Image Steganography and Steganalysis: A Survey

Yambem Jina Chanu
Dept. of CSE, NERIST,
Itanagar

Kh. Manglem Singh
Dept. of CSE, NIT Manipur

Themrichon Tuithung
Dept. of CSE, NERIST,
Itanagar

ABSTRACT

Steganography refers to the technique of hiding secret messages into media such as text, audio, image and video without any suspicion, while steganalysis is the art and science of detection of the presence of steganography. It can be used for the benefit of the mankind to serve us as well as by terrorists and criminals for malicious purposes. Both steganography and steganalysis have received a lot of attention from law enforcement and media. In the past, different steganographic techniques with properties of imperceptibility, undetectability, robustness and capacity have been proposed. Newer and more sophisticated steganographic techniques for embedding secret message will require more powerful steganalysis methods for detection. The battle between steganography and steganalysis is never ending. In this paper, an extensive review report is presented for steganography and steganalysis.

General Terms

Information Hiding, Steganography, Steganalysis

Keywords

Steganography, Steganalysis, LSB embedding, Universal staganalysis, Transform domain, RS algorithm.

1. INTRODUCTION

The important constituents of today's information hiding are cryptography, watermarking and steganography, though each of them has different objectives when serving their purpose. Cryptography is the study of processing digital data by scrambling or encrypting in data bits with a key in such a way that the data is unintelligent to the unauthorized person who does not possess the key to recover or decrypt it. It is very clear in cryptography that the encrypted data stored in the memory or being transmitted takes unreasonable amount of computer processing resources and time during its useful life time to decrypt it. However, message data after decryption may always be distributed in plain form without any restriction, even by the authorized customer. Also encryption clearly marks a message as containing interesting information, and the encrypted message becomes subject to attackers. Watermarking of digital data, on the other hand is the process that enables data called a watermark, digital signature, tag, or label into a multimedia object such as text, audio, image or video in perceptually invisible or inaudible manner without degrading the quality of the object, such that watermark can be detected or extracted later to make an assertion about the object [1-4]. The embedded information can be a serial number or random number sequence, ownership identifiers, copyright messages, control signals, transaction dates, information about the creators of the work, bi-level or gray level images, text or other digital data formats [5]. An important goal of watermarking is to make removal of the inserted watermark bits from the watermarked object impossible without degrading the quality of the object and without additional information such as a key. Second important goal of watermarking is to sense that the object has been tempered by checking that the watermark is being removed or destroyed. Third goal of watermarking is prevention against copying and transmitting music, image, video on CDs and DVDs. Violation of copyrighted materials such as music and video happens frequently [6]. There has been no technique so far developed that meets the expectations of watermarking as desired. Also, it has become a legal to develop, sell or distribute code-cracking commercial software and hardware devices for anti-piracy measures with the advent of Digital Millennium Copyright Act (DMCA) of 1998 [7]. Thus music and video industries no longer depend on watermarking to prove violation of DMCA for copyrighted materials, but they are now rely on other approaches such that, their Internet providers to locate the possible violators.

Almost infinite memory size is available for storing digital data in digital devices, more bandwidth is available for sending digital data efficiently in the Internet, and more freeware is available for embedding secret messages inside other media. Steganography refers to the technique of embedding secret messages inside different cover media such as text, audio, image and video without any suspicion. It can be used in many areas. It can be used for the benefit of the mankind to serve us as well as by terrorists and criminals for malicious purposes. The main purpose of steganography is to transmit hidden message embedded in a cover medium in a stealth way that an unauthorized person cannot extract the very presence of the embedded message. Digital image and video contain high degree of redundancy in representation, thus appealing for data hiding. Steganography finds applications in copyright control of materials, enhancing robustness of image search engines and smart IDs, where individuals' details are embedded in their photographs, video-audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets and checksum embedding [8-10]. It also finds application in medical imaging systems where a separation is considered between patients' image data or DNA sequences and their captions, e.g., physician, patient's name, address and other particulars. Cyber-crime is believed to benefit from steganography [8] as reported in USA TODAY. Examples are found for hiding data in music files [11], and even in a simpler form such as in HyperText Markup Language (HTML), executable files and Extensible Markup Language (XML) [12].

New techniques have been devised in the embedding process to make the detection difficult, however it is still possible to detect the existence of the hidden message.The art and science of detection of the existence of embedded message is called steganalysis. In addition to detection of embedded message, the main goal of steganalysis are to estimate the length of embedded message, to estimate the locations of hidden data in the stego data, to estimate the stego key used by embedding algorithm, to extract the hidden message etc. Steganalysis finds its uses in cyber forensics, cyber warfare, tracking of criminal activities over the Internet and gathering evidence for investigations in case of anti-social elements [8,13-18]. Steganalysis also finds uses in law enforcement and anti-social significance steganalysis for peaceful applications and consequently improving the security of steganographic tools by evaluating and identifying their weakness. The battle between steganography and steganalysis is never ending. Newer and more sophisticated steganographic techniques for embedding secret message will require more powerful steganalysis methods for detection.

Past decade has been growing interest in researches on image steganography and steganalysis. Existing techniques form a very small part of a very big system that calls for exciting and challenging research for the years to come [19-21].

The paper is organized as follows. In Section 2, the classification of steganographic techniques is given. Section 3 deals with the classification of steganalytic techniques, followed by conclusions in Section 4.

2. CLASSIFICATION OF STEGANOGRAPHIC TECHNIQUES

There are three basic types of steganography: spatial steganography, transform steganography and adaptive steganography.

2.1 Spatial Steganography

There are many versions of spatial steganography, but all directly change some bits in the image pixel values in hiding data. Least significance bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions [8]. To our human eye, changes in the value of the LSB are imperceptible, thus making it an ideal place for hiding information without any perceptual change in the cover object. Embedding of message bits can be done either sequentially or randomly. Embedding operation of LSB steganography may be described by the following equation [22].

$$y_i = 2\left\lfloor \frac{x_i}{2} \right\rfloor + m_i \tag{1}$$

where m_i, x_i and y_i are the i-th message bit, the i-th selected pixel value before embedding and that after embedding respectively.

Although LSB embedding methods hide data in such a way that human does not perceive it, these embeddings often can be easily destroyed by compression, filtering or a less than perfect format or size conversion. Hence, it is often necessary to employ sophisticated techniques to improve embedding reliability. Steghide, S-tools, Steganos etc. are based on LSB steganographic technique.

LSB based steganography can be easily extended to hide data in multiple bit-planes, with the precaution that embedding should be done in low bit-planes and in case if high bit-planes are involved, then local property should be checked so as to improve the perceptual quality of the stego image [23]. The image is decomposed to a set of binary images according to the bit-plane complexity segmentation (BPCS), which divides bit-plane into consecutive and non-overlapping blocks. Each block is further checked whether it is noise-like or not, and noise-like blocks are suitable for embedding data. Embedding rate of such technique is as high as 4 bit per pixel (bpp) without causing much severe visual artifacts.

