A Survey on Image Steganography Techniques

Kamred Udham Singh
Department of Computer Science, Faculty of Science
Banaras Hindu University,
Varanasi, (U.P.), India

ABSTRACT
Steganography is an important technique for information hiding in any digital object. Steganography technique is the science that includes communicating secret information in an appropriate digital multimedia cover objects such as audio, video and image files. The main objective of steganography is to hide the existence of the embedded data. Steganography technique has improved the security of existing data hiding techniques by the outstanding development in computational power. Objectives of steganography are Undetectability, robustness and capacity of the concealed data, these key factors that separate it from related techniques like cryptography and watermarking. This paper delivers a survey on digital images steganography and covering its fundamental concepts. The development of image steganographic methods in spatial representation, in JPEG format and also discuss the recent development in the field of image steganography. Specific generally used approaches for increasing steganographic security are summarized and significant research developments are also discussed.

General Terms
Robust, Security, Information, Stego, Cover Image

Keywords
Digital image, steganography, spatial domain, frequency domain, security, information hiding.

1. INTRODUCTION
The word steganography is derived from the Greek words which mean "Covered Writing". It has been used in different forms for thousands of years. In the 5thcentury BC Histaiacus shaved a slave's head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [3] [4].Steganography is the art of data hiding into cover object like image, text, audio and video.

The data hiding process in a steganography with various methods includes identifying a cover medium's redundant bits. The data embedding process generates a stego file by substituting the redundant bits with data from the hidden information. During the hiding process of the data three major factor must be considered that are capacity it includes amount of data that can be hidden in the cover object. Security refers to detect hidden data and robustness to the amount of alteration the stego object can withstand before an adversary can destroy hidden data[1].Main objective of steganography is to communicate securely with third party in such a way that the hidden data is not visible to the observer. Using steganography technique a secret information is embedded inside a unsuspicious object and sent it without anyone knowing the existence of the secret information. Maximum steganographic utilities hiding data inside an image, as it is relatively simple to implement images are frequently used in the process of steganography because it is hard to break[2]. A thorough history of steganography can be found in the literature [3] [4]. There are three techniques which are interlinked, steganography, watermarking and cryptography. First two techniques are quite difficult to tease apart especially for those coming from different disciplines. Figure 1 and Table1 may eradicate such confusion. The work presented here revolves around steganography in digital images and does not discuss other types of steganography. This paper describes different technique used in image steganography, performance, analysis & comparisons on each techniques.

2. CHARACTERIZING DATA HIDING TECHNIQUES
Steganographic techniques hide the data inside a cover object like image, audio, video or text; various features characterize the advantages and disadvantages of the techniques. Relative importance of each component depends on the application [5].

2.1 Security
Steganography technique may suffer from various active or passive attacks. If the existence of the secret information can only be estimated with the probability not higher than the random guessing in the existence of some steganalytic systems and steganography may be considered more secure under such steganalytic systems. On the other hand we can say that steganography is insecure data hiding technique.

2.1 Data Hiding Capacity
Data hiding capacity is the size of data that can be concealed relative to the size of the cover object. A larger data hiding capacity permits the use of a smaller cover image for a data of fixed size and thus decreases the bandwidth necessitated to transmit the stego-image object. Therefore, the usual practice for embedding is to make the message as short as possible so that the image is altered as little as possible.

2.2 Perceptual Transparency
Message hiding the in the cover requires some noise distortion of the cover image. It is very important that the hiding occur without loss of perceptual quality of the cover object. After concealing secret information in image should not be altered such that it is visually obvious that information has been hidden. In fact, the resulting stego-image should be so similar to the original that if you compare both side by side, you should not be able to differentiate both and the integrity of the original image must be maintained [7].In a secret

communications application, if an attacker observes some distortion that provoke suspicion of the presence of concealed data in a stego-image, the steganographic encoding technique has failed even if the attacker is unable to extract the message. For applications where the perceptual transparency of hidden data is not critical, permitting more distortion in the stego-image object can increase robustness, hiding capacity or both.

2.4 Robustness

Robustness of steganography is one of main goals to be achieved. Robustness refers to the degree of difficulty required by a steganalyst to determine whether or not the image contains a hidden data or not. Robustness is very critical in copyright protection because pirates will attempt to destroy and filter any watermarks embedded with images [6] [7].

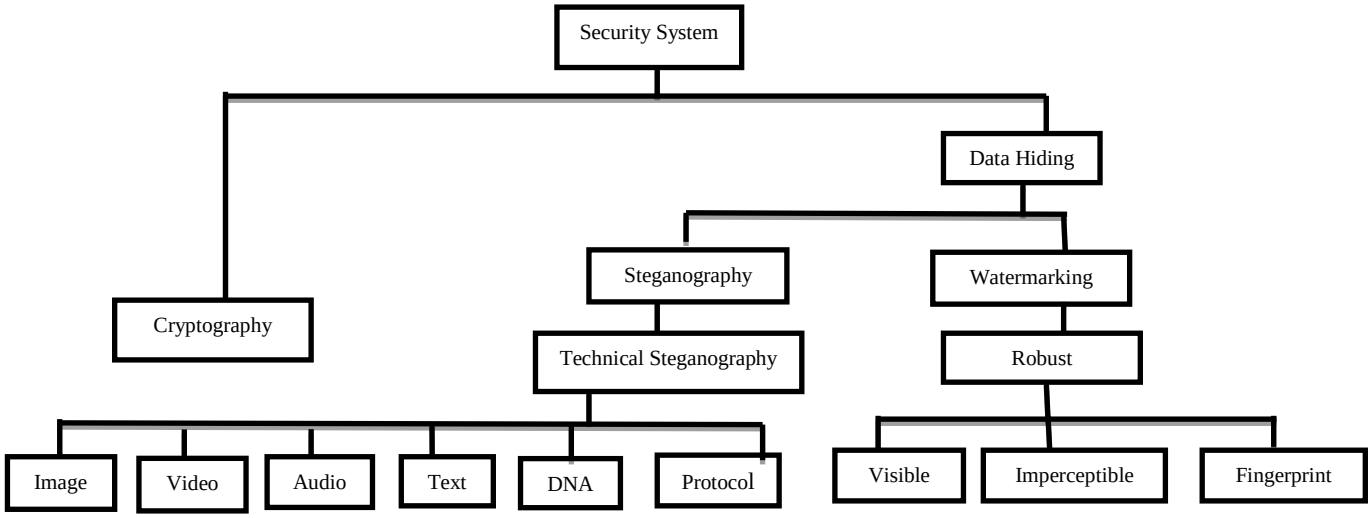

Figure 1.The different disciplines of information hiding

3. APPLICATIONS

There are various digital images steganography applications, including secret communications, and copyright protection smart ID's, printers etc. [8] [5].

