Using Disinformation to Promote the Security of SMMWB Image Steganography Method

Masoud E. Shaheen
Asst. Professor
Dept. of Computer Science
Faculty of Computers & Information,
Fayoum Univ., Egypt

Al – Hussien Seddik Saad
Asst. Professor
Dept. of Computer Science
Faculty of Science,
Minia Univ., Egypt

ABSTRACT

Information security researchers are interested in maintaining the secrecy, reliability and accessibility of data. The importance of information security comes from the need for protecting information and information system from unauthorized access, revelation, disruption, alteration, annihilation and use. Steganography and Cryptography are the two major techniques for information security. Steganography is the process that primarily concerned with hiding existent data in another transmission medium to achieve secret communication while Cryptography is about hiding the content of the message or scrambling it. However, steganography does not take the place of cryptography but rather boosts the security using its obscurity features. In this paper, the security of a previously proposed image steganography method SMMWB (Secret Message Matching With Braille) will be promoted by using the principle of disinformation instead of encryption as previously proposed methods, which means if the image steganography method has been steganalysed the eavesdropper will be able to read a fake secret message,he has been implicitly directed to read, not the real one.

Keywords

Image Steganography, Hiding Data in Digital Images. Spatial Domain Image Steganography, Text Steganography, Information Security.

1. INTRODUCTION

Authors are asked to follow some simple guidelines. In essence, you are required to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

Nowadays, due to the continuous increase of digital multimedia transmissions on the network, some important data needs to be protected during transmission. Therefore, a research topic on how the secret messages can be protected from being stolen during transmission becomes essential for studying. There are two ways to solve this problem: cryptography and steganography.

There are many common technical approaches that have a great deal of overlapping and share between Cryptography and steganography. On the other hand, there are fundamental philosophical differences that affect the requirements, thus the formulation of a technical solution will be affected too [1]. Due to this overlapping between the two fields, it has been decided to discuss fleetingly each field.

Cryptography is the process or skill of communicating in or ciphering secret writings [2]. In practice, cryptography is the science of using mathematics to encode and decode data. It allows you to store sensitive information or transmit it across public insecure channel (the internet, GSM for examples) so that, it cannot be read by anyone excluding the intended recipient using the right key [3] [2].

In fact, an understanding of cryptography starts with a basic understanding of some important terminology: -

- **Plaintext**: refers to any type of information in its primary unedited original, readable, unencrypted form. A data base document, an image file, and an executable file are all considered plaintext documents [3].

- **Cipher text**: refers to a message in its encrypted form, what some people refer to as garbled information that has been encoded into secret writing. The meaning of the information in cipher text is concealed; see Fig. 1 [3].

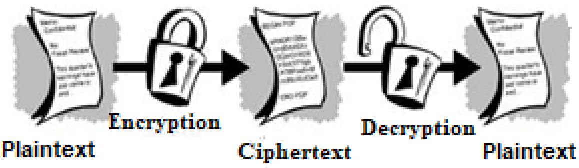

Fig 1: Encryption and Decryption

That is why encryption is the process of specifying a plaintext message and converting it into cipher text in order to ensure that, the information is hidden from anyone for whom it is not proposed, even those who can see the encrypted data. In contrast, "decryption" can be defined as the opposite of encryption which takes a cipher text that was written secretly and converts it into plaintext [3] [2].

Actually, there are some Cryptographic problems that led to the use of steganography; the first problem is that many countries issued laws and regulations on the rules of using encrypted data. Therefore, these countries proposed legislations that give the governments the authority to monitor any online communication. Some countries can send you to prison if you decline to give up your key to decrypt data [2].

Another problem is that, the cipher text looks pointless [4], this in turn appeals attention and makes the text mistrustful looking [5]. So, the attacker will interrupt the transmission or make more cautious checks on the data from the sender to the receiver [6]. Although the attacker cannot be able to remove the encryption, it is relatively easy to modify the file making it unreadable for the proposed receiver [7].

