Image Steganography Techniques: An Overview

Nagham Hamid
University Malaysia Perils (UniMAP) *nagham_fawa@yahoo.com*
School of Communication and Computer Engineering
Penang, Malaysia

Abid Yahya
University Malaysia Perlis (UniMAP)
School of Communication and Computer Engineering
Perlis, Malaysia

R. Badlishah Ahmad
University Malaysia Perlis (UniMAP)
School of Communication and Computer Engineering
Perlis, Malaysia

Osamah M. Al-Qershi
School of Electrical & Electronic Engineering
University of Science Malaysia (USM)
Penang, Malaysia

Abstract

Steganography 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 it is achieved, the message does not attract attention from eavesdroppers and attackers. Using steganography, information can be hidden in different embedding mediums, known as carriers. These carriers can be images, audio files, video files, and text files. The focus in this paper is on the use of an image file as a carrier, and hence, the taxonomy of current steganographic techniques for image files has been presented. These techniques are analyzed and discussed not only in terms of their ability to hide information in image files but also according to how much information can be hidden, and the robustness to different image processing attacks.

Keywords: Adaptive Steganography, Current Techniques, Image Files, Overview, Steganography, Taxonomy.

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 development of steganography schemes. Steganography is a powerful security tool that provides a high level of security, particularly when it is combined with encryption [1].

Steganography differs from cryptography. The goal of cryptography is to secure communications by changing the data into a form that an eavesdropper cannot understand. 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 will not. Accordingly, cryptography is not the best solution for secure communication; it is only part of the solution. Both sciences can

be used together to better protect information. In this case, even if steganography fails, the message cannot be recovered because a cryptography technique is used as well [2].

Watermarking and fingerprinting, among technologies related to steganography, are basically used for intellectual property protection [3]. A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted afterwards to confirm the authenticity of the data. The watermark is hidden in the host data in such a way that it cannot be removed without demeaning the host medium. Though this method keeps the data accessible, but it is permanently marked [4]. The hidden information in a watermarked object is a signature referring to the origin or true ownership of the data in order to ensure copyright protection. In the case of fingerprinting, different and specific marks are embedded in the copies of the work that different customers are supposed to get. In this case, it becomes easy for the intellectual property owner to identify such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [5]. Consider Fig. 1, which illustrates the types of steganography.

The performance of a steganographic system can be measured using several properties. The most important property is the statistical undetectability (imperceptibility) of the data, which shows how difficult it is to determine the existence of a hidden message. Other associated measures are the steganographic capacity, which is the maximum information that can safely embedded in a work without having statistically detectable objects [6], and robustness, which refers to how well the steganographic system resists the extraction of hidden data.

Nearly all digital file formats, with a high degree of redundancy, are known for their being used for steganography, the redundant parts refer to those parts capable of change without any possibility to detect the alteration. Image and audio files satisfy this requirement particularly well [3]. In fact, digital images are the most used carrier file formats owing to their popularity on the internet. There are a number of steganographic techniques that enable one to hide a secret message in an image file, all of which have corresponding strong and weak points. Different steganographic techniques are used for different applications. Modern steganography categorizes two main classificatory schemes for the taxonomy of algorithms. The first distinguished algorithm is based on file type. The second is a more widely used scheme, where its categorization is based on an embedding technique, which is the main focus of this paper.

This paper is organized as follows. Section 2 presents a brief description of image files and some related concepts. Section 3 describes the most common examples of older steganographic techniques. Section 4 gives an overview of steganographic techniques applicable to specific image formats, including a taxonomy that classifies the techniques depending on the approach used to hide information. Section 5 describes a performance measure for the distortion caused by embedding data in an image. The steganography techniques are compared and evaluated in Section 6. Finally, Section 7 highlights and discusses the arrived at conclusions.

2. IMAGE STEGANOGRAPHY

As stated previously, images are considered as the most popular file formats used in steganography. They are known for constituting a non-causal medium, due to the possibility to access any pixel of the image at random. In addition, the hidden information could remain invisible to the eye. However, the image steganography techniques will exploit "holes" in the Human Visual System (HVS).

2.1 Image Files

An image is defined as an arrangement of numbers and such numbers usually stand for different light intensities in different parts of the image [7]. The numeric description takes the form of a lattice where the individual points given the name 'pixels'. Pixels are displayed horizontally, row by row. In a color scheme, the number of bits is known as the bit depth and this basically refers to the number of bits assigned to each pixel [3]. Moreover, the smallest bit depth in the color

scheme is 8, i.e., 8 bits are utilized to represent the color of each pixel. Both Monochrome and gray scale images usually utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colors or shades of gray. One more point to add is that digital color images are known for being saved in 24-bit files and for utilizing the RGB color model. Almost all the color variations for the pixels of a 24-bit image are derived from three basic color terms: red, green, and blue, and each of these colors is represented by 8 bits [7]. Thus, in any given pixel, the number of different shades of red, green, and blue can reach 256 that adding up to more than 16 million combinations that finally result in more than 16 million colors. The most prominent image formats, exclusively on the internet, are the graphics interchange format (GIF), joint photographic experts group (JPEG) format, and to a lesser degree, the portable network graphics (PNG) format. The important issue to touch here is that most of the steganographic techniques attempt to exploit the structure of these formats. However, some literary contributions use the bitmap format (BMP) simply because of its simple and uncomplicated data structure [8, 9].

2.2 General Concepts

- Lossless compression is known for being preferable when the original data should stay in its entirety. In this manner, the original image information will never be removed, and this makes it possible the reconstruction of the original data from the compressed data. This is typical of images in GIF and BMP [7].

- Lossy compression saves storage space by discarding the points the human eyes find difficult to identify. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. JPEG compression uses this technique. A cover image is the image designated to carry the embedded bits or secret information [8].

- A stego image refers to the image carrying the hidden message.

- A stegokey is secret information necessary to get the hidden message from the stego image [9].

3. STEGANOGRAPHY HISTORY

Throughout history, people have hidden information in different ways. The word 'steganography' was basically derived from the Greek words with the meaning “covered writing”. Soon after, researchers used it for thousands of years in various manners [10]. During the 5th century BCE, the Greek tyrant Histiaeus was taken as a prisoner by King Darius in Susa. Histiaeus needed to send an abstruse message to his son-in-law, Aristagoras, who was in Miletus and in order to do this, Histiaeus shaved a slave’s head and tattooed the message on his scalp. As soon as the slave’s hair grew sufficiently to conceal the tattoo, he was sent to Miletus with the message [11].In ancient Greece, another method was to peal the wax off a wax-covered tablet, then write a message and to have the application of the wax again. The one in charge to receive the message would simply need to get rid of the wax from the tablet to see the message. Invisible ink was another popular form of steganography. Ancient Romans had their way in writing between the lines by using invisible ink, and by using substances such as fruit juice, urine, and milk. Using Invisible ink, though seems harmless, a letter might reflect a very different message written between the lines. Invisible ink was used as recently as World War II [12].