3.1 Secret Communications

In many circumstances, transmitting a cryptographic message attract unwanted attention. Though, the steganographic message does not publicize covert communication and consequently it avoids scrutiny of the sender, message and receiver. A blueprint, trade secret, secret military information, or other sensitive information can be transmitted without notifying potential attackers.

3.2 Copyright Protection

Inside an image a secret copyright information or watermark can be embedded to identify it as an intellectual property [6] [7]. This is achieved by Watermarking scenario where the message is the watermark and it is a complex structure. So the intruder cannot identify the copyright information. There are many techniques available to find the watermarking. . A watermark can also serve to detect whether the image has been subsequently modified [9]. Watermarking is achieved by statistical, correlation, similarity check or by measuring other quantity characteristic to the watermark in a stego-image. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent surge of interest in digital steganography and data embedding.

3.3 Smart Id's

In smart ID's the information of the person is embedded inside their image for confidential information. For an association, the authentication of the resources is accessed by the employees. So identifying the stealing related to prevention of crimes [10].

3.4 Printers

Some modern printers like HP printer use steganography technique for embedding confidential information. In these printers, very tiny yellow dots are placed into all pages. Confidential Information is concealed inside the yellow dots like date and time stamp, serial number. Property is available in laser printer for watermarking the confidential information [11].

4. IMAGE STEGANOGRAPHY METHODS

Steganography for binary images [12] [13] is mainly concentrate on hiding data in gray-scale images and color images. The luminance component of a color image is equivalent to a gray-scale image. It is commonly considered that gray-scale images are more appropriate than color images for hiding data [14] because the disturbance of correlations between color components may simply reveal the trace of embedding data. In this section we give an overview of the most important and popular steganographic techniques in digital images. The most common image file formats on the internet are Joint Photographic Experts Group (JPEG), Graphics Interchange Format (GIF) and to a lesser extent - the Portable Network Graphics (PNG). Maximum techniques were set up to exploit the structures of these file formats with some exceptions in the literature that use the Bitmap format (BMP) for its simple data structure.

4.1 Spatial domain steganography

The common ground of spatial steganography is to directly modify the image pixel values for hiding data. The embedding rate is often measured in bit per pixel (BPP). In the spatial domain steganography techniques a steganographer modifies the secret data and the cover medium in the spatial domain, which includes encoding at the level of the LSBs. This

method although simpler, has a larger impact compared to the other two types of methods [15]. According to the data embedding manner, we review six major kinds of steganography in the following.

4.1.1 Least Significant Bit Based Steganography

In least significant bit technique the LSBs of each pixel in the cover object are substituted with the binary equivalent of the message data which is to be hidden. LSB steganography technique is one of the traditional techniques which is capable of hiding secret data in a digital cover image without introducing many perceptible distortions [14]. This technique works by substituting the least significant bits of randomly selected pixels in the cover image with the secret data bits. The selection of pixels may be determined by a secret key. Least significant bit (LSB) is simple approach for embedding data in a cover object. The most popular image formats that use lossless compression is 24 Bit BMP (Bitmap), use for hiding data. It is an easier to hide data inside in a high quality and resolution image. Due to their size 24 Bit images file are best for hiding data. But you can also choose 8 Bit BMP"s or another image file format such as GIF [16]. 8-bit images are not as tolerant to LSB substitution due to their colour limitations. There has be various methods with varying success levels that Steganography software authors have come up with to hide information in 8-bit images. The only drawback with this technique is that it is highly susceptible image compression and formatting to attacks [17] [18]. The data hiding operation of LSB steganography may be defined by the following equation:

$$y_i = 2\left\lfloor \frac{x_i}{2} \right\rfloor + m_i$$

In this equation m_i,x_i, and y_i are the i[th] message bit, the i[th] selected pixel value before hiding and that after hiding, respectively. Numerous steganographic tools are using the LSB based steganographic technique, like S-tools, Steg hide; Steganos, etc. which are available on the Internet.
For example we have three adjacent pixels (9 bytes) with the RGB encoding [19] (figure 2)-

10010100	00001100	11001001
10010111	00001110	11001011
10011111	00010001	11001011

Figure: 2

1001010**1**	0000110**1**	1100100**0**
1001011**0**	0000111**1**	1100101**0**
1001111**0**	0001000**0**	1100101**0**

Figure: 3

The binary representation of number 400 is 110010000 hidden into the least significant bits of these pixels of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in red color and underline have been changed) (figure3) Number 400 was embedded into the grid and LSB have changed according to the embedded message.

4.1.2 Multiple Bit-planes Based Steganography

The procedure of LSB data hiding technique can be simply extended to concealing the data in multiple bit-planes. Non-adaptive data hiding method reduced the perceptual quality of a stego image if some high bit-planes are involved in concealing arbitrarily without employing the local property. It is one major defect of this kind of extension. Kawaguchi and Eason proposed the bit-plane complexity segmentation (BPCS) steganography to address this problem [20]. In this technique, the cover image which is denoted in pure-binary coding system will be initially transformed to canonical Gray coding system. After that the cover image is break down into a set of binary images according to the bit-plane.

Following, for each candidate hiding canonical Gray coding bit-plane, its analogous binary image is separated into successive and non-overlapping chunks of size$2^L \times 2^L$, where L = 3 is a suggested option. The complexity of an image-block is calculated by

$$\propto = \frac{k}{2\times 2^L \times (2^L - 1)} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

It is greater than a predefined threshold α_0, such a chunk is regarded as noise-like and appropriate for data hiding. In Eq. (1) k is the total number of black-and-white borders in the chunk. Simultaneously, secret message data are grouped into a series of data-chunks with the size $2^L \times 2^L$. if complexity of a data-chunk is less than α_0 then chunk is processed by a conjugation operation. The complexity of the conjugated data-chunk will be $(1-\alpha)$ greater than α_0 [20]. Then the noise-like data-chunks will substitute the noise-like image-chunks to carry secret data. After data embedding process whole image is transformed back to PBC system. Data embedding rate of BPCS steganography may achieve as high as 4 bpp without causing powerful visual artefacts.

4.1.3 Noise-adding Based Steganography

The consequence of data hiding is "pairs of value" occurs in LSB steganography. So as to avoid pairs of value statistical attack, LSB matching is proposed which is a minor alteration of LSB steganography technique [21] [22] [23]. In its place of substituting the LSB pixels of the cover image, LSB matching increase or decrease them by 1, if data bits do not match with them.

