using Cover Package. The SMMWB using Cover Package method started by randomly selecting 8 cover images from the folder as real cover images and the other 2 cover images are fake cover images, then the secret message of length 18,224 bytes has been randomly segmented into 8 different lengths to be embedded in the 8 real cover images, then the SMMWB method has been run and the PSNRs of the 8 real cover images that hold the 18,224 byte secret message are shown in table 2.

**Table 2. PSNR values of embedding 18,224 bytes of secret message using SMMWB with Cover Package.**

| Cover images (512 x 512) | Message Capacity (Bytes) | PSNR (dB) |
|---|---|---|
| | | SMMWB method |
| Baboon 1 | 18,224 | 59.534271 |
| Bird 1 | | 60.270120 |
| Baboon 2 | | 59.633817 |
| Bird 2 | | 60.298068 |
| Lena 2 | | 59.810173 |
| Pepper 2 | | 59.781006 |
| Lena 1 | | 59.842363 |
| Pepper 1 | | 59.703217 |
| **PSNR Average** | | **59.859100** |

As shown in table 2, the SMMWB using Cover Package method has been evaluated by hiding 18,224 secret bytes in 8 different 512 x 512 cover images (Baboon 1, Bird 1, Baboon 2, Bird 2, Lena 2, Pepper 2, Lena 1, Pepper 1) respectively, and the corresponding PSNR values are (59.534271, 60.270120, 59.633817, 60.298068, 59.810173, 59.781006, 59.842363, 59.703217) which are very high PSNR values that make the stego images have excellent quality. Finally, the PSNR average has been calculated to compare between the results of the two methods and it has been found that the cover package method enhanced the PSNR values of the method that applied on.

**Table 3. PSNR value of embedding 18,115 bytes of secret message using the original SMMWB method**

| Cover images (512 x 512) | Message Capacity (Bytes) | PSNR (dB) |
|---|---|---|
| | | SMMWB method |
| Baboon | 18,115 | 50.456067 |

Also in table 3, the original SMMWB image steganography method has been tested on a 512 x 512 Baboon cover image to hold 18,115 bytes secret message and the PSNR value obtained was 50.456067.

**Table 4. PSNR values of embedding 18,115 bytes of secret message using SMMWB with Cover Package.**

| Cover images (512 x 512) | Message Capacity (Bytes) | PSNR (dB) |
|---|---|---|
| | | SMMWB method |
| Baboon 2 | 18,115 | 57.489003 |
| Bird 2 | | 58.300474 |
| Lena 2 | | 57.697805 |
| Lena 3 | | 57.705008 |
| Lena 1 | | 57.742608 |
| **PSNR Average** | | **57.787000** |

As shown in table 4, the SMMWB using Cover Package method selected 5 real cover images only from the folder and has been evaluated by hiding 18,115 secret bytes in (Baboon 2, Bird 2, Lena 2, Lena 3, Lena 1) respectively, and the corresponding PSNR values are (57.489003, 58.300474, 57.697805, 57.705008, 57.742608) which are very high PSNR values. Finally, it has been found that the cover package method enhanced the PSNR values of the method that it applied on.

**Table 5. PSNR value of embedding 18,250 bytes of secret message using the original SMMWB method**

| Cover images (512 x 512) | Message Capacity (Bytes) | PSNR (dB) |
|---|---|---|
| | | SMMWB method |
| Pepper | 18,250 | 50.754112 |

Moreover in table 5, the original SMMWB image steganography method has been tested on a Pepper image to hold 18,250 bytes and the PSNR value was 50.754112.

**Table 6. PSNR values of embedding 18,250 bytes of secret message using SMMWB with Cover Package.**

| Cover images (512 x 512) | Message Capacity (Bytes) | PSNR (dB) |
|---|---|---|
| | | SMMWB method |
| Baboon 1 | 18,250 | 56.520682 |
| Bird 1 | | 57.383017 |
| Lena 1 | | 56.720069 |
| Pepper 1 | | 56.686052 |
| **PSNR Average** | | **56.827500** |

As shown in table 6, only 4 real cover images have been selected (Baboon 1, Bird 1, Lena 1, Pepper 1) respectively to hide 18,115 secret bytes in, and the corresponding PSNR values are (56.520682, 57.383017, 56.720069, 56.686052) which have a PSNR average value equals to 56.827500 that is higher than the PSNR value of the method that it applied on.

