Journal of Applied Sciences

ISSN 1812-5654

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 10 (18): 2094-2100, 2010
ISSN 1812-5654

An Overview on Hiding Information Technique in Images

[1]Ali K. Hmood, [2]B.B. Zaidan, [2]A.A. Zaidan and [1]Hamid A. Jalab
[1]Faculty of Computer Science and Information Technology,
University Malaya, 50603 Kuala Lumpur, Malaysia
[2]Faculty of Engineering, Multimedia University, Jalan Multimedia, 63100 Cyberjaya, Malaysia

Abstract: In the last few years, we have seen many new and powerful steganography techniques reported in the literature. Steganography is the art of communicating a message by embedding it into multimedia data. It is desired to maximize the amount of hidden information (embedding rate) while preserving security against detection by unauthorized parties. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this study intends to offer a state of the art overview of the hiding information technique using image file as a cover carrier to illustrate the possibility of using the image for hiding secure information for business and personal use.

Key words: Steganography, hiding information, image domain, transform domain

INTRODUCTION

Since, the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Thus the definition (Steganography) the art of concealment and transfer data through the data again host or carrier, but harmful harmless transmitters for those data do not allow any enemy or observers to discover that there is confidential data (Ahmed *et al.*, 2010).

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret (Wang and Wang, 2004). Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated (Wang and Wang, 2004). The strength of steganography can thus be amplified by combining it with cryptography (Zaidan and Zaidan, 2009).

Two other technologies that are closely related to steganography are watermarking and fingerprinting (Anderson and Petitcolas, 1998). These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are marked in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection (Marvel *et al.*, 1999). With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties (Anderson and Petitcolas, 1998).

In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge-sometimes it may even be visible-while in steganography the imperceptibility of the information is crucial (Wang and Wang, 2004). A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file,

Corresponding Author: Ali K. Hmood, Faculty of Computer Science and Information Technology, University Malaya, 50603 Kuala Lumpur, Malaysia

while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it (Anderson and Petitcolas, 1998).

STEGANOGRAPHY

The word steganography comes from the Greek Steganos, which mean covered or secret and -graphy mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening (Al-Azawi and Fadhil, 2010). Secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges.

For example ancient Greece used methods for hiding messages such as hiding. In the field of Steganography, some terminology has developed. The adjectives cover, embedded and stego were defined at the information hiding workshop held in Cambridge, England (Naji *et al*., 2009a). The term cover refers to description of the original, innocent massage, data, audio, video and so on. Steganography is not a new science; it dates back to ancient times (Zaidan *et al*., 2008). Another ingenious method was to shave the head of a messenger and tattoo a message or image on the messenger head. After allowing his hair to grow, the message would be undetected until the head was shaved again. While the Egyptian used illustrations to conceal message. Hidden information in the cover data is known as the embedded data and information hiding is a general term encompassing many sub disciplines, is a term around a wide range of problems beyond that of embedding message in content (Zaidan *et al*., 2010; Naji *et al*., 2009b). The term hiding here can refer to either making the information undetectable or keeping the existence of the information secret (Jalab *et al*., 2009; Shirali-Shahreza and Shirali-Shahreza, 2008).

Information hiding is a technique of hiding secret using redundant cover data such as images, audios, movies, documents, etc. (Zaidan *et al*., 2009). This technique has recently become important in a number of application areas. For example, digital video, audio and images are increasingly embedded with imperceptible marks, which may contain hidden signatures or watermarks that help to prevent unauthorized copy. It is a performance that inserts secret messages into a cover file, so that the existence of the messages is not apparent.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed.

The term of hide information is the process of covering the secrete message or information multimedia files to make sure there is no other party can disclose or altering it (Hmood *et al*., 2010; Majeed *et al*., 2009). Under this topic we can drive two techniques which are used to hide information one is digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove, the signal may be audio, pictures, video or text files; its mostly used for demonstrate the intellectual property rights purpose such as adding copy right logo or text (author signature) for multimedia files. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Since the main use for steganography is to send secure messages between parties, then it's aim to prevent the message being detected by any other party (Al-Frajat *et al*., 2010; Kawaguchi and Eason, 1998).