Many steganalysis techniques use “pairs of value” (PoV) that exist in LSB based steganography for detection and extraction of hidden message [24]. To defeat PoV, LSB matching (LSBM) steganographic technique adds or subtract by 1 if LSB does not match with message bit [25,26,27]. LSB matching is a special case of $\pm k$ steganography with $k = 1$ [27]. Embedding operation of LSB matching steganography may be described by the following equation.

$$p_s(i,j) = \begin{cases} p_c(i,j) + 1, \text{if} b \neq \text{LSB}\big(p_c(i,j)\big) \text{and} r > 0 \\ p_c(i,j), \qquad \text{if} b = \text{LSB}\big(p_c(i,j)\big) \\ p_c(i,j) - 1, \text{if} b \neq \text{LSB}\big(p_c(i,j)\big) \text{and} r < 0 \end{cases} \tag{2}$$

where $p_c(i,j)$, $p_s(i,j)$, $\text{LSB}(p_c(i,j)), b$ and r are the original pixel value before embedding, pixel value after embedding at the location (i,j), LSB value of the pixel $p_c(i,j)$, message bit and independent and identically distributed$(i.i.d.)$ random variable with uniform distribution on $\{-1,+1\}$ respectively.

In pixel-value differencing (PVD), a cover image is first segmented into many non-overlapping blocks of two neighboring pixels [28,29]. A difference d is calculated between two pixels in each block, $d = p_{i+1} - p_1$, with $|d| \in [0,255]$. Classify $|d|$ into a number of contiguous ranges, $R_i(k = 0,1,2,\ldots,K-1)$, where the width of R_i is a power of 2. The lower bound, upper bound and width of R_i are denoted by l_k, u_k and $w_k$respectively. If $|d|$ is in R_k, a total of $\log_2(w_k)$ secret bits are embedded into the corresponding 2-pixel block. Convert the $\log_2(w_k)$ secret bits into a decimal value $b$and calculate

$$d' = \begin{cases} l_k + b, \ if d \geq 0 \\ -(l_k + b), \ d < 0 \end{cases} \tag{3}$$

The embedding procedure is described as

$$\begin{aligned} &(p_i', p_{i+1}') = f[(p_i, p_{i+1}), d'] \\ &= \begin{cases} (p_i - r_c, p_{i+1} + r_f), \ \text{if} d \text{is odd} \\ (p_i - r_f, p_{i+1} + r_c), \ \text{if} d \text{is even} \end{cases} \end{aligned} \tag{4}$$

where $r_c = \left\lceil \frac{d'-d}{2} \right\rceil$and $r_f \left\lfloor \frac{d'-d}{2} \right\rfloor$

For any block, if there is any possibility of overflow due to embedding, the block is labeled as unusable and is excluded in embedding.

A message can be embedded in the cover image through the choice of a scalar quantizer. Input signal x is quantized to output y with a set of quantizers $Q_m(.)$ [30]. Quantization index modulation (QIM) with quantization step Δ for embedding binary data can be described as

$$y_i = Q_i(x_i) = \begin{cases} \Delta \left\lfloor \frac{x_i}{\Delta} + \frac{1}{2} \right\rfloor, \ \text{if } m_i = 0 \\ \Delta \left\lfloor \frac{x_i}{\Delta} \right\rfloor + \frac{\Delta}{2}, \ \text{if } m_i = 1 \end{cases} \tag{5}$$

A variant of QIM is dither modulation (DM), which can produce output covering all of the values of input signal, unlike QIM, which gives output only at the reconstruction points of quantizers. The equation for DM is described as

$$y_i = Q_m(x_i + d_i) - d_i \tag{6}$$

where d_i is the dither signal, determined by a key and uniformly distributed over $\left[-\frac{\Delta}{4},\frac{\Delta}{4}\right)$.

Spread-spectrum image steganography hides data in a Gaussian stego noise that is added to the cover image [31]. It is more robust and has a low probability of detection.

2.2 Transform Steganography

New algorithms have been emerging in transform domains due to weak resistance in spatial domain, fast development in computing devices and need for better security system. There are many versions of transform steganography. Some popular transform domains are discrete cosine transform (DCT), discrete wavelet transform (DWT) and singular value decomposition (SVD) respectively.

2.2.1 Discrete Cosine Transform-based Steganography

JPEG is based on DCT in lossy compression and it is the most common format of images produced by digital cameras, scanners and other photographic capture devices.

In JPEG compression, successive sub-image blocks of size of 8×8 on applying DCT produces 64 DCT coefficients, and data can be inserted in these coefficients' insignificant bits. However altering any single coefficient would affect the entire 64 block pixels [32]. No visible change can be seen in the stego-image as the changes due to insertion data are in frequency domain. JSteg embeds secret message into a cover image by successively replacing the LSBs of non-zero DCT coefficients with message bits. Existence of hidden message can be found visually, and JSteg can be easily detected by Chi-Square (X^2) - test [32].

In JPHide, the quantized DCT coefficients that are used to hide secret message bit are selected randomly by a key, generated by a pseudo random number generator, and JPHide can also use the two LSBs of the selected coefficients [33].

F5 algorithm developed by Andreas Westfeld embeds message bit into randomly chosen non-zero AC DCT coefficients by decreasing the absolute value of the coefficient if necessary by 1, and employs matrix embedding that minimizes the necessary number of changes to hide a message of certain length [34]. Neither X^2- test nor extended version could break this algorithm, Fridrich et al [35] detect F5 contents.

OutGuess provided as UNIX source code by Provos uses a pseudo random number generator to select DCT coefficients skipping 0 and 1 to insert message bit [21]. X^2- test could not break OutGuess.

Li and Wang develop a steganographic technique that modifies the quantization table (QT) of JPEG compression and their method inserts the hidden bits in middle frequency coefficients [36].

Model-based steganography (MB) developed by Sallee for JPEG images achieves a high message capacity while remains secure against several first order statistical attacks [37].

Yet Another Steganographic Scheme (YASS) does not embed data in JPEG DCT directly [38]. An image in spatial representation is divided into fixed large size blocks, called B-blocks. Within each B-block, an 8×8 sub-block, referred to as embedding host block (H-block), is randomly selected with a secret key for performing DCT. Secret message, encoded by error correction code are embedded in DCT coefficients of H-blocks by QIM, followed by inverse DCT to H-blocks. The whole image is then compressed as a JPEG image. YASS survives many active suspicious scenario.

2.2.2 Discrete Fourier Transform-based Steganography

Fast Fourier transform is not suitable for hidden communication due to round-off errors [39]. Johnson and Jajodia [8], and McKeon [40] used DFT in Fourier-based steganography.

2.2.3 Discrete Wavelet Transform-based Steganography

DWT-based steganography is still in infancy. Bhattacharya et al develop a dual steganographic technique based on DWT and spread spectrum [41]. Two different secret images after converting into 1-D vectors are inserted into two high frequency components HL_1 and HH_1 of 1-level DWT of the cover images using pseudo random number generator and session key.

Nag et al propose a steganographic technique based on DWT and Huffman coding [42]. Secret message 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.