Actually, LSB matching is treated as a special case of ±k steganography with k = 1, that increases or decreases the value of pixel by ±k for matching its LSB bits with the binary data bit [24]. Due to non-adaptive ±k embedding, the distortion may be modelled as an additive independent identically distributed noise signal with the probability mass function (PMF) as given below.

$$P_{+k} = \frac{p}{4}, P_0 = 1 - \frac{p}{2}, P_{-k} = \frac{p}{4} \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (2)$$

In the equation p is the data embedding rate in bit per pixel (BPP).Author Fridrich proposed another different noise-adding steganography technique which is known as stochastic modulation steganography [25]. Data bits are concealed in the digital cover image by adding a weak noise signal with a specified but arbitrary probabilistic distribution. In stochastic modulation steganography parametric parity function p (x, z) is used. It is required to satisfy the anti-symmetric property for x, i.e. $\mathrm{p}(\mathrm{x}+\mathrm{z},\mathrm{z}) = -\mathrm{p}(\mathrm{x}-\mathrm{z},\mathrm{z})(z \neq 0)$. Parity function proposed by Sharp [21] which is given as follows.

$$\text{If } x \in [1, 2z], p(x,z) = \begin{cases} (-1)^{x+z} & If\ z > 0, \\ 0 & If\ z = 0. \end{cases}$$

If $x \in [1, 2z], p(x, z)$ is calculated according to the anti-symmetric property.

In the data hiding process of stochastic modulation, firstly sequential or random visiting path and the stego-noise ξ_n which will be added, are generated using a secret key.

Thereafter, for the pixel x_i along the visiting path, one sample n_i of the stego-noise $\xi_n$is round off to an integer z_i. In fact if the value of $z_i = 0$, then the pixel x_i is skipped and together the next stego-noise sample is input and rounded, but when the value of $z_i \neq 0$, then the pixel x_i will be altered according to the value of the parity function. Which is given fallow

$$\text{If } p(x_i + z_i,\ z_i) = m_k \text{ then } y_i = x_i + z_i,$$

$$\text{Else if } (x_i + z_i,\ z_i) = -m_k \text{ then } y_i = x_i - z_i$$

In the above equation m_k is the k^{th}data bit. During the data hiding process, pixels which is out of the range of [0, 255] that can be definitely truncated to the closest values in this range with the needed parity.

The data embedding operations of LSB matching and $\pm k$ steganography are different from LSB steganography. The data extraction process in stochastic modulation steganography is that, first generate the same rounded stego-noise sequence z_i from the stego key as same as done during data hiding process and acquired the same pseudo-random path in the stego image. After that apply the parity function $p(x, z)$to the pixel values.

4.1.4 Prediction Error Based Steganography

For maintaining visual quality of image it is intuitive to think that secret data should be hidden in complex areas of the image. Local complexity is assessed by one way to use the pixel prediction error. Data can be hidden into the prediction errors. To predict the current pixel value use a pixel's neighboring pixel to get their difference this can be considered as a type of prediction error. It is a simple way to evaluate prediction error. In the pixel value differencing (PVD) steganography, an image is separated into non-overlapping and consecutive groups of two neighboring pixels [26]. The embedded secret data are hidden into the difference values.

Suppose two neighboring pixels,p_i and p_{i+1} , are used and their difference value is $d_i = p_{i+1} - p_i$ where $0 \leq |d_i| \leq 255$. A large $|d_i|$ means a complex block. Then classify $|d_i|$ into a set of contiguous ranges, denoted by R_k , where k = 0, 1… K - 1is the range index. Denote l_k, u_k and w_k as the lower bound, the upper bound, and the width of R_k, respectively. The value of w_k is designed to be a power of 2.If $|d_i| \in R_k$ then corresponding two pixels are expected to carry $\log_2(w_k)$ bits. That is, their pixel values are changed so that the absolute value of their new difference equals to $|d'_i| = q_{i+1} - q_i = l_k + v_i$, where v_i is the decimal value of the to-be-embedded bits. The embedding operation can be described as

$$(q_i, q_{i+1}) = \begin{cases} (p_i - r_c, p_{i+1} + s_f) & If\ d_i\ is\ odd, \\ (p_i - r_f, p_{i+1} + s_c) & If\ d_i\ is\ even \end{cases}$$

Where $s_c = \left\lfloor \frac{d'_i - d_i}{2} \right\rfloor$ and $s_f = \left\lfloor \frac{d'_i - d_i}{2} \right\rfloor$ in this way, the embedding distortion is distributed almost equally in two pixels. In Bob's side, the difference values can be obtained. If $|d'_i| \in R_k$, the decimal value of the embedded bits is computed as $v_i = |d'_i| - l_k$.

4.1.5 Quantization Based Steganography

Chen and Wornell [27] proposed quantization index modulation (QIM) as a most popular data hiding technique used in digital watermarking and it can be also used in steganography. This technique quantizes the input signal x to the output y with a set of quantizers. It is determined by the data bit m that which quantizer is used for quantization. A standard scalar Quantization index modulation with quantization step Δ for embedding binary data is basically defined as:

$$y_i = Q_M(x_i) = \begin{cases} \Delta \left\lfloor \frac{x_i}{\Delta} + \frac{1}{2} \right\rfloor & if\ m_i = 0 \\ \Delta \left\lfloor \frac{x_i}{\Delta} \right\rfloor + \frac{\Delta}{2} & if\ m_i = 1 \end{cases}$$

If the standard QIM is applied in spatial domain then the histogram shows a sign of discreteness in the integer multiple of $\Delta/2$, particularly when $\Delta > 2$. But it is infrequent for a spatial image to have such a kind of quantization phenomenon. So QIM is frequently employed to the coefficients in the transform domain which are desirable to be quantized. Noda et al. [28] stated that QIM can be used with JPEG compression.

Irregular of QIM is basically known as dither modulation (DM) [27] [29]. QIM create the output values only at the rebuilding points of quantizers but dither modulation can create the output signal acquired all of the values of the input signal. Such type of efficiency is attained by incorporating a dither signal to the input signal before quantization and deducting it after quantization. Which is depicted as,

$$y_i = Q_m(x_i + d_i) - d_i$$

In the above equation dither signal d_i is determined by a key and consistently distributed over$\left[-\frac{\Delta}{4}, \frac{\Delta}{4}\right]$. Dither signal can be frequently used in spatial image to bypass production of the histogram sparse, however it is also more frequently used for transform coefficients.

4.2 Steganography in the image frequency domain

Steganography in the image frequency domain algorithms developed to increase the performance over their ancestors (spatial domain methods). Rapid development in the field of information technology it is necessary to enhanced the security system. The discovery of the LSB data embedding technique is actually a big achievement in field of information security, weak resistance of LSB to attacks left researchers speculating that where to apply it next until they effectively applied it within the frequency domain.