The digital multimedia files steganography uses code fields for unimportant bits as places to hide encoded messages or images. While such manipulation might slightly alter the quality of the original image, it generally goes unnoticed by the naked eye. During the process characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Capacity, confidentiality and robustness, are the three main aspects affecting steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Confidentiality relates to the ability of the discloser to figure the hidden information easily. Robustness is concerned about the resist possibility of modifying or destroying the unseen data.

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display (Currie and Irvine, 1996). The redundant bits of an object are those bits that can be altered without the alteration being detected easily (Anderson and Petitcolas, 1998). Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of multimedia file formats that can be used for steganography.

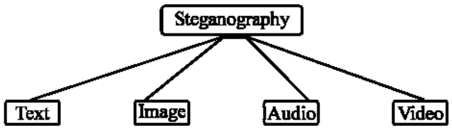

Fig. 1: Steganography in multimedia files

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every *nth* letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance (Silman, 2001). Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

Given the proliferation of digital images, especially on the Internet and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound (Silman, 2001).

This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images (Artz, 2001).

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

IMAGE STEGANOGRAPHY

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image (Johnson and Jajodia, 1998a). This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour (Owens, 2002). These pixels are displayed horizontally row by row.

The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel (Owens, 2002). The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel (Owens, 2002). Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour (Owens, 2002). All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue and each primary colour is represented by 8 bits (Johnson and Jajodia, 1998b). Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16 million combinations, resulting in more than 16-million colours (Owens, 2002). Not surprisingly the larger amount of colours that can be displayed, the larger the file size (Owens, 2002).

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain (Silman, 2001). Image - also known as spatial - domain techniques embed messages in the intensity of the pixels directly, while for transform - also known as frequency - domain, images are first transformed and then the message is embedded in the image (Lee and Chen, 2000).

Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterised as simple systems (Johnson and Jajodia, 1998b). The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format (Venkatraman *et al*., 2004).

Steganography in the transform domain involves the manipulation of algorithms and image transforms (Johnson and Jajodia, 1998a). These methods hide messages in more significant areas of the cover image, making it more robust (Wang and Wang, 2004). Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression (Venkatraman *et al*., 2004). In the next sections steganographic algorithms will be explained in categories according to image file formats and the domain in which they are performed. Figure 2 indicate the possibility of using images as a cover carrier.

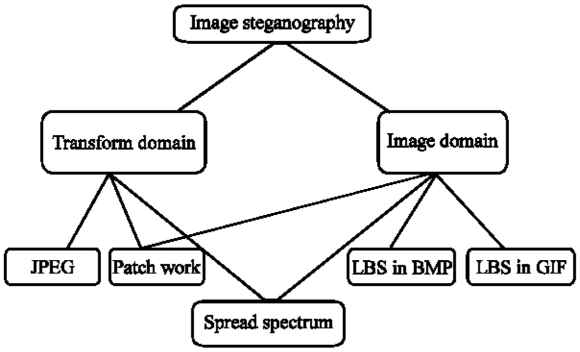

Fig. 2: Image based steganography

SUBSTITUTION SYSTEMS

Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits. The receiver can extract the information if he has knowledge of the positions where secret information has been embedded. Since only minor modifications are made in the embedding process, the sender assumes that they will not be noticed by an attacker. It consists of several techniques that will be discussed in more detail, in the following subsection:

LEAST SIGNIFICANT BIT SUBSTITUTION (LSB)

The embedding process consists of choosing a subset {j1… jl(m)} of cover elements and performing the substitution operation cji _ mi on them, which exchange the LSB of cji by mi (mi can be either 1 or 0). In the extraction process, the LSB of the selected cover-element is extracted and lined up to reconstruct the secret message.