Bhattacharya et al developed a steganographic technique based on DWT and DCT for color images [43]. Binary secret image is inserted into HH_1 of different color planes after applying 2-DWT and 2-D DCT using 2-D pseudo random key [43].

2.2.4 Singular Value Decomposition-based Steganography

Use of singular value decomposition in steganography is new. Chung et al develop an image hiding scheme based on SVD and vector quantization (VQ) [44].

Bergman and Davidson develop an image steganographic technique based on SVD [45]. The cover image I is factorized into three matrices U, V and D such that $I = UDV'$, where U and V are two orthogonal matrices, and D represents a diagonal matrix, whose diagonal elements are the singular values of I arranged in descending order of magnitudes. The secret message bits are inserted into column elements of the matrix U by adjusting the controllable attributes such that it is still orthogonal after insertion.

Hadhoud and Shallan proprose an image steganographic technique based on SVD that embeds the secret message in the orthogonal matrix U, leaving untouched the diagonal matrix S, for less embedding error and better image fidelity [46].

Raja et al propose robust and high capacity image steganography using SVD (RHISSVD), which embeds message bits in singular values of the cover image [47].

Gorodetski et al propose a robust SVD-based steganography technique, which inserts message bits into singular values of small blocks of segmented cover image by slight modification [48]. The method is robust because it embeds data in low bands of cover in a distributed way.

2.3 ADAPTIVE STEGANOGRAPHY

Some important requirements of a good steganographic scheme are undetectable, robustness against attacks, embedding capacity and imperceptibility. Adaptive steganography is a special case of the two former techniques and it tries to fulfill at least some or all requirements of a good steganographic scheme.

Manglem et al propose a steganographic technique which embeds message bits in edges of the image, which is found by using Laplacian detector on every 3×3 non-overlapping block within the cover images [49]. Some steganalysis tools such as energy gradient steganalysis fail to detect the embedded message in the stego-image, however the embedding capacity is low.

PVD-based steganographic scheme is another edge adaptive scheme, in which the number of embedded bits is determined by the difference between a pixel and its neighbors [28,50,51]. Larger the difference, the larger the number of message bits that can be embedded.

LSB matching revisited (LSBMR) is another edge adaptive steganography technique, which can release more edge regions for embedding message bits [52]. It can resist some of the steganalytic tools also.

The model-based method (MB1) generates a stego-image based on a given distribution model, using a generalized Cauchy distribution, which results in minimum distortion [37]. This algorithm can be broken by the first-order difference [53]

Chang et al propose an adaptive technique applied to LSB steganographic technique [54]. Their technique exploits the correlation between neighboring pixels to estimate the degree of smoothness.

Raja et al choose to use wavelet transforms that map integers to integers instead of using the conventional wavelet transforms, so as to overcome the difficulty of floating point conversion that occurs after embedding [55]. Their method embeds the message bits in non-overlapping 4×4 blocks of low frequency, where two pixels at a time are chosen, one on either side of the principal axis.

Wu and Shih propose a genetic algorithm (GA) based technique that generates a stego-image to break the detection system by artificially counterfeiting statistical features [56].

Kong et al propose a content based steganography scheme based on segmenting homogeneous image areas using a watershed method and fuzzy C-means (FCM) [57]. Four LSBs of each cover image is used to embed secret message bits in the region where entropy is high and two LSBs in low entropy region.

Rakesh et al propose a keyless random steganographic technique that induces enhanced security by incorporating counting out embedding [58]. Their method uses message bits embedded in the current pixel, which acts as a key for the next pixel to which data is to be embedded.

Raju et al propose an adaptive steganography technique based on LSBMR for embedding the message bits after godelizing for improved security [59].

3. CLASSIFICATION OF STEGANALYTIC TECHNIQUES

Steganalysis is the science of attacking steganography in a battle that never ends. Passive steganalysis attempts to destroy the trace of secret communication without bothering to detect the secret message by changing image format, flipping all LSBs, JPEG compression etc., while active steganalysis uses specialized algorithms that detect the existence of stego-image. Steganalysis can be classified into two categories: signature steganalysis and statistical steganalysis. Both categories can be either specific or universal. Specific steganalysis is designed for a particular steganographic embedding algorithm, while universal steganalysis is a general class steganalytic technique, which can be implemented with any steganographic embedding algorithm, even an unknown algorithm.

3.1 Signature Steganalysis

Steganography alters the media properties due to the insertion of message bits in the form of degradation or repeated patterns, which act as signatures that convey the existence of embedded message. Steganographic algorithm such as Hide & Seek produces stego-image that contain pixel values that are divisible by 4, which acts as a specific signature taking the insecure aspect for detection by steganalytic tools [60]. Similarly, steganographic tool Jpegx inserts secret message at the end of JPEG file marker, preceeding with hex code 5B 3B 31 53 00, which acts as a specific signature for detection of secret message in the stego-image [61].

3.2 Statistical Steganalysis

Statistical steganalysis is more powerful than signature steganalysis, because mathematical techniques are more sensitive than visual perception [60].

3.2.1 Specific Statistical Steganalysis

Specific statistical steganalytic tools can be used for detection of secret message from stego-images embedded by LSB embedding, LSB matching, spread spectrum, BPCS, JPEG compression and other transform domain. The powerful and popular LSB detection algorithms are Chi-square [61], RS [61], Gradient Energy-Flipping Rate Detection [63] and Histogram difference [64], which are explained in short below.

The first specific statistical steganalytic tool Chi-Square Attack developed for detection of message bits from stego-images embedded by LSB steganographic tool is based on PoV [61]. L-bit color channel can have $P = 2^L$ possible values. Splitting into 2^{L-1}pairs, which differ only in LSBs gives all possible patterns of neighboring bits of LSBs. Each of these pair is called PoV. The distribution of odd and even values of PoV is same as 0/1 distribution of secret bit if all available LSB fields are to be used. The idea of X^2 - analysis is to compare theoretically expected frequency distribution of PoVs with the real observed one, though no expected frequency is available in absence of original image. Let us assume that the pixel values $c_0, c_1, \dots, c_{P-1}$ are already sorted. For $P \leq 256,$ there are at the most 128 PoVs. For the i-th pair (c_{2i}, c_{2i+1}), $i = 1,2, \dots, k,$ we define $n_i^{'} = 1/2$(number of indices in the set $\{c_{2i}, c_{2i+1}\}$) and n_i= number of indices equal to c_{2i}.The value $n_i^{'}$ is the theoretically expected frequency if a random message has been embedded, and n_i is the actual number of occurrences of pixel value c_{2i}. Chi-square statistics is calculated as

$$X_{k-1}^{2} = \sum_{i=1}^{k} \frac{(n_i - n_i^{'})^2}{n_i^{'}} \qquad (7)$$

with $k-1$ degree of freedom.

The probability of embedding p can be calculated by

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}} \lceil \left(\frac{k-1}{2}\right)} \int_0^{X_{k-1}^{2}} e^{-\frac{x}{2}} x^{\frac{k-1}{1}-1} dx \qquad (8)$$

expressing the probability that the distributions $n_2^{'}$ and n_i are equal and $\lceil$is Euler Gamma function.