On the other hand, steganography is one of the methods which became highly recommended during the recent years. It is a word derived from the ancient Greek words "steganos", which means covered and "graphia", which in turn means writing. It can be defined as the process that primarily concerned with hiding existent data in another transmission medium to achieve secret communication such that its presence cannot be detected by attackers [6] [2] [8] or, it is the study of methods for hiding the existence of secondary message in the presence of a main message. The main message is referred to as the carrier signal or cover file; the secondary message is referred to as the payload signal or secret message [9], [10], [11].

Cover file (Carrier): It is defined as the original file into which the required secret message is embedded. It is also named as host file. The secret message should be embedded in such a way that there are no substantial changes in the structures of the cover file.

Payload (Message): It is the secret massage that has to be embedded inside the cover file in a given Steganographic model. The payload can be in the form of text, audio, images, or video. Encryption of payload may be done not only to protect data, but can also be used for authentication and increase security level [12].

Stego file (stego-object): It is the finishing file obtained after embedded the payload into a given cover file. It should have similar structures to that of the cover file.

Hiding capacity: It is the size of information that can be hidden relative to the occupying space of the cover without breaking down the quality of the cover file.

Stegokey: It is a password that may be used to encode the secret information to provide an extra level of security [13], [14], [15].

Now, the basic types of steganography will be briefly discussed. Actually, there are two basic types, linguistic steganography and technical steganography.

Linguistic steganography is an art of hiding secret messages. More specifically, it is concerned with analyzing the characteristics of language, such as the linguistic structure to hide messages. Or linguistic steganography can be termed quite simply as any form of steganography that uses language in the cover [16]. Methods for linguistic steganography are frequently of linguistically-driven generation or modification.

While technical steganography is a little wider in scope because it does not essentially deal with the written word even though it communicates information. Technical steganography is the technique of steganography where a tool, device, or technique is used to hide the message. In reality, linguistic steganography could be considered technical steganography because it is a method. It can be classified into: text, image, audio, video steganography. But in this paper, image and text steganography will be discussed in brief as they are involved in this research.

Digital image files are one of the most common types of cover objects used in modern digital steganography. These types of files are easy for any computer user to find or produce, and are predominant enough in the world of computers that their existence alone does not warrant suspicion and that it would in practical to check every such file for hidden messages [17].

Actually, there are two common methods of embedding in image steganography: Spatial domain methods in which messages are inserted into the image pixels, and transform domain methods in which a message is embedded in the pixels cover image that has been transformed [17].

Spatial domain methods embed data by substituting carefully chosen bits from the cover image pixels with secret message bits. LSB-based techniques (Least Significant Bit) are the most broadly known steganography algorithms, which work by substituting the least significant bits of an image pixel.

Whereas transform domain methods, modify the transform coefficients of the image. The transform coefficients are obtained by applying transforms, such as the Fourier transform, discrete cosine transform or the wavelet transform, to the image.

On the other hand, text steganography use text as the medium in which information to be hidden. The definition of text steganography remains comprehensive in order to distinguish it from the more specific “linguistic steganography”. Text steganography can include anything from altering the formatting of an existing text, to altering words within a text, to generating random character sequences or using context-free grammars to produce readable texts [18].

Using any of these techniques/methods, the common denominator is that hidden messages are embedded in character-based text [18].

Some methods/techniques of text steganography are Open-Space Method, Syntax method and Semantic method [16].

The open-space method uses white space on the printed page, for example, Inter - sentence spacing, End-of-line spacing and Inter-word spacing

The Syntactic method; deriving from "syntax," this method uses the manipulation of punctuation to conceal information. Syntactic is a method that uses punctuations and contradictions [16].

For example:

Dough, cereal, and milk
Dough, cereal and milk

Finally, the Semantic Method; a last category of data hiding in text includes changing the words themselves. Semantic methods and syntactic method are similar. Rather than encoding binary data by exploiting ambiguity of form, these methods assign two synonyms main or secondary value [16].