In addition to invisible ink, the Germans used the Microdot technique during the Second World War. Information, particularly photographs, was made so small that they were very difficult to detect [13].

In 1550, Jerome Cardan, an Italian mathematician, proposed a scheme of secret writing where a paper mask with holes is used. The user of such papers all what he needs is to write his secret message in such holes after placing the mask over a blank sheet of paper. The next step is to

remove the mask to fill in the blank parts of the page and in this way the message appears as innocuous text [14].

This technique, steganography, is now highly used in computers files with digital data as the carrier and networks are considered as high-speed dispatch channels. The sections that follow illustrate the taxonomy of steganographic techniques for image files, including an overview of the most important steganographic techniques for digital images.

4. TAXONOMY OF STEGANOGRAPHIC TECHNIQUES

There are quite a lot of approaches in classifying steganographic techniques. These approaches can be classified in accordance with the type of covers used with secret communications. Another possibility is done via sorting such approaches depending on the type of cover modification already applied in the process of embedding. The second approach is adopted in this work, although in some cases an exact classification is not possible. In general, the process of embedding can be defined as follows:

Let C denote the cover carrier, and $\tilde{C}$ the stego-image. Let K represent an optional key (as a seed used to encrypt the message or to generate a pseudo-random noise, which can be set to $\{\phi\}$ for simplicity), and let M be the message to be sent. Then, Em represents an embedded message and Ex represents the extracted message. Therefore,

$$Em : C \oplus K \oplus M \rightarrow \tilde{C} \quad (1)$$

$$\therefore Ex(Em(c,k,m)) \approx m, \forall c \in C, k \in K, m \in M \quad (2)$$

To distinguish between different steganographic techniques in a wide sense, one must take into consideration both the methods that modify the image and those that modify the image file format. However, the modifications to the file format are less robust [15]. The important issue to mention here is the main role compression usually plays when it comes to deciding which steganographic algorithm is better. Though lossy compression methods result in smaller image file sizes, they increase the possibility of the partial loss of an embedded message because surplus image data is to be eliminated in these techniques. Lossless compression does not compress the image file as much [16]. As a result, researchers have come up with different steganographic algorithms that suit such compression types. Steganographic techniques that modify image files for hiding information include the following:

- Spatial domain;
- Transform domain;
- Spread spectrum;
- Statistical methods; and
- Distortion techniques.

Steganographic techniques that modify the image file format involve file embedding and palette embedding. In addition, there are techniques that modify the elements in the visual image including:

The image generation technique; and the image element modification technique.
Finally, there is a special type of the spatial and transform domain techniques called the adaptive steganography technique, which we also describe for completeness. The next section explains each steganographic approach in more detail.

4.1 Spatial Domain Technique

Spatial domain steganographic techniques, also known as substitution techniques, are a group of relatively simple techniques that create a covert channel in the parts of the cover image in which

changes are likely to be a bit scant when compared to the human visual system (HVS).One of the ways to do so is to hide information in the least significant bit (LSB) of the image data [15].
This embedding method is basically based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any changes on the image [17].

The embedding operation of LSB steganography is described by the following equation:

$$Yi = 2\left|\frac{x_i}{2}\right| + m_i \quad (3)$$

where m_i, x_i, and y_i are the i-th message bit, and the i-th selected pixel value before and after embedding, respectively. Steghide, S-tools, Steganos, and other tools using LSB-based steganographic are available in [18].

Let $\{P_x(x=0), P_x(x=1)\}$ denote the distribution of the least significant bits of the cover image, and $\{P_m(m=0), P_m(m=1)\}$ denote the distribution of the secret binary message bits.

The message is to be compressed or encrypted before being embedded just to protect its secrecy. According to this, the distribution of the message may be assumed to equal an averaged distribution, such that $\{P_m(m=0) \approx P_m(m=1) \approx 1/2\}$.

In addition, the cover image and the message may also be assumed to be independent. Therefore, the noise introduced into the image may be modeled as:

$$P_{+1} = \frac{P}{2}P_x(x=0),\ P_0 = 1-\frac{P}{2},\ P_{-1} = \frac{P}{2}P_x(x=1) \quad (4)$$

Where P is the embedding rate, measured in bits per pixel (bpp). The embedding process described above, makes it clear to what extent it is possible to extract the secret message bits directly from the LSBs of these pixels already selected during this process [19].

When hiding the message bits in the image using LSB algorithms, there are two schemes, namely sequential and scattered. The LSBs of the image, in the sequential embedding scheme are replaced by the message bits, whereas in the case of the scattered embedding scheme, the message bits are randomly scattered throughout the image using a random sequence to control the embedding sequence [20].

The well-known steganographic tools based on LSB embedding are different as far as the way they hide information is concerned. Some of them change the LSB of pixels randomly, others modify pixels not in the whole image but in selected areas of it, and still others increase or decrease the pixel value of the LSB, rather than change the value [8].

Katzenbeisser and Petitcolas [21] describe several variations on the basic LSB techniques. They also describe a substitution technique for embedding a secret message into the LSB bits of the palette of GIF or BMP image format using steganography.

Bailey and Curran provide an evaluation of various techniques concerning spatial steganographic and such techniques can principally apply to GIF images [22]. From the above, we conclude that the resulting changes to the cover image using LSB techniques are very difficult to be recognized by the human eye due their being too small. Moreover, such techniques are simple and popular. The disadvantage of this technique is that it uses each pixel in the image. As a result, if lossy compression is used, some of the hidden information might be lost [23].

4.2 Transform Domain Techniques

Transform domain embedding can be defined as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. It is worth saying that most of the strong steganographic systems today operate within the transform domain [21].

Transform domain techniques have an advantage over LSB techniques because they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions [15]. The JPEG file format is the most common image file format on the internet owing to the small size of resultant images obtained by using it.

4.2.1 JPEG compression

If an image is to compress into JPEG format, the RGB color space is first turned into a YUV representation. Through this representation, the Y component represents brightness (or luminance) and the U and V components stand for color (or chrominance). It is known that the human eye is more sensitive to changes in the brightness of a pixel than to changes in its color [24]. Down sampling the color information is taken as an advantage of the JPEG to reduce the size of the file Where the color components (U and V) are splitted in the horizontal and vertical directions and consequently reducing the file size by a factor of 2 [37].