The explanation of the two-dimensional DCT for an input image F and an output image T is calculated as:

$$T_{pq} = \propto_p \propto_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{mn} \cos\frac{\pi(2m+1)p}{2m} \cos\frac{\pi(2n+1)q}{2n} \quad \ldots (1)$$

Where

$$0 \leq p \leq m-1$$
$$0 \leq q \leq n-1$$

And

$$\propto_p = \begin{cases} 1/\sqrt{M} & p = 0 \\ \sqrt{2/M} & 1 \leq p \leq M-1 \end{cases}$$

$$\propto_q = \begin{cases} 1/\sqrt{N} & q = 0 \\ \sqrt{2/N} & 1 \leq q \leq N-1 \end{cases}$$

Where M, N are the dimensions of the input image while m and n is variables which are ranging from 0 to $M-1$ and 0 to $N-1$ respectively.

JPEG is the very popular image file format which is generated by image capturing devices such as digital cameras, scanners and other photographic. Consequently, hiding secret data into JPEG images may offer better concealment. The maximum steganographic techniques embed data into the non-zero alternate current (AC) discrete cosine transform (DCT) coefficients of JPEG images. The data embedding rate of JPEG steganographic is often calculated in bit per non-zero AC DCT coefficient. Discrete cosine transform (DCT) is used broadly with image and video compression i.e. JPEG lossy compression. Every block DCT coefficients got from the equation (1) are quantized using a precise quantization table (QT). Main logic behind selecting a table with such values is that it is based on extensive experimentation which tried to balance the trade-off between quality factors and image compression. The Human Visual System (HVS) dictates the ratios between values in the quantization table.

The goal of quantization is to retain the valuable data descriptors while losing up the tightened precision produced by DCT.

$$f'(\omega_x,\omega_y)=\left\lfloor\frac{f(\omega_x,\omega_y)}{\Gamma(\omega_x,\omega_y)}+\frac{1}{2}\right\rfloor,\qquad \omega_x,\omega_y\in 0,1\ldots\ldots 7$$

Where $f(\omega_x,\omega_y)$ is an 8×8 non-overlapping image blocks, image coordinates are denoted by x and y, $f'(\omega_x,\omega_y)$denotes the result function and $\lfloor.\rfloor$ a floor rounding operator. $\Gamma(\omega_x,\omega_y)$ Signifies a quantization step is described by:

$$\Gamma(\omega_x,\omega_y)=\begin{cases}max\left(\left\lfloor\frac{200-2Q}{100}QT(\omega_x,\omega_y)+\frac{1}{2}\right\rfloor,1\right) & 50\le Q\le 100\\ \left\lfloor\frac{50}{Q}QT(\omega_x,\omega_y)+\frac{1}{2}\right\rfloor\quad , & 0\le Q\le 50\end{cases}$$

Where Q is a quality factor and $QT(\omega_x,\omega_y)$ is the quantization table. JPEG compression then applies entropy coding like Huffman algorithm to compress the resulted $QT(\omega_x,\omega_y)$ maximum redundant data and noise are lost in this stage, therefore it is call lossy compression [30].

The above scheme is a discrete theory independent of steganography. According to Li and Wang steganographic method that changes the QT and inserts the concealed data bits in the middle frequency coefficients [31]. Most of the methods here use JPEG images as carrier to embed their data. JPEG image compression uses the DCT to transform consecutive sub image blocks into 64 DCT coefficients.

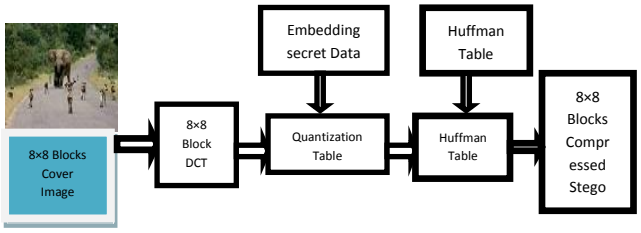

Figure 4: Data Flow Diagram of bit embedding in the frequency domain

Information is embedded into these coefficients' insignificant bits; however, changing any single coefficient would effect on the whole 64 block pixels [32]. As the modification is operating on the frequency domain in place of the spatial domain there will be no visible modification in the digital cover image given those coefficients are controlled carefully [33].

4.2.1 JSteg

The JSteg algorithm was the first algorithms to use the JPEG images. Though the algorithm stood powerfully against visual attacks and it was found that inspect the statistical distribution of the DCT coefficients which shows the existence of concealed data [34]. JSteg is simply detected using the X^2-test. Furthermore, since the DCT coefficients required to be handle with susceptible care. According to Wayner coefficients in JPEG compression generally fall along a bell curve and the concealed data embedded by JSteg distorts this [35]. an algorithm that utilizes the probability density function (PDF) to produce discriminator features fed into a neural network system which detects concealed data in this domain.[36].

There are two standard JPEG steganographic tools viz., JSteg [37] and JPHide [38] that utilized the LSB data embedding technique. JSteg hides secret data into a cover image by sequentially substituting the LSBs of non-zero quantized DCT coefficients by secret data bits. The quantized DCT coefficients which will be used to hide secret data bits in JPHide are selected at random by a pseudo-random number generator that is dissimilar to JSteg and it is controlled by a secret key. Furthermore, JPHide alters not only the LSBs of the certain coefficients but it can also switch to a mode where the bits of the second least significant bit-plane are altered.

4.2.2 F5

Westfeld [39] presented F5 steganographic algorithm. It is based on n subtraction and matrix encoding. So it is also known as syndrome coding. The absolute value of the coefficient is decreased by one if it is needed to be modified instead of substituting the LSBs of quantized DCT coefficients with the data bits. Westfeld and Pfitzmann [40], contended that such type of data embedding cannot be noticed by using the chi-square attack. The algorithm F5 embedded data bits into randomly selected DCT coefficients and it also employs matrix embedding which minimizes the necessary number of modifications to conceal a data of certain length. In the process of data embedding, the length of data and the number of non-zero AC coefficients are used to determine the best matrix embedding which minimizes the number of modifications of the cover image.

According to J. Fridrich et. al [41] a shrinkage happens when the similar bit has to be re-embedded, in case the original coefficient is either ''1'' or ''-1'' as at the decoding phase all zero coefficients will be skipped whether they were changed or not. X^2-test could break this solid algorithm. So F5 did not handle attacks for too long. J. Fridrich et al. [42] proposed a steganalysis which detect F5 contents.

4.2.3 OutGuess

N. Provos and P. Honeyman [43] proposed OutGuess as UNIX source code. OutGuess was a better alternative as it used a pseudo-random-number generator to select DCT coefficients. There are two famous released version of OutGuess first is OutGuess-0.13b, which is susceptible to

statistical analysis and second is OutGuess-0.2, which contains the capacity to conserve statistical properties.