For example, the word "big" could be considered main value and "large" secondary. Whether a word has main or secondary value bears no relevance to how often it will be used, but main words will be read as ones, secondary words as zeros when decoding [16].

After briefly discussing image and text steganography, now one of the most important steganography problems will be discussed. Of course, steganography is not perfect, no security technology is. Even though a message is concealed by stego, if someone knows it is there and knows the algorithm that was used to conceal it, and if the message is not encrypted, he or she can read it. Even if the message is encrypted/coded, it can decrypted (decoded), modified or even destroyed [2].

As stated before, steganography and cryptography are both methods to protect information from undesirable parties but neither technology alone is perfect and compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can be amplified by combining it with cryptography. So, cryptography is used to supplement steganography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of security [19].

However, there is a problem, if the steganography algorithm is steganalysed and the encrypted text extracted from the image, the eavesdropper will try to crack or decrypt it as well. So, this layer of security which encrypts the secret message will make the eavesdropper more interested in knowing the original secret message, because-as it has been said before, one of the disadvantages of encryption is that the cipher text looks meaningless and attracts attention. If the cracker cannot decipher it, it can be destroyed.

But in this proposed layer of security the principle of disinformation is used by adding a text steganography layer in place of the encryption layer, which means if the steganography algorithm has been steganalysed, the eavesdropper will see a readable fake message and he will not doubt for a moment that the message holds another message inside. So, the only intended person who will be able to read the real secret message from the fake secret message because he is the only one knows about it.

Finally, this paper is organized as follows. Section I provides a brief introduction about cryptography, image steganography and text steganography. Section II discuss some previously proposed methods that tried to enhance the security of image steganography methods by using encryption. In section III, the related works have been presented briefly. Section IV explains in details the proposed method. Section V contains the results and discussion. Finally, section VI concludes the paper.

2. PREVIOUS WORK

In this section, some previously proposed image steganography methods will be discussed. These methods tried to enhance the security of image steganography method by adding an encryption layer before the steganography algorithm.

In [20], a model which combines cryptographic and steganographic techniques presented. These two techniques encrypt the data as well as hide the encrypted data in another medium so the fact that a message being sent is concealed. In cryptography they used a Simplified Data Encryption Standard (S-DES) algorithm to encrypt secret message and then a steganography method is used to hide encrypted message.

Also in [21], the authors established a high security model by combining cryptographic and steganographic security. In cryptography they were using Advanced Encryption Standard (AES) algorithm to encrypt secret message and then pixel value differencing (PVD) with K-bit least-significant-bit (LSB) substitution was used to hide encrypted message into true color RGB image.

Moreover, in [22] the authors developed an algorithm for RGB image based steganography (for BMP image) and for betterment of security dual level of security protocols have been used in this algorithm. Where first phase was encrypting the file with International Data Encryption Algorithm (I.D.E.A) and the second phase was inserting the data bit by bit in the carrier image.

Also in [23], the authors enriched the security by encrypting the secret message by using AES Encryption (Advanced Encryption Standard) and embedded within skin region of image using an image steganographic algorithm.

Moreover, in [24] the authors suggested an algorithm that is using two layers of security to maintain the privacy, confidentiality and accuracy of the data. For hiding the data, a username and password were required prior to use the system. Login information is used together with the secret key to hide the data inside the selected Image. Finally, the secret message has been compressed (Zip file). The purpose of zipping the file is because the zipped text file is more secured, then the zipped file converted into binary and hidden in the cover image.

As shown in these methods, almost all of the previous attempts try to enhance the security of image steganography methods - by adding a layer of security using an encryption algorithm on the secret message before hiding it in the cover image. But the problem is, as stated before, if the image steganography algorithm has been steganalysed and the secret message has been shown to be encrypted, the eavesdropper will also try to decrypt the message or in the worst case alter it or destroy it because he was not capable to read it.