Then, the image is transformed. For JPEG images, the discrete cosine transform (DCT) is used; the pixels can be converted with such mathematical processing by simply “spreading” the position of the pixel values over the image or part of it [17]. With DCT transformation, a signal is transformed from the representation of an image into the frequency domain, this is done by sorting the pixels into (8 × 8) pixel blocks and transforming these blocks into 64-DCT coefficients which are affected by any modification of a single DCT coefficient.

The quantization phase of the compression is counted as the next step. Besides it is considered as biological property where the human eye is imposed. Basically, the human eye is known for being capable of identifying small differences in brightness over a relatively large area. The same does not apply when considering the distinction between different strengths in high-frequency brightness [3]. Consequently, the strength of higher frequencies can be reduced without any change in the image appearance. The JPEG format is done by dividing all the values in a block via a quantization coefficient, so the results are made approximate to integer values. The last point is to encode the coefficients by using Huffman coding just to reduce the size.

4.2.2 JPEG Steganography

Previously, it was believed that steganography could not be used with JPEG images owing to the lossy compression, which results in parts of the image data being altered. JPEG images are the products of digital cameras, scanners, and other photographic image capture devices. This is simply why concealing secret information in JPEG images might provide a better disguise. Data in most of the steganographic systems seems to be embedded into the non-zero discrete cosine transform (DCT) coefficients of JPEG images. The major JPEG steganographic methods can be described as follows:

- JSteg/JPHide. Jsteg and JPHide are two classic JPEG steganographic tools that employ the LSB embedding technique [21]. JSteg functions to hide the secret data in a cover image by simply exchanging the LSBs of non-zero quantized DCT coefficients with secret message bits. The quantized DCT coefficients, already used to conceal secret message bits in JPHide, are selected randomly by a pseudo-random number generator. JPHide, on the other hand, tends not only to modify the LSBs of the selected coefficients, but it

can also switch to a process where bits of the second least-significant bit-plane are likely to be worked out [8].

- F5. The F5 steganographic algorithm was introduced by Westfeld [25]. Rather than replacing the LSBs of quantized DCT coefficients with the message bits, the absolute value of the coefficient is reduced by the F5 algorithm by one if it needs modification. Due to the author's argument, the use the chi-square attack can never detect this type of embedding [26]. In addition to embedding message bits into randomly chosen DCT coefficients, the F5 algorithm employs matrix embedding that reduces the number of changes necessary for hiding a message of a certain length. Both, the message length and the number of non-zero coefficients are required in the embedding process to determine the matrix embedding needed to decrease the number of modifications required in the cover image [18].

- OutGuess. OutGuess is provided by Provos as a UNIX source code for which there are two widely known released versions [27]. The first one is the OutGuess-0.13b, which is exposed to statistical analysis, and the second is OutGuess-0.2, which includes the ability to safeguard statistical properties. Hereafter, OutGuess refers to OutGuess-0.2. There are two stages representing the embedding process of OutGuess. The first of which is that OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0s and 1s.Soon after modifications are made to the coefficients already left during embedding to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be subjected to a chi-square attack [18, 26].

- MB. Model-based steganography (MB) can be defined as a general framework for conducting both steganography and steganalysis by simply using a statistical model of the cover media [28]. The MB method for JPEG images is capable of having high message capacity while remaining secure against many first-order statistical attacks [18].

- YASS. Yet another steganographic scheme (YASS) belongs to JPEG steganography, but does not conceal data in JPEG DCT coefficients directly [29]. Instead, an input image in the spatial domain is divided into blocks with a fixed large size, called big blocks (or B-blocks). A later stage is to randomly select within each B-block, an 8 × 8 sub-block known as embedding host block (or H-block). Then via using error correction codes, secret data is encoded and embedded in the DCT coefficients of the H-blocks. Finally, the entire image is compressed and distributed as a JPEG image after inversing DCT on the H-blocks [18].

4.2.3 Wavelet transform technique

Wavelets transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis. The discrete wavelet transform (DWT) method is favored over the discrete cosine transform (DCT) method, owing to the resolution that the WT provides to the image at various levels [30].

Wavelets are mathematical functions that divide data into frequency components, which makes them ideal for image compression. In contrast with the JPEG format, they are far better at approximating data with sharp discontinuities [15].

In [31, 32], a group of writers discuss a steganography technique, based on wavelet compression techniques, that attaches attribute information to images in order to reduce the amount of information stored in a database of images. They use the homogenous connected region interested ordered transmission (HCRIOT) wavelet algorithm for image encoding and compression. This technique embeds secret information in the edge and detail regions of the

image where the human eye is less sensitive to the noise generated by the technique. In general, the human eye is more sensitive to noise in the smooth regions of an image.

In the project described in [33], researchers use vector quantization, called Linde-Buzo-Gray (LBG), associated with block codes, known as BCH codes, and one-stage discrete Haar wavelet transforms. They emphasize that modifying data by using a wavelet transformation produces good quality with few perceptual artifacts.

A group of scientists at Iowa State University are developing an advanced application called artificial neural network technology for steganography (ANNTS), with the aim of detecting all current steganography methods, which include DCT, DWT, and DFT. They found that the inverse discrete Fourier transform (IDFT) includes a rounding error that makes DFT inappropriate for steganography applications [34].

The research discussed in [35] proposes, a data hiding technique in the DWT domain. DWT with the first level is used to decompose both secret and cover images, where each is broken into disjoint (4 × 4) blocks. Then a comparison is made between the blocks of the secret image and the cover blocks to determine the best match. Later, error blocks are produced and embedded into the coefficients of the best matched blocks in the HL part of the cover image.

In [30], the authors proposed high capacity and high security steganography using the discrete wavelet transform (HCSSD). The wavelet coefficients of both the cover and the payload are merged into a single image using embedding strength parameters alpha and beta. The cover and payload are preprocessed to minimize the pixel range to ensure accurate recovery of the payload at the receiving end. The capacity of the proposed algorithm is increased as only the approximation band of the payload is considered. The entropy, mean square error (MSE) and capacity are improved with an acceptable peak signal to noise ratio (PSNR).

4.3 Spread Spectrum Technique

Spread spectrum transmission in radio communications transmits messages below the noise level for any given frequency. When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image.

- Cover image as noise
  A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit. To permit the transmission of more than one bit, the cover image has to be broken into sub images [15].