The process of data embedding in OutGuess is initiated into two phases. In First phase OutGuess embeds secret data bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0's and1's. In second phase, corrections are then made to the coefficients that is not selected during the embedding phase, for making the global discrete cosine transform (DCT) histogram of the stego image match that of the cover image. OutGuess cannot be detected by chi-square attack [40]. TheX2-test does not detect the data which is randomly distributed. Provos et al. [43] [44] suggest applying an extended version of the X2-test to select Pseudo-randomly embedded data in JPEG images.

4.2.4 YASS

Data is not embedded in JPEG DCT coefficients directly by the Yet Another Steganographic Scheme (YASS) which is related to JPEG steganography [45]. In its place, an input cover image in spatial representation is initially separated into blocks in the fixed big size, and these blocks are named big blocks (or B-blocks). Each B-block further divide in 8×8 sub-blocks, and such blocks referred to as embedding host block (or H-block). These host blocks are selected randomly with a secret key for performing DCT. Subsequent, secret data is encoded by error correction codes and embedded it in the DCT coefficients of the H-blocks by Quantization index modulation (QIM). The entire digital image is compressed and distributed as a JPEG image after performing the inverse DCT to the H-blocks. For extracting data from stego image, image is firstly JPEG-decompressed to spatial domain. After that the data are fetched from the DCT coefficients of the H-blocks. Later the position of the H-blocks may not overlay with the JPEG 8×8 grid. The data embedding artifacts induced by YASS are not directly resembled in the JPEG DCT coefficients. The process of self-calibration is a strong technique in JPEG steganalysis for assessing the cover image statistics, is deactivated by YASS [46] [47]. Additional advantage of YASS is that the embedded data may endure in the active warden scenario. YASS-like method to increase the security performance of YASS via enhancing block randomization proposed by Yu et al [48]. Huang et al [49] proposed a comparative security performance of YASS and F5 against state-of-the-art steganalytic techniques.

4.2.5 Discrete Wavelet Transform

It is well known that steganography in the discrete wavelet transform (DWT), the reader is advised to see few examples in the available literature in DWT [50] [51] [52]. Abdulaziz and Pang [53] stated that use vector quantization called Linde-Buzo-Gray (LBG) coupled with block codes known as BCH code and 1-stage discrete Haar wavelet transforms. They acknowledged that transforming data using a wavelet transformation conserves good quality with little perceptual artefacts.

Abdelwahab and Hassan [54] proposed a steganographic technique in the DWT domain. Both secret and cover images are decomposed using DWT. They are divided into the discrete disjoint 4×4 blocks and blocks of the secret image fit into the cover blocks to determine the best match. Next, error blocks are created and embedded into the coefficients of the best matched blocks in the HL of the cover image. There are two keys must be needed for communication , one which holds the indices to the matched blocks in the CLL (cover approximation) and another for the matched blocks in the CHL of the cover.

Nag et al proposed a data hiding technique based on DWT and Huffman coding [55]. Secret data after applying Huffman coding is embedded in high frequency components of 2-D DWT of the cover image and low frequency component is kept untouched, not to disturb visual quality of image.

4.2.6 Model-Based Steganography

A general framework proposed by Sallee [56] for the operating steganography and steganalysis with the help statistical model of the digital cover media. This steganographic method for JPEG images, achieves a high data capacity while remaining secure against several first order statistical attacks. MB acquired the separation of the carrier into a deterministic random variable X_{det} and an in-deterministic variable X_{indet} . While an appropriate model is occupied to define the distribution of X_{indet}, which resembled the dependencies with X_{det}. A common model is parameterized with the definite values of X_{det} of an actual cover image, which advance it to a cover specific model. The main determination of this model is to determine the conditional distributions $\mathrm{P}(X_{indet} | X_{det} = X_{det})$. An arithmetic decompression function is mainly used for the appropriate uniformly distributed data bits for the required distribution of X_{indet} by substituting X_{indet} to X_{indet}^{*} that has like properties and comprises the confidential data.

4.2.7 Adaptive image steganography

Adaptive image steganography is a form of enhanced image steganography. Adaptive steganography is a special case of the two former techniques. Which is also known as ‘‘Statistics-aware embedding’’ [3], ‘‘Masking’’ [34] or ‘‘Model-Based’’ [56]. Adaptive steganography technique takes statistical global features of the image before attempting to interact with its LSB/DCT coefficients. The statistics dictate where to make the changes [57] [58]. It is characterized by a random adaptive selection of pixels depending on the cover image and the selection of pixels in a block with large local STD (standard deviation). An adaptive least-significant bit (LSB) steganographic method includes pixel value differencing (PVD) which uses the difference value of two consecutive pixels to estimate the total number of secret data bits that can be embedded into the two pixels. This technique helps to differentiate the smooth and edge areas. A k-bit LSB substitution technique is used for embedding data in the pixels located in the edge areas. This method results in larger payload capacity and high image quality. Another technique proposed under adaptive image steganography is the LSB Matching proposed by A. Ker et al [59]. LSB matching randomly increases or decreases the pixels. J. Spaulding et al proposed BPCS (bit plane complexity segmentation) to compensate for the drawback of the traditional LSB substitution techniques of data embedding [60].

Wayner [35] described about noise in a book to what he called ‘‘life in noise’’, pointing to the usefulness of data embedding in noise. It has been proven to be robust with respect to compression, cropping and image processing [32] [61] [62]. Author describe model-based method (MB1) in literature [56], generates a stego-image based on a specified distribution model, using a generalized Cauchy distribution, which results in the minimum distortion. Due to lack of a perfect steganographic model, this steganographic algorithm can be

broken using the first-order statistics [63]. Additionally, it can also be detected by the difference of ‘‘blockiness’’ between a stego-image and its estimated image reliably [64]. The discovery of ‘‘blockiness’ ’led the author in literature [56] to produce an improved version called MB2, a model-based with de-blocking.

According to Chin-Chen et al. [65] an adaptive technique for index- based images using code word grouping applied to the LSB substitution technique. This technique is to exploit the correlation between neighboring pixels to estimate the degree of smoothness and its resulting embedding capacity was high.

Yang et al. [66] stated that an adaptive LSB steganographic technique using PVD and LSB substitution. In this scheme, the difference value of two consecutive pixels is used to estimate the data concealing capacity into the two pixels. Pixels located in the edge areas are embedded by a k-bit LSB substitution technique. This technique conceal more secret data into the edged areas than smooth areas in the cover image.

5. ANALYSIS

Performance measurement for image distortion is done by the peak-signal-to-noise ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego-images. It is defined as:

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

Where MSE denotes Mean Square Error which is defined as:

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

Where x and y are the coordinates of image, M and N are the dimensions of the image, S_{xy} is the generated stego-image and $C_{xy}$is the digital cover image. C_{max}^2 Holds the maximum value in the image, for example:

$$C_{max}^2 \leq \begin{cases} 1, & double\ precision \\ 255, & unit8\ bit \end{cases}$$

According to authors [33] [67] [68] [69] that $C_{max} = 255$ as a default value for 8bit gray scale images. It can be the case that examine image has only up to 253 or fewer representations of gray colors. C_{max} is raised to a power of 2 results in a severe alteration to the PSNR value. Thus C_{max} can be well-defined as the actual maximum value rather than the largest possible value. PSNR is often represented on a logarithmic scale in decibels (dB). PSNR values falling below 30dB pointed a fairly low quality, i.e., distortion caused by embedding. However, a high quality stego-image should struggle for 40dB and above.