In the case of a 24-bit bitmap each pixel is represented by 4 bytes. Of those, 3 bytes, or 24 bits, are used to store the red, green and blue values for the pixel. The fourth byte is reserved and should be zero. To store each character in the low order bit plane of the raster data, it is necessary to obtain an 8 bit representation of the character. For example, the character A is represented by the number 65. The equivalent binary representation is 0100 0001. Each of the 8 bits used to represent the letter A is then stored in the low order bit of one byte of raster data. Thus, to store a single letter, 8 bytes of raster data are consumed. This leads to a limit of embeddable information of size lengthOfRasterData/8. Consider hiding the letter A in the first 8 bits of raster data of an image. The first 8 bytes could possibly be (from left to right, top to bottom):

‘1001 1001’ ‘1110 0011’ ‘0110 1001’ ‘0001 1100’
‘0001 1100’ ‘0110 0100’ ‘1011 0000’ ‘1010 1001’

And the character A is:

‘0100 0001’

Therefore, we need to set bits 7, 5, 4, 3, 2 and 1 to zero, this is accomplished by AND with the mask ‘1111 1110’. The result for the first byte is:

```
        ‘1001 1001’
AND     ‘1111 1110’
        ‘1001 1000’
```

So, the low order bit is set to ‘0’. This is repeated for all bits that will be set to carry a ‘0’.

We now need to set bits 6 and 0 to ‘1’. This is accomplished by OR with the mask ‘0000 0001’. The result for the second byte is:

```
        ‘1110 0011’
OR      ‘0000 0001’
        ‘1110 0011’
```

Although the resulting bit has not changed, we have ensured that the least significant bit has been set to ‘1’. Because the byte values for the red, green and blue pixels will only change by at most 1, the change in the resulting image will be imperceptible to the human eye. The resulting image will not, however, be well protected against statistical attack.

PSEUDORANDOM PERMUTATION

If all cover bits are accessed in the embedding process, the cover is a random access cover and the secret message bits can be distributed randomly over the whole cover. This technique further increases the complexity for the attacker, since it is not guaranteed that the subsequent message bits are embedded in the same order.

IMAGE DOWNGRADING AND COVER CHANNELS

Image downgrading is a special case of a substitution system in which image acts both as a secret message and a cover. Given cover-image and secret image of equal dimensions, the sender exchanges the four least significant bits of the cover grayscale (or colour) values with the four most significant bits of the secret image. The receiver extracts the four least significant bits out of the stego-image, thereby gaining access to the most significant bits of the stego-image. Whereas, the degradation of the cover is not visually noticeable in many cases, four bits are sufficient to transmit a rough approximation of the secret image.

COVER REGIONS AND PARITY BITS

Any nonempty subset of {c1,……..,cI(c)} is called a cover-region. By dividing the cover into several disjoint regions, it is possible to store one bit of information in a whole cover-region rather than in a single element. A parity bit of a region I can be calculated by:

B (I) ==_LSB (cj) mod2 [27]   j€I

PALETTE-BASED IMAGE

There are two ways to encode information in a palette-based image; either the palette or the image data can be manipulated. The LSB of the colour vectors could be used for information transfer, just like the substitution methods presented. Alternatively, since the palette does not need to be sorted in any way, information can be encoded in the way the colours are stored in the palette. For N colours since there are N! Different ways to sort the palette, there is enough capacity to encode a small message. However, all methods which use the order of a palette to store information are not robust, since an attacker can simply sort the entries in a different way and destroy the secret message.

QUANTIZATION AND DITHERING

Dithering and quantization to digital image can be used for embedding secret information. Some Steganographic systems operate on quantized images. The difference between adjacent pixels xi and xi +1 is calculated and fed into a quantize á which outputs a discrete approximation ΔI of the different signal (xi - xi +1). Thus in each quantization step a quantization error is introduced. In order to store the ith message bit in the cover-signal, the quantized difference signal ΔI is computed. If according to the secret table ΔI does not match the secret bit to be encoded, ΔI is replaced by the nearest ΔI where the associated bit equals the secret message bit. The resulting value ΔI is those fed into the entropy coder. At the receiver side, the message is decoded according to the difference signal ΔI and the stego-key.

TRANSFORM DOMAIN TECHNIQUES

It has been seen that the substitution and modification techniques are easy ways to embed information, but they are highly vulnerable to even small modification. An attacker can simply apply signal processing techniques in order to destroy the secret information. In many cases even the small changes resulting out of loose compression systems yield total information loss. It has been noted in the development of Steganographic systems that embedding information in the frequency domain of a signal can be much more robust than embedding rules operating in the time domain. Most robust steganographic systems known today actually operates in some sort of transform domain.