3. RELATED WORK

In this section, two steganography methods, formerly suggested, will be the topic outlined in this paper. Instead of encoding before enveloping the secret message in the cover message, "New Text Steganography Technique by Using Mixed-Case Font" [25] will work as a shield, this is the first method. The second one is the image steganography method which depends on a protection layer called “Enhancing SMM Image Steganography Method by LSBraille Image Steganography Method. (SMMWB; Secret Message Matching with Braille) [19].

In [25], the new suggested text steganography targets the text file which carries the secret message data so that the consequent document unnoticeably has identical meaning of the initial file. It is mainly through transforming the alphabets letters-case from capital to small letters and vice versa that this method functions. The hidden message is turned into a flow of bits and marked with the cover text, so every letter reacts to 0 is a small letter and every letter reacts to 1 is a capital letter and so on. In other words, the cover text will have precisely 7 letters in which every secret letter is embedded. Hence, an enormous amount of secret messages inserted in a cover text in contrast to other text steganography methods.

In [19], the authors suggested an image steganography method on the basis of the formerly proposed one; SMM image steganography method (Image Steganography by Matching Secret Message with Pixels of Cover Image or, Secret Message Matching) [26] is a method that works by attributing Alpha channel to a 255-pixel image; suggesting a completely transparent channel, turning the R,G ,B channels of the cover image into search spaces, inspecting these secret numbers in the search spaces of the cover image, in case these numbers were discovered, the index is inserted in the correspondent Alpha pixel by utilizing Least Significant Bit (LSB) method. Otherwise, new search space will be experienced. The second one is LSBraille image steganography method (Image Steganography Method by Using Braille Method of Blind People) [27], this method depends on using Braille reading and writing of blind people which represents the secret message characters, thus, it saves more than one-fourth of the needed embedding space. The suggested method utilizes Braille characterization as each character is represented by specifically 6 dots using the 6-dots matrix (Braille Cell). In this way, the SMMWB method will function as follows: SMM method will launch, then ask if the whole message is embedded or not. If the whole message is not inserted, the LSBraille method will work by pursuing the fixed alpha pixels (Alpha = 255) and the method will utilize the search spaces matching these Alpha pixels to embed the rest of secret digits in.

4. PROPOSED METHOD

In this section, the proposed method will be presented; it is the method that enhances the security of SMMWB image steganography method by using text steganography method. As it has been said before, almost all previously proposed methods use the encryption of the secret message as a layer of security before embedding, and the problem is that after the steganalysis of the steganography algorithm the eavesdropper becomes more interested in cracking the cipher text, modifying --or deleting it.

Here in our proposed method after the steganalysis of the steganography algorithm, the eavesdropper will be able to read the fake secret message which is a stego text not a secret text. So, this layer of security is a disinformation layer for the eavesdropper.

Disinformation term is defined in the Wikipedia as intentionally false or inaccurate information--spread deliberately. It is an act of deception and false statements to convince someone of the untruth. Disinformation should not be confused with misinformation; information that is unintentionally false. So, the principle of disinformation is achieved by using a fake secret message based on text steganography.

The proposed method will be divided into three sides not two sides (sender and receiver) as other steganography methods. In other steganography methods, the attacker and the receiver sides are the same because the security layer can be breached. But in our proposed method the attacker cannot notice that there is a security layer to be breached.