  When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum steganography. When the sub cover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum steganography. These techniques require searching the image for the carrier in order to then retrieve the data. These techniques are robust against gentle JPEG compression and can be made more robust through the pre-distortion of the carrier. In this case, after the carrier is created, and before the message is added, the carrier is compressed using JPEG compression and decompression such that it will be unaffected by later JPEG compression of the cover image [36]. The capacity can be traded directly for robustness, and it depends greatly on the image.

- Pseudo-noise
  This technique shows that the hidden data is spread throughout the cover image and that is why it becomes difficult to detect [37]. Spread spectrum image steganography (SSIS) described by Marvel et al., combined spread spectrum communication, error control

coding, and image processing to hide information in images, is an example of this technique [38]. The general additive embedding scheme can be described as follows:

$$Y_i = X_i + \gamma W_i \quad \text{for } i = 1, 2, ..., N \tag{5}$$

Where X_i is a sequence of the original data from the cover,

W_i is a pseudo-random sequence generated from a pseudo-random number generator (PRNG) initialized by a secret stego key,

γ is an embedding strength parameter (gain factor), and Y_i is a sequence of possibly altered data.

In SSIS, the process goes like this: the message is hidden in noise and then it is combined with the cover image to reach into a stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image becomes imperceptible not only to the human eye but also through computer analysis without access to the original image.

The last few years witnessed the development of several steganography techniques one of which is spread spectrum steganography. In 1996, Smith and Comiskey described three schemes, namely direct sequence, frequency hopping, and chirp [36]. In image steganography, it is noticed that high frequencies usually aid the invisibility of the hidden information, but at the same time, they are not efficient as far as robustness is concerned. In contrast, low frequencies are better with respect to robustness, but are far too visible to be useful. Such conflicting points are reconciled by the spread spectrum technique via allowing the embedding of a low-energy signal in each one of the frequency bands, and as illustrated in [21].

Instead of using direct sequences, two new processing methods are proposed and shown in [39].Such methods include block spread spectrum and duplicate spreading. Spread spectrum techniques are capable of being combined with transform embedding by using transformation techniques in order to get the payload capacity increased. In [40][5], the authors introduce a technique based on discrete Fourier transform (DFT) that can significantly increase the number of transform coefficients that can transmit hidden information. A blind image steganography, based on a hybrid direct sequence/frequency hopping (DS/FH) technique, is described in [41], in which the system retrieves the hidden message without needing the original image. The authors in [42] found that using a signature vector, when embedding a spread spectrum (SS) message, maximizes the signal-to-interference-plus-noise ratio (SINR) at the output of the corresponding maximum-SINR linear filter.

The research in [43] describes the benefits of combining the spread spectrum technique with the advantages of error correction coding and DFT simply to the robustness of the system increased.

Finally, an analysis is presented in [44] proposes using a code division multiple access (CDMA) spread spectrum for both the spatial domain and the transform domain for image steganography in MMS. Their experimental results reveal that the spread spectrum detection method is highly robust for normal signal manipulation.

4.4 Statistical Methods

Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This

modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation [17].

Statistical steganographic techniques exploit the existence of a "1-bit", where nearly a bit of data is embedded in a digital carrier. This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if a "1" is transmitted, otherwise it is left unchanged [45]. To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message [15].

Another technique, called data masking, has been proposed in [46]. According to this technique, the message signal is processed such that it views the properties of an arbitrary cover signal.
In work [28], the authors propose a method where the transformed image coefficients are broken down into two parts to allow the coded message signal to replace the perceptually insignificant component. Hence, the statistics of the quantized (non-zero) AC DCT coefficients are modified taking into consideration the parametric density function. This process requires a low precision histogram of each frequency channel in addition to matching the model with each histogram by deciding the corresponding model parameters.

However, statistical steganographic methods in their simplest form, for which sub-images are simply sub-rectangles of the original image, are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. To counter these attacks, the sub-images could be selected based on picture elements, for example, the faces in a crowd, and error correction coding could be utilized within the message. These defenses can make the statistical steganographic method approximately as robust as the underlying watermarking scheme [15].

4.5 Distortion Techniques

Distortion techniques require knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder, on the other hand, adds a sequence of changes to the cover image [46]. So, information is described as being stored by signal distortion [30].

Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is selected to match the secret message required to transmit [45].

The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, then the message bit is a "1." Otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such manner that the statistical properties of the image are not affected (which is different from many LSB methods). However, the need for sending the cover image limits the benefits of this technique. As in any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, rotating, or scaling, the receiver can easily detect the modification. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be fully recovered [15].

An early approach to hiding information was to do so in text. Most text-based hiding techniques are of the distortion type. For example, the layout of a document or the arrangement of words might show or reflect the presence of information. Considering one of these techniques, can show the adjustment of the positions of lines and words where spaces and "invisible" characters are added to the text, providing a method of sending hidden information [45].

4.6 File Embedding

Different image file formats are known for having different header file structures. In addition to the data values, such as pixels, palette, and DCT coefficients, secret information can also be hidden

in either a header structure or at the end of the file [47]. For example, the comment fields in the header of JPEG images usually contain data hidden by the invisible Secrets and Steganozorus. Camouflage, JpegX, PGE10, and PGE20 add data to the end of a JPEG image.

Image storage formats such as TIFF, GIF, PNG, and WMF have a file header that can be exploited to hide arbitrary information. In this case, that arbitrary data may be a secret message. It is possible to append data to many image storage formats without affecting the image. When the image is processed for display, the image user will decode the image size from the file header, and any tracking information attached to the end of the file will be ignored. Using this technique, it is possible to attach a message of any size to a cover image. However, the message could be removed from the cover image by simply resaving the image in the same file format [15]. The limitations of this method are that despite the large payload, it is not that difficult to identify and defeat, it is weak when lossy compression and image filtering are concerned, and the resaving of the image implies complete loss of hidden data [48].

4.7 Pallet Embedding

In a palette-based image, what matters is the fact that only a subset of colors from a particular color space is used to colorize the image. Researchers believe that every palette-based image format consists of two parts. The first part is a palette that assigns N colors as a list of indexed pairs (i, c_i), assigning a color vector c_i to every index i, and the actual image data, which specifies a palette index for each pixel, rather than the color value itself. The file size gets decreased via this approach when only a limited number of color values are used in the image. Two of the most popular formats are the graphics interchange format (GIF) and the bitmap format (BMP). However, owing to the availability of advanced compression techniques, their use has diminished [21].

In some cases, the palette itself can be used to hide secret information. Because the order of the colors in the palette usually does not matter, the ordering of colors can be used to transfer information. In essence, a hidden message can be embedded using the difference between two colors in the palette (i.e., one secret message bit for every two colors in the palette). Color palettes are used to minimize the amount of information images that are used to represent colors [15].