# 5. CONCLUSION

In this paper, a method called "Cover Package" has been proposed which can be defined as a collection of real cover images that are used simultaneously to hold one secret message within them by using any image steganography technique.

The way of linking the whole images together was the linked lists' structure; as each image is treated as a node and contains data (secret message) and link to the next image, until reaching the null node which indicates the end of the list.

The proposed method was applied on a lot of previously proposed image steganography techniques such as SMMWB; as shown in the results and discussion section; and it has been found that the proposed cover package method enhanced the performance of the method that has been applied on and enabled this method to achieve the four required goals for any image steganography system.

As shown in the results and discussion section, we couldn't compare one image with multiple images so, the only available solution was to take the average PSNR of the cover package and compare it with the PSNR of the previously used image.

So, any previously proposed image steganography technique either successful or not can be reused again by applying the new proposed Cover Package method on. That’s means the proposed method can bring any previously proposed image steganography technique to life again.

Finally, it can be said that the proposed method makes the previously proposed image steganography techniques more efficient than were in their original form.

## 6. REFRENCES

[1] Nagham H., Abid Y., Badlishah A. and Osamah M. A., "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Vol. 6, Issue 3, 2012.

[2] Hemalatha S., Dinesh A., Renuka A. and Priya R. K., "A Secure and High Capacity Image Steganography Technique", Signal & Image Processing : An International Journal (SIPIJ), Vol.4, No.1, February 2013.

[3] Archana S., Antony J. and Dr. Kaliyamurthie K. P., "A Novel Approach on Image Steganographic Methods for Optimum Hiding Capacity", International Journal Of Engineering And Computer Science, Vol. 2, Issue 2, Feb 2013.

[4] Samir K. B. and Suman C., "Image Steganography Using DNA Sequence", Asian Journal Of Computer Science And Information Technology, Vol. 1, Issue 2, 2011.

[5] Mrs. Kavitha, Kavita K., Ashwini K. and Priya D., "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun 2012.

[6] Poornima R. and Iswarya R.J., "An Overview of Digital Image Steganography", International Journal of Computer Science & Engineering Survey (IJCSES), Vol. 4, No.1, February 2013.

[7] Ms.Sravanthi G.S., Mrs.Sunitha D., Riyazoddin S.M. and Janga R., "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of Computer Science and Technology Graphics & Vision, Vol.12, Issue 15, Version 1.0, 2012.

[8] Atallah M. A., "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, No. 79, 2012.

[9] Abdelmgeid A. A. and 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.

[10] Vanmathi C. and Prabu S., "A Survey of State of the Art techniques of Steganography", International Journal of Engineering and Technology (IJET), Vol. 5, No. 1, Feb-Mar 2013.

[11] Al-Hussien S. S., "Enhancing the (MSLDIP) Image steganographic method (ESLDIP Method)", International Conference on Graphic and Image Processing (ICGIP 2011), Proc. of SPIE Vol. 8285, Issue 82853I, 2011.

[12] Abdelmgeid A. A. and Al – Hussien S. S., "New Technique for Encoding the Secret Message to Enhance the Performance of MSLDIP Image Steganography Method (MPK Encoding)", International Journal of Computer Applications, Vol. 59, No.15, December 2012.

[13] Abdelmgeid A. A. and 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.

[14] Shikha S. and Sumit B., "Image Steganography: A Review", International Journal of Emerging Technology and Advanced, Vol. 3, Issue 1, January 2013.

[15] 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.

[16] Chincholkar A.A. and Urkude D.A., "Design and Implementation of Image Steganography", Journal of Signal and Image Processing, Vol. 3, Issue 3, 2012.

[17] Chinchu E. A. and Iwin T. J., "An Analysis of Various Steganographic Algorithms", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE). Vol. 2, Issue 2, February 2013.

[18] Rosziati I. and Teoh S. K., "Steganography Imaging System (SIS): Hiding Secret Message inside an Image", Proceedings of the World Congress on Engineering and Computer Science (WCECS 2010), Vol. I, October 20-22, 2010.

[19] http://lib.bioinfo.pl/ ,"Elementary data structures: stacks, queues, lists", BioInfoBank Institute, 2010.