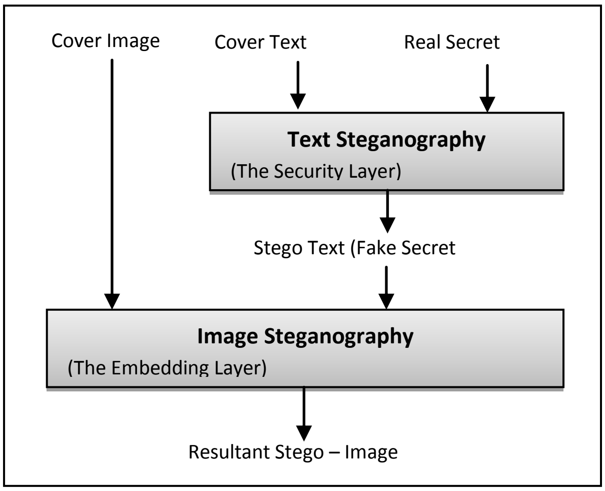

Fig 2: Sender Side

First of all, at the sender side, as in fig. 2, the first step is that the sender will choose the real secret message, the cover text and the cover image, then the real secret message and the cover text will fed as inputs to the text steganography algorithm (the security layer) and the output will be the stego text or the fake secret message. Then the fake secret message and the cover image will feed as inputs to the image steganography algorithm (the embedding layer) and the output will be the stego image that will be sent over the insecure channel.

Secondly, from the attacker party, as in fig.3, (Attacker Limits), the eavesdropper will attempt to steganalyse the hidden image. Once succeeded, the message is readable for the attacker. so the eavesdropper will not try to steganalyse it one more time or crack it as in the encryption layer and he will stop at this limit. While at the receiver side, as in fig. 3 (Receiver Limits), the receiver is aware of the disinformation layer that has been added to the algorithm and he will reach to the real secret message.

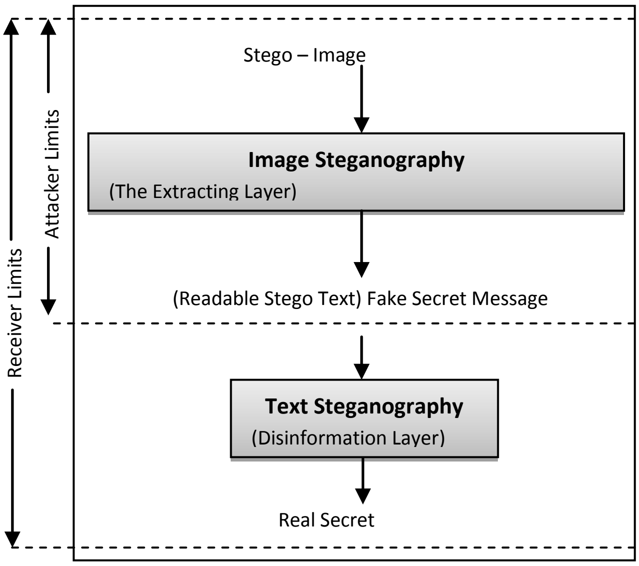

Fig 3: Attacker and Receiver Sides

And here are the encoding and the decoding algorithms:-

Algorithm 1: *Secured SMMWB Encoding Algorithm*

Input:

Cover Image **CI**, Real Secret Message **RM**, Cover Text **CT**.

Output:

Stego - Image **SI**.

Steps:

1) **CI**, **RM** and **CT** will be inputted into the encoder system by the sender.
2) **RM** will be embedded in **CT** by using the text steganography algorithm, the output will be the Stego Text **ST**.
3) **ST** will be embedded in the **CI** by using the image steganography algorithm, the output will be SI.
4) **SI** will be sent over an insecure channel.

Algorithm 2: *Secured SMMWB Decoding Algorithm*

Input:

Stego - Image **SI**.

Output:

Real Secret Message RM.

Steps:

1) **SI** will be inputted into the decoder system by the receiver.
2) **SI** will feed into the image steganography algorithm; the output will be the Fake Secret

Message FM.

3) **FM** will feed into the text steganography algorithm; the output will be the Real Secret Message **RM**.

5. RESULTS AND DISCUSSION

In fact, while all previously discussed papers suggesting security improvement of image steganography, tangible results that should be seen during adding the security layer to the steganography system or improving its security does not exist. That is why the discussed SMMWB system that utilizes disinformation has been tested through taking the real secret message, the cover text and the cover image. Here are details about the system and how it functions.