Since steganographic message within the bits of the palette and/or the indices is embedded in the palette-based steganography, one must be careful not to exceed the maximum number of colors [49, 50].

4.8 Image Generation Technique

Many techniques have been proposed that encrypt messages so that they are unreadable or as secret as possible. Big Play Maker hides information by converting the secret text message into a larger and a slightly manipulated text format. The same principle can be employed in image creation, in which a message is converted to picture elements and then collected into a complete stego-image. This method cannot be broken by rotating or scaling the image, or by lossy compression. Parts of the message may be destroyed or lost because of cropping, but it is still possible to recover other parts of the message by encoding the message with error correcting information.

Generally, this technique uses pseudo-random images, because if a malicious third party detects a group of images passing through a network without any reason for them being there (i.e., random images), he or she may suspect that the images contain secret information and block their transmission [15].

4.9 Image Element Modification Techniques

Some steganographic techniques do not try to hide information using the actual elements of the image. Instead, they adjust the image elements in completely undetectable ways, for example, by modifying the eye color or hair color of some person in a photograph. These modifications can

then be used to carry the hidden information. In addition, this information will survive rotations, scaling, and lossy compression.
The feasibility of modifying objects within images as a tactic for hiding information has been discussed by [51]. It is important to keep in mind that when this method is used, the same cover image must not be used more than once, because the elements used will become apparent. This technique can be achieved manually with any photo editing software. With the advent of computer vision systems that identify objects within pictures, these methods have become more viable.

4.10 Adaptive Steganography

Adaptive steganography is a special case of the spatial and transform techniques. Moreover, it is introduced as statistics-aware embedding and masking. Global statistical characteristics of the image are basically used before any attempt to deal with its frequency transformed coefficients. These statistics decide what changes can be made. A random adaptive selection of pixels actually characterizes this method, relying on the cover image and the selection of pixels in a block with a large standard deviation (STD). The latter is intended to avoid areas of uniform color, such as smooth areas. This technique is known for exploiting images with existing or deliberately added noise and with images that show color complexity [52, 53, 54, 55].

An adaptive technique applied to the LSB substitution method has been proposed in [56]. The idea behind this method is to make use of the correlation between neighboring pixels so as to calculate the degree of smoothness. The researchers shed light on the options of having two-, three-, and four-sided matches. The payload (embedding capacity) they were able to obtain was high.

A technique called the “adaptive more surrounding pixels using” (A-MSPU) technique, which improves the imperceptibility problems of multiple base notational systems (MBNS), has been discussed in [57]. This technique pays attention to the edge areas of a cover image while re-expressing the secret bits in multiple base notational systems. The suggested approach uses the same probability parameter to get the secret bits scattered and it also uses surrounding pixels with the maximum number to determine the capacity of every target pixel. Most steganographic techniques use either three or four adjacent pixels of a target pixel. The proposed technique is able to utilize all eight adjacent neighbors, which improves the imperceptibility value.

5. PERFORMANCE MEASURE

As a performance measure for image distortion due to embedding, the well-known peak-signal-to-noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images [55]. It is defined as:

$$PSNR = 10\log(\frac{C_{\max}^{2}}{MSE}) \tag{6}$$

where MSE denotes the mean square error, which is given as

$$MSE = \frac{I}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \tag{7}$$

Here, $C_{\max}$ indicates the maximum value in the image, for example:

$$C_{\max} \leq \begin{cases} 1 & in\, double\ precision\, images \\ 255 & in\, 8-bit\, unsigned\ \text{int}\, eger\, images \end{cases}$$

In addition, x and y are the image coordinates, M and N are the dimensions of the image, S_{xy} is the resultant stego image, and C_{xy} is the cover image. In [58, 59], C_{xy} is set to 255, as an agreed default value for 8-bit images. It can be that an image has only up to 253, or fewer, gray colors. Having $C_{\max}$ is raised to the power of 2 results in a strong change to the PSNR value. For this reason, $C_{\max}$ is considered as the actual maximum value rather than the largest possible value [48]. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values below 30 dB indicate low quality (i.e., distortion caused by embedding is clear). A high-quality stego image should strive for a PSNR of 40 dB, or higher.

6. EVALUATION OF DIFFERENT TECHNIQUES

All the above mentioned algorithms with respect to image steganography are not void of weak and strong points. Consequently, it is important to decide the most suitable approach to be applied. As defined before, there are several parameters to measure the performance of the steganographic system. Fridrich in Fig. 2 shows the relationship between three parameters [60]. These parameters are as follows:

- Undetectability (imperceptibility): this parameter is the first and the primary requirement; it represents the ability to avoid detection, i.e., where the human eye fail to notice it. However, the techniques that do not alter the image in such a way to be perceptible to the human eye may still alter the image in a way that it is detectable by the statistical tests. Truly secure steganographic techniques should be undetectable neither by the human eye nor by the statistical attacks.
- Robustness: it is the second parameter that measures the ability of the steganographic technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation (like cropping or rotating), data compression, and image filtering. Watermarks are an example of a robust steganographic technique (out of the scope of this paper).
- Payload capacity: it is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully. When compared with watermarking, that requires embedding only a small amount of copyright information, steganography is seen to hide communication and consequently a sufficient embedding capacity is required. Accordingly and by using this parameter, small amounts of data could be hidden without being detected by the human eye. Larger amounts of information, on the other hand, may detect artifacts by the HVS or statistical tests.

The following paragraphs compare the previously mentioned steganographic techniques in terms of the competing parameters.

- LSB technique in the spatial domain is a practical way to conceal information but, at the same time, it is vulnerable to small changes resulting from image processing or lossy compression [7]. Although LSB techniques can hide large quantities of information i.e., high payload capacity, they often compensate the statistical properties of the image and thus indicate a low robustness against statistical attacks as well as image manipulation.

- The promising techniques such as DCT, DWT and the adaptive steganography are not tended to attacks, especially when the hidden message is small. This can be justified in

relation to the way they change the coefficients in the transform domain, thus, image distortion is kept to a minimum. Generally speaking, such techniques tend to have a lower payload when they are compared to the spatial domain algorithms [8]. The experiments on the discrete cosine transform (DCT) coefficients have introduced some promising results and then they have diverted the researchers' attention towards JPEG images. Working at some level like that of DCT turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding, especially in terms of compression survival [8].