Van Der Weken et al. [70] proposed other similarity measures (SMs). They analyzed the efficiency of ten SMs in addition to a modified version of PSNR created based on neighborhood chunks which better adapt to human perception. Kutter and Petitcolas [71] discussed a new measure adapted to the human visual system to produce a fair performance comparison between different approaches of invisible watermarking.

6. IMPROVING STEGANOGRAPHIC SECURITY

There are few factors which affect the steganographic security, like the number of modified pixels/coefficients, the properties of cover images, the amplitude of the stego-noise signal, etc. Here we discuss some techniques for making the steganography undetectable and much robust.

6.1 Increasing the Data Embedding Efficiency

Surely the sender cannot differentiate the cover image and stego image if cover images don’t necessity to be modified at all for transmission of secret information. So the Security of the steganographic technique may improve and the embedding modifications to the image will decrease if the probability of modification to the image is less. Data embedding efficiency is defined as the amount of embedded bits per one embedding modification. So, enhancing the embedding efficiency, it is a possible way to improve the steganographic security. Crandall [72] proposed and Westfeld [39] implemented Matrix encoding technique which can be used to enhance the embedding efficiency. The key concept is to separate the coefficients into groups and after that use the Hamming error correction codes to limit the modifications in each group. A (d; n; k) code can be used to modify at most d coefficients to embed k bits into n coefficients. When the embedding rate is low then embedding efficiency gets high is the main limitation of using Hamming code. According Fridrich et al. [73] use random linear codes to cope with the case when the data embedding rate is high. To improve embedding efficiency can be found in articles [74] [75] [76].

6.2 Reducing the Data Embedding Distortion

Enhancing the data embedding efficiency, it can decrease the embedding modifications to the image. But it cannot assurance that the distortion to the image will decreased. If all coefficients are not used for transmitting data, sender has the freedom to choose the coefficients which has the minimum resultant distortions after data embedding for modification.

Thus, the stego image will be too close to the digital cover image statistically and perceptually, it improving the steganographic security. First technique which addressing this issue is Perturbed quantization (PQ) steganography [46]. It is understood by modifying some coefficients whose quantization errors are the minimum after data embedding. This technique can be used in a data-reducing process that includes real quantization and transform, like resizing and JPEG compression. Modified matrix encoding (MME) steganography proposed by Kim et al., which modifying coefficients whose both quantization errors and embedding errors are the minimum when embedding data during the JPEG compression process. Uncompressed image is used as an input and employs matrix encoding in this technique during the data embedding process. Ref. [41] stated that minimizing the embedding distortions does make the steganography less noticeable. Fridrich discuss that the exchange between embedding efficiency and embedding distortion [78].

6.3 Selecting Appropriate Digital Cover Images

In some situations, sender has the freedom to select the unsuspicious stego images for transmission of secret data. A technique is proposed by Kharrazi et al. [57] for selecting the best cover images according to the accessibility of the data of a potential steganalyzer. It essentially assumes that the steganalyzer is not error free.

7. FEATURE OF STEGANOGRAPHIC TECHNIQUES

Features of steganography techniques are given in the table 1.

Table 1. Main Feature of steganographic techniques

Steganography	Features
LSB	Modification in the least significant bit
LSB Matching	Plus or minus 1 randomly
Stochastic Modulation	Modulate the embedded data as noise
QIM/DM	Quantizer is determined by data bit (generally in transform domain)
PVD	Embedded data in the difference of neighboring pixel
JSteg	Modification in the least significant bit of JPEG DCT coefficients
MB	Preserve the low-precision model
F5	Decrease the coefficients absolute values and use matrix embedding
YASS	Use randomized locations

8. CONCLUSIONS

In this paper attempts has been made to discuss a background on the key algorithms of digital image steganography. It is to be known that the emerging techniques viz., DCT, DWT and adaptive steganography are not too prone to attacks, particularly when the hidden data is small in size. The reason behind this that they modified coefficients in the transform domain, by which image distortion is kept to a least. Particularly such methods tend to have an inferior payload compared to spatial domain algorithms. There are the many ways to reduce the bits needed to encode a hidden data. Robustness is a real requirement for a steganography and ‘‘many steganography systems that are designed to be robust towards a specific class of mapping. It is also lucid to generate an undetectable steganography algorithm which is capable of resisting image processing manipulations which might occur by accident and not via an attack. The paper gives a few clues and recommendations for designing the steganographic system. Steganography techniques generally struggle for achieving a high embedding rate. It is a good substitute channel for images, video files have several outstanding features for data hiding like large capacity and good imperceptibility.

9. REFERENCES

[1] Hniels Provos & Peter Honeyman,”Hide & Seek: An Introduction to Steganography” IEEE Computer Society Pub-2003.

[2] Ge Huayong, Huang,”Steganography and Steganalysis Based on Digital Image”, International conference & signal Processing-2011IEEE.

[3] N.F. Johnson and S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Computer, 31(2) (1998) 26-34.

[4] J.C. Judge, Steganography: Past, present, future. SANS Institute publication, http://www.sans.org/reading_room/whitepapers/steganography/552.php, 2001.

[5] W Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems Journal, Vol. 35, No. 3 and 4, pp.313-336, 1996

[6] M. Swanson, M. Kobayashi, and A. Tewfik, “Multimedia data embedding and watermarking technologies,” Proceedings of the IEEE, Vol. 86, No. 6, pp. 1064-1087, June 1998.

[7] R. Wolfgang, C. Podilchuk and E. Delp, “Perceptual watermarks for images and video,” to appear in the Proceedings of the IEEE, May, 1999. (A copy of this paper is available at: http://www.ece.purdue.edu/~ace).

[8] N. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen,” IEEE Computer, pp. 26-34, February 1998.

[9] R. B. Wolfgang and E. J. Delp, “Fragile watermarking using the VW2D watermark,” Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents, SPIE Vol. 3657, San Jose, CA, January 1999.

[10] J. Flores-Escalante, J. Pérez-Díaz and R. Gómez-Cárdenas, Design and Implementation of An Electronic Identification Card, Journal Of Applied Research And Technology

[11] Aravind K. Mikkilineni, Osman Arslan , Pei-Ju Chiang, Roy M. Kumontoy, Jan P. Allebach,George T.-C.Chiu, Edward J. Delp, Printer Forensics using SVM Techniques , This research was supported by a grant from the National Science Foundation, under Award Number 0219893

[12] M. Wu, E. Tang, and B. Lin, Data hiding in digital binary image, Proc. of 2000 IEEE International Conference on Multimedia and Expo,vol. 1, pp. 393-396, 2000.