Actually, as all of previously proposed papers dealing with security enhancement of image steganography, there are no results' tables to be shown while adding a security layer to the steganography system or enhancing the security of it. So, the proposed SMMWB system using Disinformation has been tested by taking the real secret message, the cover text and the cover image and here is the detailed example of the system and how it worked.

Suppose that the **Real Secret Message** is "*Password is: AAA*", and the **Cover Text** is "*This information is classified, we will postpone our meetings to the next Monday at seven pm, you can come and get the money with you, waiting your reply today*", then the **Resultant Stego Text (Fake Secret Message)** will be "*tHiS inforMAtion Is CLAssIFiED. We wILl POStPONe OUr MEETiNGS to The NExt MondaY at seveN Pm. You CaN COme ANd gET ThE monEy with yOu. waitInG your rEpLy todaY*".

Then the **Fake Secret Message** plus the **Cover Image** chosen by the sender, suppose it is a Lena image, will feed into the **SMMWB** image steganography method, and then the resultant image will be the **Stego Image** that will be sent by the sender.

At the attacker side, the attacker will try to steganalyse the stego image (steganography algorithm) and if he succeeded, the message that he will read will be "*tHiS inforMAtion Is CLAssIFiED. We wILl POStPONe OUr MEETiNGS to The NExt MondaY at seveN Pm. You CaN COme ANd gET ThE monEy with yOu. waitInG your rEpLy todaY*" which is the fake secret message.

While, at the receiver side, the receiver will access the real secret message which has "Password: AAA". So, the disinformation has been achieved, as there are two secret messages one for the attacker which is the fake message and the other --for the receiver which is the real one.

6. CONCLUSION

In this paper, security reinforcement has been made to the previously discussed image steganography method SMMWB (Secret Message Matching with Braille) by utilizing the idea of disinformation fulfilled by adding a text steganography layer before hiding the secret message into the cover image.

According to Wikipedia, disinformation is deliberately misleading information -- developed on purpose. It is an act of imposition to persuade someone of a trick.

If the stego image is steganalysed, the eavesdropper will read a fake secret message (Readable stego–text) that will convince the eavesdropper that he reached the real secret message successfully. But the eavesdropper did not know that he red what he is implicitly was directed to read not the real secret message.

So, the eavesdropper is disinformed and only the receiver will know that there is another layer of security or there is a real secret message inside this fake secret message.

In the result and discussion section, the instance explains two secret messages; the first one is the fake secret massage which is formed by the disinformation layer and the second one is the real secret message.

An important note is that, this technique can be applied by using any other text steganography and image steganography methods.

By using this technique, the problem of the cipher text which is attracting attention has disappeared and the security raised to its maximum because the eavesdropper will not be aware of that, the readable message contains another readable message inside.

7. REFERENCES

[1] I. J. Cox, m. L. Miller, J. A. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography", ISBN 978-0-12 372585-1, 2nd edition, Elsevier inc, 2008.

[2] E. Cole, "Hiding In Plain Sight: Steganography and The Art of Covert Communication", ISBN 0-471-44449-9, Wiley publishing, inc, 2003.

[3] An Introduction to Cryptography, Network Associates, Inc. and its Affiliated Companies, 3965 Freedom Circle, Santa Clara, CA 95054, 1999.

[4] I. V. S. Manoj, "Cryptography and Steganography", International Journal of Computer Applications, volume 1 - no. 12, pp. 61 - 65, 2010.

[5] K. Gopalan and Q. Shi, "Audio Steganography Using Bit Modification – A Tradeoff On Perceptibility and Data Robustness for Large Payload Audio Embedding", 978-1-4244-7115-7/10, IEEE, 2010.

[6] G. Liu, Y. Dai, and Z. Wang, "Breaking Predictive-Coding Based Steganography and Modification For Enhanced Security", IJCSNS International Journal of Computer Science and Network Security, vol. 6 no. 3b, pp. 144 - 149, Mar 2006.

[7] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, vol. 1, no. 3, pp. 137-14, 2009.