Chi- square test works well for sequential embedding, and it is less effective for random embedding unless the embedded bits are hidden in majority of the pixels.

Fridrich et al introduce a powerful steganalytic method known as RS analysis that utilizes the spatial correlation in the stego-images [62]. The basic idea is to discover and quantify the weak relationship between the LSB plane and the image itself. The image I to be analyzed is divided into $G(x_1, \dots, x_n)$ disjoint groups of n adjacent pixels. By defining a discrimination function f, which captures the smoothness of G as follow.

$$f(x_1, \dots, x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i| \qquad (9)$$

With invertible flipping function $F_1: 0 \leftrightarrow 1,\ 2 \leftrightarrow 3,\ \dots,\ 254 \leftrightarrow 255$, shifting function $F_{-1}: -1 \leftrightarrow 0,\ 1 \leftrightarrow 2,\ \dots, 255 \leftrightarrow 256$ and identity function $F_0 = F_0(x), \forall x \in P,$ and with n- tuple mask M with values in $\{-1, 0,\ 1\}$ is classified into three types: R_M, S_MandU_M.

- Regular. $G \in R_M \Leftrightarrow f(F_M(G) > f(G)$ (10)
- Singular.$G \in S_M \Leftrightarrow f(F_M(G) < f(G)$(11)
- Unusable. $G \in U_M \Leftrightarrow f(F_M(G) = f(G)$ (12)

Similarly, we can classify the groups $R_{-M}, S_{-M}$and U_{-M} for the mask $-M$, where $-M$ is the complement of M. As a matter of fact, it holds that
$\frac{R_M + S_M}{T} \leq 1$and $\frac{R_{-M} + S_{-1M}}{T} \leq 1$,

where T is the total number of G groups.
For typical images, the following hold true.
$R_M \approx R_{-M}$ and $S_M \approx S_{-M}$.

The greater the message size, the lower the difference between R_{-M} and S_{-M}, and the greater the difference between R_M and S_M. This behavior is used in detection of hidden message from the stego-image [62].

Zhi et al propose GEFR based on the relation between the length of the embedded message and the gradient energy [63]. Let $I(n)$ be a unidimensional signal. The gradient $r(n)$ before embedding message is

$$r(n) = I(n) - I(n-1) \qquad (13)$$

The gradient energy (GE) of the cover $I(n)$ is

$$GE = \sum |I(n) - I(n-1)|^2 = \sum |r(n)|^2 \qquad (14)$$

After hiding of a signal $S(n)$ in the original signal, $I(n)$ becomes $I'(n)$ and the gradient is re-written as

$$\begin{aligned} r^{'}(n) &= I^{'}(n) - I^{'}(n-1) \\ &= I(n) + S(n) - \big(I(n-1) + S(n-1)\big) \quad (15) \\ &= r(n) + S(n) - S(n-1) \end{aligned}$$

The probability distribution function of $S(n)$ is

$$\begin{cases} \rho_{S(n)=0} = \frac{1}{2} \\ \rho_{S(n)=\pm 1} = \frac{1}{4} \end{cases} \qquad (16)$$

After embedding, the new gradient energy GE' is

$$\begin{aligned} GE^{'} &= \sum |r(n)|^2 = \sum |r(n) + S(n) - S(n-1)|^2 \\ &= \sum |r(n) + \Delta(n)|^2 \end{aligned} \qquad (17)$$

where $\Delta(n) = S(n) - S(n-1)$.
In order to perform detection we need to know a function known as flipping function. Let us consider a cover image I with $W \times H$ pixels and $p \leq W \times H$ be the size of the hidden message .So after applying the flipping function the following are the results.

- For $= W \times H$, there is $\frac{W \times H}{2}$ pixels with inverted LSB. That means that the embedding rate is 50% and the gradient energy is given by $GE = (\frac{W \times H}{2})$.
- The original image's gradient energy is given by $GE(0)$. After inverting all available LSBs using F, the gradient energy becomes $GE^{'} = W \times H$.
- For $p < W \times H$, there is $\frac{p}{2}$ pixels with inverted LSB. Let $I(\frac{p}{2})$ be the modified image. The resulting gradient energy is $GE = \frac{p/2}{W \times H} = GE(0) + p$. If F is applied over $I(\frac{p}{2})$, the resulting gradient energy is $GE = \frac{W \times H - p/2}{W \times H}$.

Using these above mentioned properties, Zhi et al. proposed the detection procedure [63]:

1. Find the test image's gradient energy $GE = \frac{p/2}{W \times H}$;
2. Apply F over the test image and calculate $GE = \frac{W \times H - p/2}{W \times H}$;
3. Find $GE = \left(\frac{W \times H}{2}\right) = \left[GE = \frac{p/2}{W \times H} + GE = \frac{W \times H - p/2}{W \times H}\right]/2$;
4. $GE(0)$ is based on $GE = \left(\frac{W \times H}{2}\right) = GE(0) + W \times H$;
5. Finally, the estimated size of the hidden message is given by

$$p^{'} = GE = \frac{p/2}{W \times H} - GE(0) \qquad (18)$$

Zhang et al introduce the difference image histogram method [64]which deploy the measure of weak correlation between successive bit planes to construct a classifier for which will help to distinguish stego-images and cover images. Here the difference image histogram is used as statistical analysis tool. The difference image is defined as

$$D(i,j) = I(i,j) - I(i,j+1) \qquad (19)$$

where $I(i,j)$denotes the value of the image I at the position (i,j).

There exists a difference between the difference image histograms for normal image and the image obtained after flipping operation on the LSB plane. To know this difference image histogram concept in details we need to know some notions first. Let I be the test image with $M \times N$ pixels. The embedding ratio $\rho$is defined as the percentage of the embedded message length to the maximum capacity.If the difference image histogram of an image is represented by h_i, that of the image after flipping all bits in the LSB plane by f_i and that of the image after setting all bits in the LSB plane to zero by g_i. The following relations exist between three planes as follows:

$$h_{2i} = f_{2i} = a_{2i,2i} g_{2i}$$
$$h_{2i+1} = a_{2i,2i+1} g_{2i} + a_{2i+2,2i+3} g_{2i+2} \qquad (20)$$
$$f_{2i+1} = a_{2i,2i-1} g_{2i} + a_{2i+2,2i+3} g_{2i+2}$$

$a_{2i,2i+j}$is defined as the translation coefficient from the histogram $g_i$to h_i, when $j = 0,1,-1$ we have

$$0 < a_{2i,2i+j} < 1$$
Otherwise (21)
$$a_{2i,2i+j} = 0$$

and they satisfy $a_{2i,2i-1} + a_{2i,2i} + a_{2i,2i+1} = 1$ (22)

Combining equation (20) and (21), the following iterative formulae are found.

$$a_{0,1} = a_{0,-1} = \frac{g_0 - h_0}{2g_0}$$

$$a_{2i,2i-1} = \frac{h_{2i}}{g_{21}} \qquad (23)$$

$$a_{2i,2i-1} = \frac{h_{2i-1} - a_{2i-2,2i-1} g_{2i-2}}{g_{2i}}, i \geq 1$$
$$a_{2i,2i+1} = 1 - a_{2i,2i} - a_{2i,2i-1}, i \geq 1$$

For $\rho = 100\%$ the LSB plane is independent of the remained bit planes. For such stego images we have$a_{2i,2i-1} \cong 0.25$, $a_{2i,2i} \cong 0.5$, $a_{2i,2i+1} \cong 0.25$.