[13] G. Liang, S. Wang, and X. Zhang, Steganography in binary image by checking data-carrying eligibility of boundary pixels, Journal of Shanghai University, vol. 11, no. 3, pp. 272-277, 2007.

[14] Jessica Fridrich, Miroslav Goljan, and Rui Du, Reliable detection of lsb steganography in color and Gray scale images. Proc. of 2001 ACM workshop on Multimedia and security: new challenges, pp.27-30, ACM Press, 2001.

[15] P. Alvarez, Using extended file information (EXIF) file headers in digital evidence analysis, International Journal of Digital Evidence, Economic Crime Institute (ECI) 2 (3) (2004) 1–5.

[16] V. Lokeswara Reddy, Dr.A.Subramanyam, Dr.P. Chenna Reddy, “Implementation of LSB Steganography and its Evaluation for Various File Formats”, Int. J. Advanced Networking and Applications 868 Volume: 02, Issue: 05, Pages: 868-872 (2011)

[17] Morkel, T., Eloff, J.H.P., Olivier, M.S.: An Overview of Image Steganography. University of Pretoria, South Africa (2002)

[18] Wang, H., Wang, S.: Cyber Warfare: Steganography vs. Steganalysis. Communications of the ACM 47(10) (2004)

[19] T. Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa, June/July 2005

[20] Eiji Kawaguchi and Richard O. Eason, Principle and applications of bpcs steganography, In Multi-media Systems and Applications, vol. 3528, pp. 464-473, SPIE, 1998.

[21] T. Sharp, An implementation of key-based digital signal steganography, Proc. of the 4th Information Hiding Workshop, vol. 2137, pp. 13-26, Springer, 2001.

[22] J. Mielikainen,Lsb matching revisited, IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.

[23] X. Li, B. Yang, D. Cheng, and T. Zeng, A generalization of lsb matching, IEEE Signal Processing Letters, vol. 16, no. 2, pp. 69-72, 2009.

[24] J. Fridrich, D. Soukal, and M. Goljan, Maximum likelihood estimation of secret message length embedded using pmk steganography in spatial domain, Proc. of IST/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VII, vol. 5681, pp. 595-606, 2005.

[25] J. Fridrich and M. Goljan, Digital image steganography using stochastic modulation, Proc. Of IST/SPIE Electronic Imaging: Security and Watermarking of Multimedia Contents V, vol. 5020, pp. 191-202, 2003

[26] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value diRerencing, Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613-1626, 2003.

[27] B. Chen and G. W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. Information Theory, vol. 47, no. 4, pp. 1423-1443, 2001.

[28] H. Noda, M. Niimi, and E. Kawaguchi, High-performance jpeg steganography using quantization index modulation in dct domain, Pattern Recognition Letters, vol. 27, no. 5, pp. 455-461, 2006.

[29] J.J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, Scalar costa scheme for information embedding, IEEE Trans. Signal Processing, vol. 51, no. 4, pp. 1003-1019, 2003.

[30] A.C. Popescu, Statistical tools for digital image forensics, Ph.D. Dissertation, Department of Computer Science, Dartmouth College, USA, 2005. Available from: http://www.cs.dartmouth.edu/~farid/publications/apthesis 05.htmlS, on 16-05-07 at 12:20.

[31] X. Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences 177 (15) (2007) 3099–31091.

[32] A.M. Fard, M. Akbarzadeh-T, F. Varasteh-A, A new genetic algorithm approach for secure JPEG steganography, in: Proceedings of IEEE International Conference on Engineering of Intelligent Systems, 22–23 April 2006, pp. 1–6.

[33] A.I. Hashad, A.S. Madani, A.E.M.A. Wahdan, A robust steganography technique using discrete cosine transform insertion, in: Proceedings of IEEE/ITI Third International Conference on Information and Communications Technology, Enabling Technologies for the New Knowledge Society, 5–6 December 2005, pp. 255–264.

[34] N. Provos, P. Honeyman, Hide and seek: an introduction to steganography, IEEE Security and Privacy 1 (3) (2003) 32–44.

[35] P. Wayner, Disappearing Cryptography, second ed, Morgan Kaufmann Publishers, 2002.

[36] C. Manikopoulos, S. Yun-Qing, S. Sui, Z. Zheng, N. Zhicheng, Z. Dekun, Detection of block DCT-based steganography in gray-scale images, in: Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9–11 December 2002, pp. 355–358.

[37] Derek Upham, Jsteg, http://zooid.org/ paul/crypto/jsteg/.

[38] Allan Latham, Jphide, http://linux01.gwdg.de/ alatham/stego.html.

[39] A. Westfeld, F5-A steganographic algorithm: high capacity despite better steganalysis, in: Proceedings of Fourth International Work-shop on Information Hiding, Lecture Notes in Computer Science, vol. 2137, Pittsburgh, USA, April 2001, pp. 289–302.

[40] A. Westfeld and A. Pfitzmann, Attacks on steganographic systems-breaking the steganographic utilities ezstego, JSteg, steganos, and s-tools-and some lessons learned. Proc. Of the 3rd Information Hiding Workshop, vol.1768, pp. 61-76, Springer, 1999.

[41] J. Fridrich, T. Pevny, J. Kodovsky Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities, in: Proceedings of the ACM Ninth Workshop on Multimedia & Security, Dallas, Texas, USA, September 20–21, 2007, pp. 3–14.

[42] J. Fridrich, M. Goljan, D. Hogeg, Steganalysis of JPEG images: breaking the F5 algorithm, in: Proceedings of Information Hiding: Fifth International Workshop, IH 2002 Noordwijkerhout, The Netherlands, Lecture Notes in Computer Science, Springer, October 7–9, 2002, 2578/2003, pp. 310–323.

[43] N. Provos, P. Honeyman, Detecting steganographic content on the Internet, Centre for Information Technology Integration, University of Michigan, Technical report, August 31, 2001

[44] N. Provos, Defending against statistical steganalysis, Centre for Information Technology Integration, University of Michigan, Technical report, February 2001.

[45] K. Solanki, A. Sarkar, and B. S. Manjunath, Yass: Yet another steganographic scheme that resists blind steganalysis, Proc. of the 9th Information Hiding Workshop, Springer, vol. 4567, pp. 16-31, 2007.

[46] J. Fridrich, Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes, Proc. of the 6th Information Hiding Workshop, Springer, vol. 3200 , pp. 67-81, 2004.