[8] N. Cvejic, "Algorithms for Audio Watermarking and Steganography", ISBN 951-42-7383-4 (nid.) ISBN 951-42 7384-2 (PDF), Oulu University press, 2004.

[9] A. T. Al-Taani and A. M. Al-Issa, "A Novel Steganographic Method for Gray- Level Images", International Journal of Computer, Information, Systems Science, and Engineering, pp. 5 - 10, 2009.

[10] S. K. Muttoo and S. Kumar, "Data Hiding in JPEG Images", Bvicam's International Journal of Information Technology, pp. 13 - 16, BIJIT - 2008.

[11] A. E. Ali, "A New Text Steganography Method By Using Non Printing Unicode Characters", Eng. & Tech. Journal, vol. 28, no. 1, pp. 72 - 83, 2010.

[12] H. S. M. Reddy and K. B. Raja, "High Capacity and Security Steganography Using Discrete Wavelet

Transform", International Journal of Computer Science and Security (IJCSS), vol. 3, issue 6, pp. 462 - 472.

[13] Y. Srinivasan, "High Capacity Data Hiding System Using BPCS Steganography", Electrical Engineering, Faculty of Texas Tech University, M.Sc. Thesis, December, 2003.

[14] S. Anguraj, D. Balamurugan, "Implementation Of Audio Steganography In Real-Time Protocol (RTP) and Hypothesis of RTP Features", 1st National Conference on Intelligent Electrical Systems (NCIES'09), pp. 181 - 185, 24-25 April 2009.

[15] B. W. Ford, "File Format Extension Through Steganography", Texas State University-San Marcos, Dept. of Computer Science, M.Sc. Thesis, January 5, 2010.

[16] G. Kipper, "Investigator's Guide to Steganography", ISBN 0849324335, Auerbach publications, 2004.

[17] E. J. Farn and C. C. Chen, "Jigsaw Puzzle Images For Steganography", Optical Engineering vol. 48, no. 7, pp. 1 - 12, July 2009.

[18] K. Bennett, "Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information In Text", CERIAS Tech Report 2004-13, Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907-2086.

[19] A. A. Ali and A. H. Seddik, " Enhancing SMM Image Steganography Method by using LSBraille Image Steganography Method (SMMWB; Secret Message Matching With Braille)", International Journal of Computer Applications (0975 – 8887), Volume 70– No.8, May 2013.

[20] A. Agarwal, "Security Enhancement Scheme for Image Steganography using S-DES Technique", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 4, April 2012.

[21] P. Vitthal, B. Rajkumar and P. Archana, " A Novel Security Scheme for Secret Data using Cryptography and Steganography", I. J. Computer Network and Information Security, 2012, 2, 36-42.

[22] N. Bagchi and "Secure BMP Image Steganography Using Dual Security Model (I.D.E.A, image intensity and Bit Randomization) and Max-Bit Algorithm", International Journal of Computer Applications (0975 - 8887),Volume 1 – No. 21, 2010.

[23] M. gowtham, T. Senthur, M. Sivasankaran, M. Vikram and B. Sreeja, " AES BASED STEGANOGRAPHY", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 1, January 2013.

[24] R. Ibrahim and T. Suk, "Steganography Imaging System (SIS): Hiding Secret Message inside an Image", Proceedings of the World Congress on Engineering and Computer Science 2010 Vol I, WCECS 2010, October 20-22, 2010, San Francisco, USA.

[25] A. A. Ali and A. H. Seddik, " New Text Steganography Technique by using Mixed-Case Font", International Journal of Computer Applications (0975 – 8887) Volume 62– No.3, January 2013.

[26] A. A. Ali and A. H. Seddik, " 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)ISSN 2249-6831 Vol. 3, Issue 2, Jun 2013, 1-10 © TJPRC Pvt. Ltd.

[27] A. A. Ali and A. H. Seddik, " Image Steganography Technique By Using Braille Method of Blind People (LSBraille)", International Journal of Image Processing (IJIP), Volume (7) : Issue (1) : 2013.