For a natural image there exists weak correlation between the LSB plane and the remained bit planes. As more and more secret messages are embedded, such that correlation becomes weaker and weaker and finally the LSB plane becomes independent of the remained bit planes.

From Equation (20) we know that h_{2i+1} consists of two parts: $a_{2i,2i+1} g_{2i}$ and $a_{2i+2,2i+3} g_{2i+2}$ statistical test shows that these two parts contribute equally for natural images *i.e.*

$$a_{2i,2i+1} g_{2i} \cong a_{2i+2,2i+3} g_{2i+2} \qquad (24)$$

Let us denote $\alpha_i = a_{2i+2,2i+1}/a_{2i,2i+1}$, $\beta_i = a_{2i+2,2i+3}/a_{2i,2i-1}$ and $\gamma_i = g_{2i}/g_{2i+2}$ then the statistical hypothesis of the steganalytic method is that for a natural image the following equation should be satisfied.
$\alpha_i \approx \gamma_i$

while for stego-images with the LSB plane fully embedded

$\alpha_i \approx 1$

The quantity α_i can be viewed as the measure of the weak correlation between the LSB plane and its neighboring bit planes. The relationship between α_i and the embedding ratio ρ will be modeled using a quadratic equation $y = ax^2 + bx + c$. By considering four critical points($P_1 = (0, \gamma_i), P_2 = (p, \alpha_i), P_3 = (1,1), P_4 = (2 - p, \beta_i)$) the following equations have been developed

$$c = \gamma_i;$$
$$ap^2 + bp + c = \alpha_i;$$
$$a + b + c = 1; \qquad (25)$$
$$a(2-p)^2 + b(2-p) + c = \beta_i;$$

Assuming $d_1 = 1 - \gamma_i$; $d_2 = \alpha_i - \gamma_i$; $d_3 = \beta_i - \gamma_i$ then the above equation (8) can be simplified as follows

$$2d_1 p^2 + (d_3 - 4d_1 - d_2)p + 2d_2 = 0 \qquad (26)$$

The embedding ratio ρ can be obtained from the root of the above whose absolute value is smaller if the discriminantis smaller than zero, then $\rho \approx 1$.

Fridrich et al develop the Raw Quick Pair (RQP) [65] for detecting LSB embedding in 24-bit color images, based on analyzing close pairs of colors and the total number of unique colors. Their method cannot be used for gray-scale images and it works reliably for number of unique pairs in the image less than 30%.

Avcibas et al propose a specific steganalytic method for LSB embedding for detection in 7th and 8th bit planes of an image based on correlation between contiguous bit planes as well as the binary texture characteristics within the bit planes which are affected by embedding [66].

Dumitrescu et al [67], inspired by the work of Fridrich et al [62] propose a steganalytic method for an LSB embedding-based on a finite state machine whose states are selected multisets of sample pairs called trace multisets. Their method measures the length of embedded message precisely, even for very short message size.

Ker et al propose a specific steganalytic method for LSB matching for images [68]. Histogram Characteristic Function (HCF), introduced by Harmsen et al for color images is used for gray-scale images [69]. Calibrating center of mass (COM) using a downsampled image and computing adjacency histogram instead of usual histogram were used for applying HCF. It was found that HCF-COM performed quite good for color images, but it turned out to have poor performance for gray-scale images.

The presence of embedded message in BPCS steganography can be revealed by observing the complexity histogram of high significant bit-planes [70]. Yu proposed a specific BPCS steganalytic method that detects hidden message in spatial as well as transform domain [71], based on isotropy, a statistical feature of the image, which is changed due to message embedding. Detection utilizes Chi-square method.

Zhang et al propose a specific steganalytic method for attacking PVD steganography based on observing the histogram of the prediction errors [28,29].

Sullivan et al formulate two steganalytic methods [72] for defeating QIM/DM steganographic method. The first method distinguishes the standard QIM stego-images from the plain-quantized cover images. The second method differentiates the DM stego-image from the unquantized cover images.

The most popular image format is JPEG and it is an ideal target for steganography. Zhang and Ping propose JSteg for attacking on sequentially and random embeddedmessage in JPEG images, based on the statistical model of DCT coefficients [73]. It is found that the quantized DCT coefficients of JPEG images usually distributed uniformly around zero in cover images are changed due to message embedding.

An attack on F5 steganography based on modification of the shape of the histogram of DCT coefficients in JPEG images after embedding message was proposed [34,74]. The steganalytic method is as follow. The stego-image is decompressed to the spatial domain, then cropped by 4 columns, and recompressed using the same quantization parameters as that of the original stego-image. A blurring operation is applied as a preprocessing step to remove possible JPEG blocking artifacts from the cropped image before recompressing. The resulting DCT coefficient provides the estimate of the cover image histogram. Hong and Again present a steganalytic algorithm for breaking steganographic techniques such as F5 based on features extracted from spatial and DCT domains [75]. Support vector machine (SVM) is used to classify the cover images and stego-images.

Fridrich et al propose an attack on OutGuess steganography based on measuring the discontinuity along the boundaries of 8×8 JPEG grid [76]. Measure of the discontinuity gives an spatial feature called blockiness, which is proportional to the number of altered DCT coefficients due to embedding. The change rate of the blockiness is used to estimate the embedding rate.

Stego-image in MB steganography can be differentiated from a cover image by the method proposed by Bohme and Westfeld [77]. Their method is based on more outlier high precision bin in the histogram of the cover image than in a stego-image.

Li et al propose a steganalytic method for an attack on YASS steganography based on the fact that the locations of H-blocks are not randomized enough in YASS [78].

Liu et al propose a neural network based steganalytic method for DFT, DCT and DWT steganography [79]. Neural network is trained using the statistics of cover images and stego-images. Their method gives promising results. Liu et al propose another steganalytic method for detection of wavelet domain steganography [80]. Neural network is able to discriminate between stego-images and cover images based on two parameters namely shape and scale, which are found from wavelet coefficients in each subband of wavelet transform.

3.3 Universal Statistical Steganalysis

Universal statistical steganalysis requires less or even no priori information of the targeted steganographic methods for detection of hidden message. It takes a learning based strategy that involves training based on cover and stego-images regardless of the embedding domains and algorithms. Neural network, clustering algorithms and other soft computing tools are used to construct the detection model from the experimental data.

Avcibas et al propose a steganalytic technique that exploits for detection of hidden message using image quality metrics and multivariate regression analysis [81]. Their method use analysis of variance technique to identify appropriate image quality metrics, which is fed to multivariate regression along with a training set of cover and stego-images.