- Spread spectrum techniques are generally quite robust against statistical attacks, since the hidden message is spread throughout the image. However, a determined attacker is capable of compromising the embedded data using some digital processing, such as noise reduction filters, which are similar to the ones used in the decoding process to estimate the original cover. Spread spectrum encoding is extensively used in military communications due to its robustness against detection. When a message is embedded, an attacker cannot be easily recognized and it will be difficult to extract it without knowing the suitable keys. SISS is very good for steganography because of the reasonable high capacity and high difficulty proposed in the process of detection and extraction [9].

- The statistical techniques in most cases are vulnerable to cropping, rotating, and scaling attacks, along with any attacks that work against the watermarking technique. Defenses could be considered to make the statistical techniques as robust as the watermarking scheme. The payload capacity and invisibility depends on the cover image selected.

- Unlike many LSB methods, distortion techniques do not upset any statistical properties of the image. In contrast, the need to send the cover image over a secure channel limits the worth of this technique. As in any steganographic technique, the cover image should never be used more than one time. If an attacker alters the stego-image by cropping, rotating, or scaling, the alteration can easily be perceived by the receiver and can fairly be reversed to the point where the message encoded with error correcting information can be fully recovered. Error correcting information also aids if the stego-image is filtered through a lossy compression scheme such as JPEG. Adopting this technique limits the hidden information capacity, since adding distortion to the cover image is the basis of embedding algorithm. As a result, the distorted image will be more vulnerable to the HVS.

- Techniques that modify image file formatting information have the following drawbacks: they have a large payload; however, they are easily detected and defeated; they are not robust against lossy compression and image filters, and the issue of saving the image one more time totally breaks the hidden data [48].

- Hiding information via steganographic techniques that modify the elements in the visual image results in a stegoimage that will survive rotation, scaling and much lossy compression like JPEG. A reasonable payload capacity can be achieved with this technique as well. Table 1 summarizes the evaluation of the mentioned techniques through this paper.

	LSB	Transform Domain	Spread Spectrum	Statistical Techniques	Distortion Techniques	File and Pallet Embedding
Imperceptibility	High*	High	High	Medium*	Low	High*
Robustness	Low	High	Medium	Low	Low	Low
Payload Capacity	High	Low	High	Low*	Low	High

TABLE 1: A comparison of Image Steganography Techniques

*: Indicates dependency on the used cover image

7. CONCLUSION

This paper reviewed the main steganographic techniques for both lossy and lossless image formats, such as JPEG and BMP. The consequences are presented in terms of a taxonomy that focuses on three principal steganographic techniques for hiding information in image files. Those techniques include those modifying the image in the spatial domain, in the transform domain, and those modifying the image file formatting. Each of these techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or undetectability, capacity, and robustness). From TABLE 1, one can deduce that while one technique may lack in payload capacity, another may lack in robustness. For example, file formatting techniques can store large amounts of information, but they are easily detected and attacked. Likewise, LSB techniques in a spatial domain have a high payload capacity, but they often fail to prevent statistical attacks and are thus easily detected. It is important to notice that the hiding capacity in LSB technique depends on the cover image being used. LSB in BMP images is capable of hiding relatively a large message, but large amount of altered bits results in a larger possibility of detection by human eye. While LSB in GIF images is approximately the same as that of using LSB in BMP images. The only difference is related to the structure of the GIF images, since they only have a bit depth of 8. Thus, the amount of hidden information is less than with BMP. In addition, LSB in GIF is mainly dependent on the file format and the image itself. Incorrect choice of cover image could result in visible message.

Besides, file and spatial domain approaches are considered not to be robust against lossy compression and filtering. Transform domain techniques are considered more robust for lossy compression image formats, but this advantage is achieved at the expense of payload capacity. However, it is possible to defeat the transform domain techniques, but with some efforts.
For most of steganography applications, JPEG file format can be used, especially for images that have to be communicated over an open systems environment like the Internet

Thus, for an agent to send secret information using steganographic techniques, he or she must select a suitable steganographic algorithm and suitable cover image as well. The required application is the only thing to decide the most appropriate steganographic method among all the present image steganographic techniques.

In short, one must have the determination to compromise on some characteristics to ensure the high performance of other characteristics.

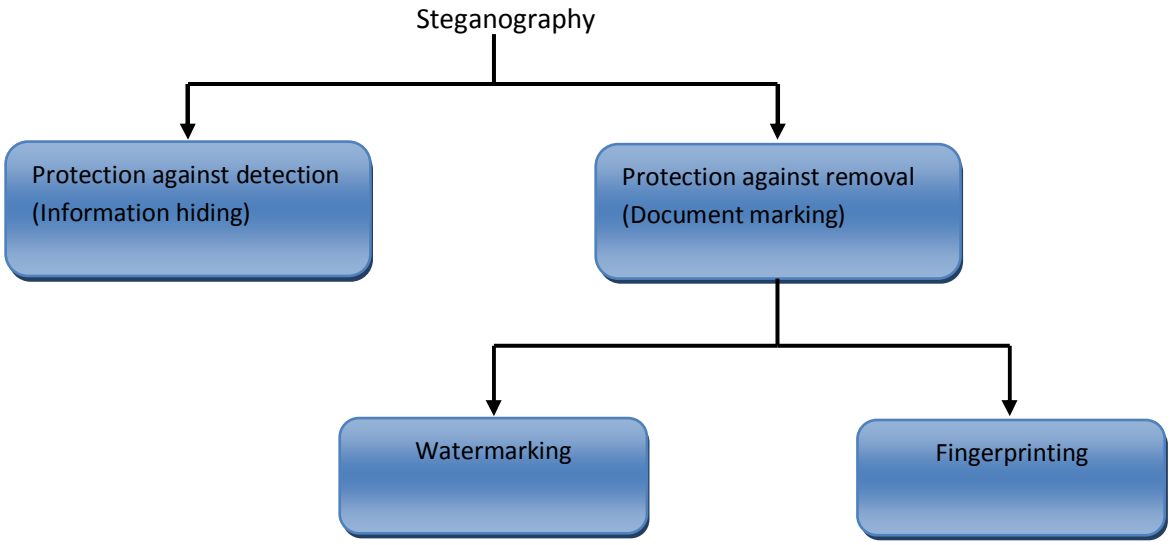

FIGURE 1: Steganography Types

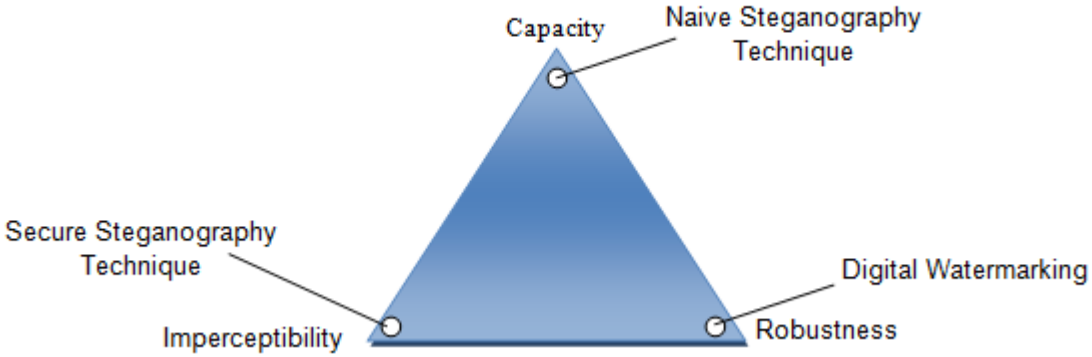

FIGURE 2: Competing factors in steganographic systems [60]