Transformation domain methods hide message in a significant area of the cover image which makes them more robust to attack, such as adding noise, compression, cropping some image processing. However, whereas they are more robust to various kinds of signal processing, they remain imperceptible to the human sensory system. Many transform domain variations exist. One method is to use the Discrete Cosine Transformation (DCT) as a vehicle to embed information in image. Another method would be the use of wavelet transforms.

Transforms embedding embeds a message by modification (selected) transform (e.g., frequency) coefficient of the cover message. Ideally, transform embedding has an effect on the spatial domain to apportion the hidden information through different order bits in a manner that is robust, but yet hard to detect. Since an attack, such as image processing, usually affects a certain band of transform coefficient, the remaining coefficient would remain largely intact. Hence, transform embedding is, in general, more robust than other embedding methods.

SPREAD SPECTRUM (SS) TECHNIQUES

Spread spectrum techniques are defined as Means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information.

The band spread is accomplished by means of a code which is independent of the data and a synchronized reception with the code at the receiver is used for dispreading and subsequent data recovery. Although, the power of the signal to be transmitted can be large, the signal-to-noise ratio in every frequency band will be small, even if parts of the signal could be removed in several frequency bands, enough information should be present in the other bands to recover the signal. This situation is very similar to a steganography system which tries to spread a secret message over a cover in order to make it impossible to perceive. Since spread signals tend to be difficult to remove, embedding methods based on SS should provide a considerable level of robustness.

In information hiding, two special variants of spread spectrum techniques are generally used: direct sequence and frequency-hopping scheme. In direct-sequence scheme, the secret signal is spread by a constant called ship rate, modulated with a pseudorandom signal and added to the cover. On the other hand, in the frequency-hopping schemes the frequency of the carrier signal is altered in a way that it hops rapidly from one frequency to another. SS are widely used in the context of watermarking.

STATISTICAL STEGANOGRAPHY

Statistical steganography techniques utilize the existence of 1-bits steganography schemes, which embed one bit of information in a digital carrier. This is done by modifying the cover in such a way that some statistical characteristics change significantly if a 1 is transmitted. Otherwise, the cover is left unchanged. So the receiver must be able to distinguish unmodified covers from modified ones. A cover is divided into l(m) disjoint blocks B1...... B l(m). A secret bit, mi is inserted into the ith block by placing 1 into Bi if mi = 1.

Otherwise, the block is not changed in the embedding process.

IMAGE BASED STEGANOGRAPHY ISSUES AND CONSIDERATION

Eve controls the communication between Alice and Bob and is willing to interrupt certain types of communication. Ideally, Eve would inspect each message and decide whether communication is allowed or not. Thus, encrypted data is not allowed since Eve cannot decipher the content. It is assumed that all plain data is examined by Eve, although this might become difficult if the innocent traffic between Alice and Bob is large. Thus, Alice is left with the attempt to hide un-allowed messages within commonly accepted data that is also called cover data. One attractive type of cover data is natural image data, since:

- Images contain a significant amount of data, hopefully enabling high secret communication rates
- Natural image data can be modified slightly without leading to visible artifacts
- Images are in many scenarios innocent data types to Eve, e.g., Alice might be allowed to send some pictures from products of her company to Bob

Due to these properties, image steganography has been investigated quite often within the last years. However, one should also consider the fact that a really suspicious Eve can broke up the last argument and no longer allows the communication of image data between Alice and Bob if Eve learns that image steganography works. However, since this paper should be longer than two pages, we simply ignore this argumentation and consider natural image data as innocent even if image steganography works.

Thus, Alice is left with embedding her message such that the steganographic image r does not look suspicious to Eve. Eve can analyse the steganographic image r with respect to:

- The size measured in bits per pixel
- The subjective quality
- Statistical properties

The first item leads to the conclusion that uncompressed image data looks to Eve as suspicious as encrypted data. Thus, the steganographic image r has to be always in a compressed format.