Farid propose a universal steganalytic technique for gray-scale images based on feature extraction [82]. A Fisher Linear Discriminant analysis is used to discriminate between cover and stego-images based on mean, variance, kurtosis, skew of subband coefficients and error statistics from an optimal linear predictor of coefficient magnitudes, which are calculated using separable quadrature mirror filters (QMF). A better classifier based non-linear support vector machine is proposed [83].

The steganalytic method proposed by Harmsen and Pearlman uses HCF-COM as feature in the detection scheme, and Mahalanobis-distance is used to measure the dissimilarity between the cover and stego-images [69].

Lie and Lin propose a steganalytic method that uses the gradient energy and statistical variance as two features for detection of hidden messages in spatial or DCT domain [84].

Zou et al propose a steganalytic method based on Markov model of threshold prediction error image [85]. The prediction error is obtained by subtracting the prediction values from the pixel values and then threshold with a predefined threshold. SVM with linear and non-linear kernals are used as classifier.

A universal steganalytic method proposed by Shi et al uses statistical moments of characteristic functions of the prediction-error image, the test image, and their wavelet subbands as selected as features [86]. Artificial neural network is utilized as the classifier.

Chen et al propose a steganalytic method based on statistical analysis of empirical matrix (EM), which produces the moments of projection histogram (PH) and moments of characteristic function of projection histogram as features [87]. SVM is used as classifier.

Zhan and Zhang propose a universal steganalytic method based on higher-order wavelet decomposition to capture statistical difference between the cover images and stego-images [88]. Analysis of variances (ANOVA) is applied to wavelet statistics and SVM is used as classifier.

Liu et al propose a universal steganalytic method based on wavelet packet transform (WPT), which gives subband coefficients, which in turn gives multi-order absolute characteristic function moments of histogram as features [89]. A back-propagation (BP) neural network is used as classifier using these features.

Don and Tan propose a steganalytic method based on higher-order statistics of characteristic functions of three types of image run-length histograms as features [90]. SVM is used as classifier.

Mankun et al models LSB matching as a kind of image degradation with certain additive noise proportional to embedding rate and obtain the cover image’s estimation by wavelet denoising [91]. Features of 1-D statistical gray-scale histogram of test image and estimated images are used to train and SVM is used as classifier.

Chen et al propose an image estimation technique utilizing the alpha-trimmed mean for distinguishing cover images and stego-images and the method can estimate hidden messages from images in spatial and JPEG compression domains [92].

Gul and Kurugollu propose “LogSv”, a steganalytic method based on integrating singular values calculated over image sub-blocks resulting a steganalyzer [93].

Cho et al propose a steganalytic method that classify image blocks into multiple classes of steganalytic results of decomposed image blocks [94]. A classifier finds whether a block is a cover image block or a stego-image block.

He et al propose a Radial Basis Function Neural Network (RBFNN) optimized by the Localized Generalization Error Model (L-GEM) for steganography detection, and DCT features and Markov features are used as inputs of neural networks for detection [95].

Ramezani et al compare Fisher linear discriminant, Gaussian naïve Bayes, multilayer perceptron and k nearest neighbor for staganalysis of suspicious images [96]. Statistics of histogram, wavelet statistics, amplitudes of local extrema from 1-D and 2-D adjacency histograms, center of mass of histogram characteristic function and co-occurrence matrices for feature extraction are used in this method.

4. CONCLUSIONS

This paper presents a background discussion on major algorithms of steganography and steganalysis for digital images. Some important algorithms of steganography in spatial domain are discussed in details with special emphasis so that researchers and steganalysts will have knowledge of how to develop such techniques. Steganalytic techniques such as Chi-square, RS, Gradient Energy, Histogram Difference attacks etc for the detection of embedded message bits from stego-images are also explained with equations. Different types of both specific and universal steganalytic techniques in spatial domain as well in transform are described in short in this paper.

5. REFERENCES

[1] F. Petticolas, Information hiding techniques for steganography and digital watermarking, StefenKatzenbeisser, Artech house books, ISBN 158053-035-4, Dec. 1999.

[2] F. Hartung and M. Kutter, Multimedia watermarking techniques, Proceedings of the IEEE, vol. 87, no. 7, July 1999.

[3] S. Voloshynovkiy, S. Pereira, T. Pun, J. Eggers and J. Su, Attacks on digital watermarks: classification, estimation-based attacks and benchmarks, IEEE communications Magazine 39, 9 (August) 2001, pp. 118-126.

[4] A. Sequeira and D. Kundur, Communications and information theory in watermarking: A survey, In proc. of SPIE Multimedia systems and application IV, vol. 4518, pp. 216-227.

[5] J.O. Ruanaidh, H. Peterson, A. Herrigel, S. Pereira and T. Pun, Cryptographic copyright protection for digital images based on watermarking techniques, Elsevier Theoretical Computer Science, vol 226, no. 1, pp. 117-142, 1999.

[6] C. Bergman and J. Davidson, Unitary embedding for data hiding with the SVD, Security, Steganography, and Watermarking of Multimedia Contents VII, SPIE, vol. 5681, San Jose, Jan., 2005.

[7] "Digital millennium copyright act ", http://thomas.loc.gov

.cgi-bin/query/z?c105:H.R.2281.ENR:

[8] N.F. Johnson and S. Jajodia, Exploring steganography,: seeing the unseen, IEEE Computer, vol. 31, no. 2, pp. 26-34, 1998.

[9] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paiz, S. Pogreb, Applications of data hiding, IBM Systems Journal vol. 39, no. 3 & 4, pp. 547-568, 2000.

[10] J. Fridrich and M. Golan and R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia Magazine, Special Issue on Security, pp. 22-28, October-November 2001.

[11] C. Hosmer, Discovering hidden evidence, Journal of Digital Forensic Practice, vol.1, pp. 47-56, 2000.

[12] J.C. Hermandez-Castro, I. Blasco-Lopez, J.M. Estevez-Tapaidor, Steganography in games: A general methodology and its application of the Game of Go, Elsevier Science Computers and Security, pp. 64-71, vol. 25, 2006.

[13] H. Wang and S. Wang, Cyber warfare Steganography vsSteganalysis, ACM Commun. vol. 47, pp. 76-82, October 2004.

[14] A. Nissar and A.H. Mir, Classification of steganalysis techniques: A study, Elsevier Digital Signal Processing, vol. 20, pp. 1758-1770, 2010.

[15] W. Bender, W. Butera, D. Gruhl, R. Hwang, F.J. Paizand and S. Pogreb, Applications for data hiding, IBM Systems Journal, vol. 39, no. ¾, pp. 547-568, 2000.

[16] S. Miaou, C. Hsu, Y. Tsai, and H. Chao, A secure data hiding technique with heterogeous data-combining capability for electronic patient records, Proc. of 22nd IEEE EMBS, pp. 280-283, July 2000.