8. REFERENCES

[1] S.A. Halim and M.F.A Sani. "Embedding using spread spectrum image steganography with GF (2^m)," in Proc. IMT-GT-ICMSA, 2010, pp. 659-666.

[2] N.N. El-Emam. (2007). "Hiding a large amount of data with high security using steganography algorithm." Computer Science. [On-line]. 3(4), pp. 223-232. Available: www.thescipub.com/pdf/10.3844/jcssp.2007.223.232 [Dec., 2011].

[3] T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc. ISSA, 2005, pp. 1-11.

[4] L. Chun-Shien. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. USA: Idea Group Publishing, 2005, pp. 1-253.

[5] R.J. Anderson and F.A.P. Petitcolas. (1998, May). "On the limits of steganography." IEEE Journal of Selected Area in Communications. [On line]. 16(4), pp. 474-481. Available: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf [Jun., 2011].

[6] I.J. Cox, M.L. Bloom, J.A. Fridrich, and T. Kalkert. Digital watermarking and steganography. USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

[7] N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the unseen." IEEE Computer Journal. [On line]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[8] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal. [On line]. 90(3), pp. 727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2011].

[9] M. Fortrini. "Steganography and digital watermarking: A global view." University of California, Davis. Available: http://lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf . [June 2011].

[10] N. Provos and P. Honeyman. (2003, Jun.). "Hide and seek: An introduction to steganography." IEEE Security and Privacy Journal. [On line], 1(3), pp. 32-44. Available: http://niels.xtdnet.nl/papers/practical.pdf [Jul., 2011].

[11] N.F. Johnson. (1995, Nov.). "Steganography. Technical report." Available: http://www.jjtc.com/pub/tr_95_11_nfj/ [Sep., 2011].

[12] D. Sellars. "An introduction to steganography. Internet: http://www.cs.uct.ac.za/courses/CS400W/papers99/stego.html [Jul., 2011].

[13] T. Jamil. (1999, Feb.). "Steganography: The art of hiding information in plain sight." IEEE Potentials. [On line], 18(1), pp. 10-12. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=747237 [Sep., 2011].

[14] S.B. Sadkhan. "Cryptography: Current status and future trends." in Proc. IEEE Conference on Information & Communication Technologies, 2004, pp. 417-418.

[15] P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. [On line], 5(1), pp. 41-52. Available: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47 [Oct., 2011].

[16] M.S. Prasad, S. Naganjaneyulu, CH.G. Krishna, and C. Nagaraju. (2009, Oct.). "A novel information hiding technique for security by using image steganography." Journal of Theoretical and Applied Informaion Technology. [On line]. 8(1), pp. 35-39. Available: www.jatit.org/volumes/research-papers/Vol8No1/6Vol8No1.pdf [Apr. 2011].

[17] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr.). "Image steganography: Concepts and practice." WSPC/Lecture Notes Series: 9in x 6in, [On line], pp. 1-49. Available: http://iwearshorts.com/Mike/uploads/2011/06/10.1.1.62.8194.pdf [Aug. 2011].

[18] B. Li, J. He, J. Huang, and Y.Q. Shi. (2011, Apr.). "A survey on image steganography and steganalysis." Journal of Information Hiding and Multimedia Signal Processing. 2(2), [On line], pp. 142-172. Available: http://bit.kuas.edu.tw/~jihmsp/2011/vol2/JIH-MSP-2011-03-005.pdf [Dec., 2011].

[19] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. (1996). "Techniques for data hiding." IBM System Journal. 35(3/4), [On line], pp. 313-336.
Available: http://www.almaden.ibm.com/cs/people/dgruhl/313.pdf [Nov., 2011].

[20] M. Juneja and P.S. Sandhu. "Designing of robust image steganography technique based on LSB insertion and encryption." IEEE International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp. 302-305.

[21] N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[22] K. Curran and K. Baily. (2006, Jul.). "An evaluation of image based steganography methods." Multimedia Tools and Applications Journal. [On line]. 30(1), pp. 55-88.
Available: http://dl.acm.org/citation.cfm?id=1164470 [May, 2011].

[23] A.R. Naghsh-Nilchi, L. Pourmohammadbagher. (2006, Jun.). "A new approach to steganography using sinc-convolution method." PWASET Journal. [On line]. 14(1), pp. 324-329. Available: http://www.waset.org/journals/waset/v20/v20-4.pdf [May, 2011].

[24] D.L. Currie and C.E. Irvine. "Surmounting the effects of lossy compression on steganography." in Proc. of the 19th National Information Systems Security Conference, 1996, pp. 194-201.

[25] A. Westfeld. "F5-A steganographic algorithm: high capacity despite better steganalysis." in Proc. of the 4th Information Hiding Workshop, LNCS, 2001, pp. 289-302.

[26] A. Westfeld and A. Pfittzmann. "Attacks on steganographic systems- breaking the steganographic utilities Ezstego, Jsteg, Steganos, and S-tools-and some lessons learned." in Proc. of the 3rd Internet Workshop on Information Hiding, 1999, pp. 61-76.

[27] N. Provos. "Defending against statistical steganalysis." in Proc. of the 10th USENIX Security Symposium, 2001, pp. 323-325.

[28] P. Sallee. "Model-based steganography." in Proc. the 2nd International Workshop on Digital Watermarking, LNCS, 2004. pp. 254-260.

[29] K. Solanki and B.S. Manjunath. "Yass: Yet another steganographic scheme that resists blind steganalysis." in Proc. of the 9th Information Hiding Workshop, LNCS, 2007. pp. 1-16.

[30] H.S. Majunatha Reddy and K.B. Raja. (2009). "High capacity and security steganography using discrete wavelet transform." International Journal of Computer Science and Security. [On line]. 3(6), pp. 462-472.
Available:
http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume3/Issue6/IJCSS-163.pdf [Jun., 2011].