CONCLUSION

The past few years have seen an increasing interest in using images as cover media for steganographic communication. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least Significant Bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. In this paper, we have discussed the possibility of using the image as a cover carrier for hiding secure data, the image based steganography issues has been illustrated.

REFERENCES

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Anderson, R.J. and F.A.P. Petitcolas, 1998. On the limits of steganography. IEEE J. Selected Areas Commun., 16: 474-481.

Artz, D., 2001. Digital steganography: Hiding data within data. IEEE Internet Comput., 5: 75-80.

Currie, D.L. and C.E. Irvine, 1996. Surmounting the effects of lossy compression on steganography. Proceedings of the 19th National Information Systems Security Conference, Oct. 22-25, Baltimore, Maryland, pp: 194-201.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Jalab, H., A. Zaidan and B.B. Zaidan, 2009. Frame selected approach for hiding data within MPEG video using bit plane complexity segmentation. J. Comput., 1: 108-113.

Johnson, N.F. and S. Jajodia, 1998a. Exploring steganography: Seeing the unseen. Computer, 31: 26-34.

Johnson, N.F. and S. Jajodia, 1998b. Steganalysis of images created using current steganography software. Proceedings of the 2nd International Workshop on Information Hiding, April 14-17, Springer Verlag, London, UK., pp: 273-289.

Kawaguchi, E. and R.O. Eason, 1998. Principle and applications of BPCS-steganography. Proc. SPIE, 3528: 464-473.

Lee, Y.K. and L.H. Chen, 2000. High capacity image steganographic model. IEEE Proc. Vision Image Signal Process., 147: 288-294.

Majeed, A., M.L.M. Kiah, H.T. Madhloom, B.B. Zaidan and A.A. Zaidan, 2009. Novel approach for high secure and high rate data hidden in the image using image texture analysis. Int. J. Eng. Technol., 1: 63-69.

Marvel, L.M., C.G. Jr. Boncelet and C. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 8: 1075-1083.

Naji, A.W., S.A. Hameed, M.R. Islam, B.B. Zaidan, T.S. Gunawan and A.A. Zaidan, 2009a. Stego-analysis chain, session two novel approach of stego-analysis system for image file. Proceedings of the International Conference on IACSIT Spring Conference, April 17-20, Singapore, pp: 398-401.

Naji, A.W., A.A. Zaidan, B.B.A. Shihab and O.O. Khalifa, 2009b. Novel approach of hidden data in the unused area 2 within exe file using computation between cryptography and steganography. Int. J. Comput. Sci. Network Secur., 9: 294-300.

Owens, M., 2002. A discussion of covert channels and steganography. SANS Institute. http://www.sans.org/reading_room/whitepapers/covert/discussion-covert-channels-steganography_678.

Shirali-Shahreza, M. and S. Shirali-Shahreza, 2008. High capacity persian/arabic text steganography. J. Applied Sci., 8: 4173-4179.

Silman, J., 2001. Steganography and steganalysis: An overview. SANS Institute. http://www.sans.org/reading_room/whitepapers/stenganography/steganography-steganalysis-overview_553.

Venkatraman, S., A. Abraham and M. Paprzycki, 2004. Significance of steganography on data security. Proceedings of the International Conference on Information Technology: Coding and Computing, April 5-7, Las Vegas, Nevada, pp: 347-347.

Wang, H. and S. Wang, 2004. Cyber warfare: Steganography vs. steganalysis. Commun. ACM., 47: 76-82.

Zaidan, B.B., A.A. Zaidan and F. Othman, 2008. Enhancement of the amount of hidden data and the quality of image. Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia.

Zaidan, A. and B. Zaidan, 2009. Novel approach for high secure data hidden in MPEG video using public key infrastructure. Int. J. Comput. Network Security, 1: 1985-1993.

Zaidan, B.B., A.A. Zaidan, A.Y. Taqa and F. Othman, 2009. An empirical study for impact of the increment the size of hidden data on the image texture. Proceedings of the International Conference on Future Computer and Communication, April 3-5, Kuala Lumpur, Malaysia, pp: 1-12.

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.