[17] U.C. Nirinjan, and D. Anand, Watermarking medical images with patient information, Proc. of 20th IEEE International Conference of Biological Society, pp. 703-706, 29 October – 1 November 1998.

[18] Y. Li, C. Li and C. Wei, Protection of mammograms using blind steganography and watermarking, Proc. of IEEE ISIAS, pp. 496-499, 2007.

[19] R. J. Anderson and F.A.P. Pettitcolas, On the limits of steganography, IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, pp. 474-481, 1998.

[20] H. Wang and S. Wang, Cyber warfare: Steganography vsSteganalysis, Communications of ACM, vol. 47, no. 10, pp. 76-82, 2004.

[21] N. Provos and P. Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, vol. 1, no. 3, pp. 32-44, 2003.

[22] B. Lin, J. He, J. Huang and Y.Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 142-172, April 2011.

[23] E. Kawaguchi and R.O. Eason, Principle and applications of BPCS steganography, in Multimedia Systems and Applications, vol. 3528, pp. 464-473, SPIE, 1998.

[24] A.Westfeld and A. Ptzmann, Attacks on steganographic systems-breaking the steganographic Utilities ezstego, jsteg, steganos, and s-tools and some lessons learned, Proc. of 3rd Information Hiding Workshop, vol. 1768, pp. 61-76, Springer,1999.

[25] J. Mielikainen, LSB matching revisted, IEEE Signal Processing Letters, vol. 13, no. 5, pp. 285-287, 2006.

[26] 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.

[27] J. Fridrich, D. Soukal and M. Goljan, Maximum likehood destination 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.

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

[29] Y. H. Yu, C.C. Chang and Y.C. Hu, Hiding secret data in images via predictive coding, Pattern Recognition, vol. 38, no. 5, pp. 691-705, 2005.

[30] 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.

[31] L.M. Marvel, C.G. Boncelet Jr. and C.T. Retter, Spread spectrum steganography, IEEE Trans. Image Processing vol. 8, no. 8, pp. 1075-83, 1999.

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

[33] A. Latham, JPHide, http://linux01.gwdg.de/alatham/steg

o.html

[34] A. Westfeld, F5 – A steganographic algorithm: high capacity despite better staganalysis, Proc. of International Hiding Workshop, vol. 2137, pp. 289-302, Springer 2001.

[35] J. Fridrich, M. Goljan and D. Hogeg, Steganalysis of JPEG images breaking the F5 algorithm,, Proc. Information Hiding, 5th International Workshop, IH 2002, Noordwijkerhout, The Netherlands, Lecture Notes in Computer Science, October 7-9, 2578/2003, pp. 310-323, 2002.

[36] X. Li and J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Science, vol. 177, no. 15, pp. 3099-3191, 2007.

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

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

[39].K.B. Raja , C.R. Chowdary, K.R. Venugopal and L.M. Patnaik, A secure image steganography using LSB DCT and compression techniques on raw images, Proc. IEEE ICISIP05, pp. 170-176, 14-17 December 2005.

[40] McKeon, Strange Fourier steganography in movies, Proc. IEEE ICEIT, pp. 178-182, 17-20 May 2007.

[41] T. Bhattacharya, N. Dey and S.R.B. Chaudhuri, A session based dual steganographic technique using DWT and spread spectrum, International Journal of Modern Engineering Research, vol. 1, no. 1, pp.157-161,

[42] 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.

[43] T. Bhattacharya, N. Dey and S.R.B. Chaudhuri, A session based multiple image hiding technique using DWT and DCT, IJCA, vol.38, no. 5, pp. 18-21, 2012.

[44] K.L. Chung, C-H. Shen, and L-C. Chang, A novel SVD- and VQ based image hiding scheme, Elsevier Pattern Recognition Letters, vol. 22, pp. 1051-1058, 2001.

[45] C. Bergman and J. Davidson, Unitary embedding for data hiding with the SVD, Security, Steganography and Watermarking of Multimedia Contents VII, SPIE, vol. 5681, San Jose CA, January 2005.

[46] M.M. Hadhoud and A.A. Shallan, An efficient SVD image steganographic approach, IEEE ICCES, pp. 257-262, 14-16, December 2009.

[47] K.B. Raja, U.M. Rao, K.A. Rashmi, K.R. Venugopal and U.M. Patnaik, Robust and high capacity image steganography using SVD, IET-UK ICTES, pp. 718-723, 20-22 December 2009.

[48] V.I. Gorodetski, L.J. Popyack, V. Samoilov and V.A. Skormin, SVD-based approach to transparent embedding data into digital images, Lecture Notes in Computer Science, vol. 2052, pp. 263-274, 2001.

[49] Kh. Manglem Singh, L. Shyamsundar Singh, A. Buboo Singh and Kh. Subhabati Devi, Proc. International Conference on Information and Communication technologies pp, pp. 238-241, March 2007.

[50] X. Zhang and S. Wang, Vulnerability of pixel value differencing steganography in histogram analysis and modification for enhanced security, Pattern Recognition Letters, vol. 25, pp. 331-339, 2004.

[51] C.H. Yang, C.Y. Weng, S.J. Wang, H.M. Sun, Adaptive data hiding in edge areas of images with spatial LSB domain system, IEEE Transaction Inf. Forensic Security, vo. 3, no. 3, pp. 488- 497, September 2008.

[52] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. on Information Forensics and Security, vol. 5, no. 2 June 2010.

[53] R. Bohme and A. Westfeld, Breaking Cauchy model-based JPEG steganography with first order statistics, Proc. European Symposium on Research in Computer Security, 13th September 2004, Lecture Notes in Computer Science, vol. 3193, pp. 125-140.

[54] C.C. Chang, P. Tsai and M.H. Lin, An adaptive steganography for index-based image using codeword grouping, Advances in Multimedia Information Processing-PCM, Springer, vol. 3333, pp. 731-738, 2004.

[55] K.B. Raja, S. Sindhu, T.D. Mahalakshmi, S. Akshatha, B.K. Nithin, M. Sarvajith, K.R. Venugopal, I.M. Patnaik, Robust image adaptive steganography using integer wavelets, Proc. on 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE'08, pp. 614-621, 6-8 January 2008.

[56] Y.T. Wu and F.Y. Shih, Genetic algorithm based methodology for breaking the steganalysis systems, IEEE Trans. on Systems, Man, and Cybernetics – Part B, Cybernetics, 36(1), pp. 24-31, 2006.

[57] J. Kong, H. Jia, X. Li, Z. Qi, A novel content-based information hiding scheme, Proc. On International Conference on Computer Engineering and Technology, vol. 1, pp. 436-440, pp. 22-24, January 2009.

[58] R. Rakesh, S. Devathi, P. Sekhar, C. Sekharan, B. Surendra and K. Tatikonda, Message guided adaptive random steganography using counting-out embedding, IJCA, vol. 24, no. 6, June 2011.

[59] P.R.S.S.V. Raju, Y. Vamsidhar and R.C. Sriram, Edge adaptive image steganography on LSB using Godel numbering, IJCST, vol. 2, no. 1, December 2011 (Online).