[47] Tomas Pevny and Jessica Fridrich, Merging markov and dct features for multi-class jpeg steganalysis. Proc. of SPIE: Electronic Imaging, Security, Steganography, and

Watermarking of Multimedia Contents IX, vol. 6505, pp. 3-14, 2007.

[48] Lifang Yu, Yao Zhao, Rongrong Ni, and Yun Q. Shi, A high-performance yass-like scheme using randomized big-blocks, Proc. of the IEEE International Conference on Multimedia and Expo (ICME 2010), 2010.

[49] Fangjun Huang, Jiwu Huang, and Yun Qing Shi, An experimental study on the security performance of YASS, IEEE Trans. Information Forensics and Security, vol. 5, no. 3, pp. 374-380, 2010.

[50] W.Y. Chen, Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation, Applied Mathematics and Computation 185 (1) (2007) 432–448.

[51] V.M. Potdar, S. Han, E. Chang, A survey of digital image water-marking techniques, in: Proceedings of the IEEE Third International Conference on Industrial Informatics (INDIN), Perth, Australia, 10–12 August 2005, pp. 709–716.

[52] B. Verma, S. Jain, D.P. Agarwal, Watermarking image databases: a review, in: Proceedings of the International Conference on Cogni-tion and Recognition, Mandya, Karnataka, India, 22–23 December 2005, pp. 171–179.

[53] N.K. Abdulaziz, K.K. Pang, Robust data hiding for images, in: Proceedings of IEEE International Conference on Communication Technology, WCC-ICCT'02, vol. 1, 21–25 August 2000, pp. 380–383.

[54] A.A. Abdelwahab, L.A. Hassan, A discrete wavelet transform based technique for image data hiding, in: Proceedings of 25th National Radio Science Conference, NRSC 2008, Egypt, March 18–20, 2008, pp. 1–9.

[55] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, A novel technique for image steganography based on DWT and Huffman coding, IJCSS, vol. 4, no. 6, pp. 561-570.

[56] P. Sallee, Model-based steganography, Proc. of the 2nd International Workshop on Digital Water-marking, vol. 2939, pp. 154-167, Springer, 2003.

[57] M. Kharrazi, H.T. Sencar, N. Memon, Performance study of common image steganography and steganalysis techniques, Journal of Electrical Imaging 15 (4) (2006) 1–16.

[58] R. Tzschoppe, R. Baum, J. Huber, A. Kaup, Steganographic system based on higher-order statistics, in: Proceedings of SPIE, Security and Watermarking of Multimedia Contents V. Santa Clara, California, USA 2003, vol. 5020, pp. 156–166.

[59] A. Ker, "Steganalysis of LSB Matching in Grayscale Images." IEEE Signal Processing Letters, vol. 12(6), pp. 441–444, 2005

[60] J. Spaulding, H. Noda, M.N. Shirazi, E. Kawaguchi, BPCS steganography using EZW lossy compressed images, Pattern Recognition Letters 23 (13) (2002) 1579–1587.

[61] C.C. Chang, H.W. Tseng, A steganographic method for digital images using side match, Pattern Recognition Letters 25 (12) (2004) 1431–1437.

[62] E. Franz, A. Schneidewind, Adaptive steganography based on dithering, in: Proceedings of the ACM Workshop on Multimedia and Security, September 20–21, 2004, Magdeburg, Germany, pp. 56–62.

[63] R. Bohme, A. Westfeld, Breaking cauchy model-based JPEG steganography with first order statistics, in: Proceedings of the European Symposium on Research in Computer Security, ESORICS 2004, Valbonne, France, 13th September 2004, Lecture Notes in Computer Science, vol. 3193, p p. 125–140.

[64] L. Yu, Y. Zhao, R. Ni, Z. Zhu, PM1 steganography in JPEG images using genetic algorithm, Soft Computing 13 (4) (2009) 393–400

[65] C.C. Chang, P. Tsai, M.H. Lin, An adaptive steganography for index- based images using code word grouping, Advances in Multimedia Information Processing-PCM, Springer, vol. 3333, 2004, pp. 731–738.

[66] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Hung-Min Sun Adaptive data hiding in edge areas of images with spatial LSB do-main systems. IEEE Transactions on Information Forensics and Security, 2008, vol. 3, no. 3, p. 488-497.

[67] Y.H. Yu, C.C. Chang, I.C. Lin, A new steganographic method for color and grayscale image hiding, Computer Vision and Image Under-standing 107 (3) (2007) 183–194.

[68] M. Drew, S. Bergner, Spatio-chromatic de-correlation for color image compression, Technical Report, School of Computing Science, Simon Fraser University, Vancouver, Canada, 2007, available from:/http:// fas.sfu.ca/pub/cs/TR/2007/CMPT2007-09.pdfS.

[69] M. Saenz, R. Oktem, K. Egiazarian, E. Delp, Colour image wavelet compression using vector morphology, in: Proceedings of the European Signal Processing Conference, September 5–8 2000, Tampere, Finland, 2000, pp. 5–8

[70] D. Van Der Weken, M. Nachtegael, E. Kerre, Using similarity measures and homogeneity for the comparison of images, Image and Vision Computing 22 (9) (2004) 695–702.

[71] M. Kutter, F. Petitcolas, A fair benchmark for image watermarking systems, in: Proceedings of Electronic Imaging '99, Security and Watermarking of Multimedia Contents, San Jose, California, USA, 25–27 January 1999, vol. 3657, pp. 226–239

[72] R. Crandall, Some notes on steganography, Posted on steganography mailing list, http://os.inf.tu-dresden.de/ westfeld/crandall.pdf, 1998.

[73] J. Fridrich and D. Soukal, Matrix embedding for large payloads, IEEE Trans. Information Forensics and Security, vol. 1, no. 3, pp. 390-395, 2006.

[74] W. M. Zhang, X. P. Zhang, and S. Z. Wang, A double layered plus-minus one data embedding scheme, IEEE Signal Processing Letters, vol. 14, no. 11, pp. 848-851, 2007.

[75] J. Fridrich, P. Lisonek, and D. Soukal, On steganographic embedding efficiency, Proc. of the 8th

Information Hiding Workshop, Springer, no. 4437, pp. 282-296, 2007.

[76] JAurgen Bierbrauer and Jessica Fridrich, Constructing good covering codes for applications in steganography, LNCS Trans. Data Hiding and Multimedia Security III, vol. 4920, pp. 1-22, 2008.

[77] Y. Kim, Z. Duric, and D. Richards, Modified matrix encoding for minimal distortion steganography. Proc. of the 8th Information Hiding Workshop, Springer, vol. 4437, pp. 314-327, 2006.

[78] Jessica Fridrich, Minimizing the embedding impact in steganography, Proc. of the 8th ACM workshop on Multimedia and Security, ACM Press, pp. 2-10, 2006.