[31] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao. "Exploring on steganography for low bit rate Wavelet based coder in image retrieval system." in Proc. of IEEE TENCON, 2000. pp. 250-255.

[32] S. Areepongsa, N. Kaewkammerd, Y.F. Syed, and K.R. Rao. "Steganography for low bit-rate Wavelet based image coder." in Proc. of IEEE ICIP, 2000. pp. 597-600.

[33] N.K. Abdulaziz and K.K. Pang. "Robust data hiding for images." in Proc. of IEEE International Conference on Communication Technology, 2000. pp. 380-383.

[34] L.D. Paulson. (2006, Aug.). "New system fights steganography. News briefs." IEEE Computer Society. [On line]. 39(8), pp. 25-27.
Available:
http://journals2.scholarsportal.info/details.xqy?uri=/00189162/v39i0008/25_nsfs.xml [Jul., 2011].

[35] A.A. Abdelwahab and L.A. Hasan. "A discrete Wavelet Transform based technique for image data hiding." in Proc. of 25th National Radio Science Conference, 2008. pp. 1-9.

[36] J.R. Smith and B.O. Comiskey. "Modulation and information hiding in images." in Proc. of the 1st Information Hiding Workshop, 1996. pp. 207-226.

[37] H. Wang and S. Wang. (2004, Oct.). "Cyber Warfare: steganography vs. steganalysis." Communications of the ACM. [On line]. 47(10), pp. 76-82.
Available: www.csc.liv.ac.uk/~leszek/COMP526/week4/comp526-3.pdf [Mar., 2011].

[38] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter. (1999). "Spread spectrum image steganography." IEEE Trans. image processing. [On line]. 8(8), pp. 1075-1083.
Available: http://www.mendeley.com/research/spread-spectrum-image-steganography-1/ [Apr., 2011].

[39] C.L. Tsai, K.C. Fan, and C.D. Chung. "Secure information by using digital data embedding and spread spectrum techniques." IEEE 35th International Carnahan Conference on Security Technology, 2001. pp. 156-162.

[40] F. Alturki and R. Merserau. "Secure blind image steganographic technique using Discrete Fourier Transform." in Proc. IEEE International Conference on Image Processing, 2001. pp. 16-162.

[41] K.C. Widadi, P.H. C.C. Wah. "Blind steganography using direct sequence/frequency hopping spread spectrum technique. in : Information, Communications and Signal Processing, 5th International Conference, 2006. pp. 1125-1129.

[42] M. Gkizeli, D.A., and M.J. Medley. (2007, Feb.). "Optimal signature design for spread-spectrum steganography." IEEE Signal Processing Society. [On line]. 16(2), pp. 391-405. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4060938 [Oct. 2011].

[43] R.S. Youail, A.-K.A.-R. Khadhim, and V.W. Samawi. "Improved stegosystem using DFT with combined error correction and spread spectrum." in 2nd IEEE ICIEA, 2007. pp. 1832-1836.

[44] R.S. Singh, M.A. Khani, and N. Singh. (2010, Dec.). "Spread spectrum image steganography in multimedia messaging service of mobile phones." International Journal of Electronics Engineering. [On line]. 2(2), pp. 365 – 369.
Available: http://www.csjournals.com/IJEE/PDF%202-2/Article_29.pdf [Oct., 2011].

[45] S.C. Katzenbeisser. "Principles of Steganography." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.

[46] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. "Data masking: a secure-covert channel paradigm." in IEEE Workshop on Multimedia Signal Processing, 2002. pp. 339-342.

[47] Y.O. Yildiz, K. Panetta, and S. Agaian. (2007, Apr.). "New quantization matrices for jpeg steganography." International Society for Optical Engineering. [On line]. 6579(1), pp. 6579OD.
Available: link.aip.org/link/?PSISDG/6579/65790D/1 [Nov., 2011].

[48] A. Shaddad, J. Condell, K. Curran, and P. Mckevitt. "Enhancing steganography in digital images." IEEE Canadian Conference on Computer and Robot Vision, 2008. pp. 326-332.

[49] S.S. Agaian, B.M. Rodriguez, and J.P. Perez. "Palette-based steganography used for secure digital image archiving." IS&T Archiving Conference, 2005. pp. 159- 164.

[50] C.H. Tzeng, Z.F. Yang, and W.H. Tsai. (2004, May). "Adaptive data hiding in palette images by color ordering and mapping with security protection." IEEE Trans. on Communications. [On line]. 52(5), pp. 791-800.
Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1299069 [Dec., 2011].

[51] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb. (2000, Jul.). "Applications for data hiding." IBM Systems Journal. [On line]. 39(3&4), pp. 447- 568. Available:
http://www.almaden.ibm.com/cs/people/dgruhl/afdh.pdf [Dec., 2011].

[52] E. Franz and A. Schneidewind. "Adaptive steganography based on dithering." in Proc. of the 2004 workshop on Multimedia and Security, 2004. pp. 56-62.

[53] R. Bohm and A. Westfeld. "Breaking cauchy model-based JPEG steganography with first order statistics." In Proc. of ESORICS'2004, 2004. pp. 125-140.

[54] A.M. Fard, M. Akbarzadeh-R., and F. Varasteh-A. "A new genetic algorithm approach for secure JPEG steganography." in Proc. of IEEE International Conference on Engineering of Intelligent Systems ICEIS, 2006. pp. 216-219.

[55] A. Shaddad, J. Condell, K. Curran, and P. Mckevtt. "Biometric inspired digital image steganography." In Proc. of the 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008. Pp. 159-168.

[56] C.C. Chang, P. Tsai, and M.H. Lin. "An adaptive steganography for index- based images using code word grouping." Lecture Notes in Computer Science, 2004. pp. 731-738.

[57] M. Afrakhteh and S. Ibrahem. "Adaptive steganography scheme using more surrounding pixels." IEEE International Conference on Computer Design and Applications, 2010. pp. 225-229.

[58] Z.Z Kermani and M. Jamzad. "A robust steganography algorithm based on texture similarity using Gabor filter." in Proc. of IEEE 5th International Symposium on Signal Processing and Information Technology ISSPIT, 2005. pp. 578-582.

[59] A.I. Hashad, A.S. Madani and A.E.M.A. W ahdan. "A robust steganography technique using Discrete Cosine Transform insertion." In Proc. of IEEE/ITI 3rd International Conference on Information and Communications Technology, 2005. pp. 255-264.

[60] J. Fridrich. "Applications of data hiding in digital images." Tutorial for the ISPACS'98 Conference, 1998.