[60] N.F. Johnson and S. Jajodia, Steganalysis of images created using current steganography software, in Lecture Notes in Computer Science, vol. 1525, Springer-Verlag, pp. 273-289, 1998.

[61] T.A Hawi, M.A. Qutayari and H. Barada, Steganalysis attacks on stego-images using stego signatures and statistical image properties, in Proc. IEEE TENCON, vol. 2, pp. 104-107, 2004.

[62] J. Fridrich and M. Goljan, Practical steganalysis of digital images – state of the art, Security and Watermarking of Multimedia Contents IV, E.J. Delp III and P.W. Wong, editors, Proc. of SPIE, 4675, pp. 1-13, 2002.

[63] l. Zhi, S.A. Fen and Y. Xian, A LSB steganography detection algorithm, Proc. of IEEE Symposium on Personal Indoor and Mobile Radio Communication, vol. 3, pp. 2780-2783, September 2003.

[64]T.Zhang and X.Ping, Reliable detection of LSB steganography based on the difference image histogram, IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 3, pp.545-548 April 2003.

[65] J. Fridrich, R. Du and I. Meng, Steganalysis of LSB encoding in color images, Proc. of IEEE Conference on Multimedia and Expo, July 31- August 2, 2000.

[66] I. Avcibas, N. Memon, and B.Image steganlysis with binary similarity measures, IEEE ICIP, September 2002.

[67] S. Dumitrescu, X. Wu, Z. Wang, Detection of LSB steganography via sample pair analysis, IEEE trans Signal processing, pp. 1995-2007, 2003.

[68] A.D. Ker, Steganalysis of LSB matching in gray-scale images, IEEE Signal Processing Letters, 12(6), pp. 441-444, June 2005.

[69] J.J. Harmsen and W.A. Pearlman, Steganalysis of additive noise modelable information hiding, Proc. SPIE Imaging, Security and Watermarking of Multimedia Content, pp. 131-142, January 2003.

[70] M. Niimi, R.O. Eason, H. Noda and E. kawaguchi, Intensity histogram steganalysis in bpcs steganography, Proc. of IST/SPIE Electronic Imaging: Security and Watermarking of Multimedia Contents, vol. 4314, pp. 555-564, 2001.

[71] X. Yu, T. Tan and Y. Wang, Reliable detection of bpcs steganography in natural images, Proc. of ICIG, 2004.

[72] K.. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran and B.S. Manjunath, Steganalysis of quantization index modulation data hiding, Proc. of IEEE ICIP, pp. 165-168, vol. 2, 2004.

[73] T. Zhang and X. Ping, A fast and effective steganalytic technique against JSteg like algorithms, ACM symposium on Applied Computing, 9-12 March, 2003.

[74] J. Fridrich, M. Goljan and D. Hogea, Steganalysis of JPEG: Breaking the F5 algorithm, Proc. of 5th Information Hiding Workshop, Springer, vol. 2578, pp. 310-323, 2002.

[75] C. Hong and S.S. Agaian, Spatial-frequency feature vector fusion based steganalysis, IEEE international Conference on Man & Cybernetic, vol. 3, no. 8-11, pp. 1866- 1870, 2006.

[76] J. Fridrich, M. Goljan and D. Hogea, Attacking the OutGuess, Proc. of ACM Workshop on Multimedia and Security, ACM Press, pp. 3-6, 2002.

[77] B. Bohme and A. Westfeld, Breaking Cauch model-based JPEG steganography with first order statistics, Proc. of 9th European Symposium on Research in Computer Security, Springer, vol. 3193, pp. 125-140, 2004.

[78] B. li, Y.Q. Shi and J. Huang, Steganalysis in YASS, Proc. of 10th ACM Workshop on Multimedia and Security, ACM Press, pp. 139-148, 2008.

[79] S. Liu, Y. Hongnun and W. Goa, Neural network based steganalysis in still images, Proc. of International Conference on Multimedia and Expo, ICME, vol. 2, pp. 509-512, July 2003.

[80] S. Liu, Y. Hongnun and W. Goa, Steganalysis based on wavelet texture analysis and neural network, Proc. of WCICA, 2004.

[81] I. Avcibas, N. Memon and B. Sankur, Steganalysis using image quality metrics, In Security and Multimedia Contents, SPIE, 2001.

[82] H. Farid, Detecting hidden messages using higher-order statistical models, Proc. of IEEE ICIP, vol. 2, pp. 905-908, September 2002.

[83] S. Lyu and H. Farid, Detecting hidden messages using higher-order statistics and support vector machines, Proc. of 5th International Workshop on Information Hiding, 2002.

[84] W-N. Lie and G-S. Lin, A feature based classification for blind image steganalysis, IEEE Transaction Multimedia, vol. 7, no. 6, pp. 1007- 1020, December 2005.

[85] D. Zou, Y. Q. Shi, W. Su and G. Xuan, Steganalysis based on Markov model of threshold prediction-error image, IEEE ICME, 2006.

[86] Y.Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen and C. Chen, Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction error image and neural network, IEEE ICME, 6-8 July 2005.

[87] X. Chen, Y. Wang, T. Tan and L Gei, Blind image steganalysis based on statistical analysis of empirical matrix, IEEE ICPR, 2006.

[88] S-H. Zhan and H-B. Zhang, Blind steganalysis using wavelet statistics and ANOVA, IEEE Conference on Machine Learning and Cybernetics, vol. 5, pp. 2515-2519, 19-22 August, 2007.

[89] X. Luo, F. Liu, J. Chen and Y. Zhang, Image universal analysis based on wavelet packet transform, 10th IEEE Workshop on Multimedia Signal Processing, pp. 780-784, 2008.

[90] J. Dong and T. Tan, Blind image steganalysis based on run-length histogram analysis, Proc. of 15th IEEE ICIP, pp. 2064-2067, 2008.

[91] X. Mankun, L. Tianyun and P. Xijian, Steganalysis of LSB matching based on histogram features in grayscale image, IEEE ICCT, pp. 669-672, 10-12 November 2008.

[92] M-C. Chen, S.S. Agaian, C.I.P. Chen and B.M. Rodriguez, Alpha-trimmed image estimation for JPEG steganography, Proc. of IEEE International Conference Systems, Man and Cybernetics, pp. 4581-4585, 2009.

[93] G. Gul and F. Kurugollu, A novel universal steganalyzer design, “LogSv”, Proc. on IEEE ICIP, pp. 4249-4252, 2009.

[94] S. Cho, B-H. Cha, J. Wang and C-C. J. Kuo, Block based image steganalysis: Algorithm and performance evaluation, Proc. on IEEE ISCAS, pp. 1679-1682, 2010.

[95] Z-M. He, W.W.Y. Ng, P.P.K. Chan and D.S. Yeung, Steganography detection using localized generalization error model, Proc. on IEEE Systems, Msn and Cybernetics, pp. 15441549, 2010.

[96] m. Ramezani and S. Ghaemmaghami, towards genetic feature selection in image steganalysis, Proc. on 7th IEEE CCNC, pp. 1-4, 2010.