Performance analysis of image steganalysis techniques and future research directives

Sanchita Pathak*, Ratnakirti Roy and Suvamoy Changder

Department of Computer Applications, National Institute of Technology, Durgapur, India
Email: sanchitapathak.nitdgp@gmail.com
Email: rroy.nitdgp@gmail.com
Email: suvamoy.nitdgp@gmail.com
*Corresponding author

Abstract: Steganography is a technique of hiding information imperceptibly inside other medium so that the very fact of communication taking place remains hidden. Recently, the reach of internet has extensively widened through social networking and blogging websites and a high amount of digital media interchange, especially in the form of digital images is being witnessed. This poses a huge threat to security from hackers and terrorists, as this medium can be used for covert communication, thus justifying the need for good steganalysis techniques to detect the existence of hidden messages in digital images. This paper analyses some steganalysis techniques which attack various kinds of spatial domain steganography techniques. Some of them are chi-square attack, triples analysis, sample pair analysis, TPVD steganalysis and analysis of adjacent pixel pair steganalysis. This paper also identifies the current research challenges and discusses possible directions for future research in this field.

Keywords: steganography; steganalysis; spatial domain steganography; chi-square attack; triples analysis; sample pair analysis; SPA; TPVD steganalysis; analysis of adjacent pixel pair steganalysis.


Biographical notes: Sanchita Pathak pursued her Master of Technology degree in Software Engineering from National Institute of Technology, Durgapur. She holds a Bachelor of Technology degree in Computer Science and Engineering from West Bengal University of Technology. Her research interest areas include image steganography, watermarking and steganalysis.

Ratnakirti Roy pursued his doctoral research at National Institute of Technology, Durgapur and holds a PhD, specialising in information security and data hiding systems. He holds a Master’s degree in Computer Applications from University of North Bengal. His areas of research interest include image steganography, digital watermarking, computational photography, cyber-psychology, cryptography among many others. He has several international publications in the area of image steganography and allied topics.
Suvamoy Changder is currently working as an Assistant Professor in the Department of Computer Applications, National Institute of Technology (NIT), Durgapur, India, with an experience of more than 13 years in teaching. He received his MCA in Computer Applications from University of North Bengal, Darjeeling, India, MTech and PhD in Computer Science and Engineering from NIT, Durgapur, India. His research area includes data security, steganography, watermarking, data base management systems and algorithms. He has several international conference and journal publications on the related field of data security and steganography.

1 Introduction

Steganography is a Greek word which is composed of two words, stegos meaning ‘cover’ and graafia meaning ‘writing’, which defines steganography as covered writing. This is an ancient art which was used first by the Romans against the Persians. In ancient times, people were used as the carrier of secret messages by shaving their head and writing the messages on their head. When their hair grew back, the sender sent the person to the concerned receiver without anyone else having any knowledge of the existence of the hidden message. The person’s head was then shaved again at the receiver’s side to get the hidden message. Among other historical uses of steganography, there are messages hidden on hard-boiled eggs by writing on their shells using a vinegar solution, and minute changes in the handwriting of characters or in their spacing (Ziou and Jafari, 2014). During World War II, many invisible inks were used. Messages were written on paper with liquids, for example, juice, which were normally invisible but when paper was heated, the message reappeared. Nowadays, steganography is studied and performed as a branch of information hiding.

If sufficient evidence about the presence of hidden message is obtained it breaks the security of the carrier and the whole purpose of steganography is defeated. The collection of such evidence or proof is the sole purpose of steganalysis. Hence, steganalysis is described as the process of attacking steganography methods for detecting, extracting, destructing and manipulating the hidden data in a stego-object. Generally, steganography algorithms do not show any visual distortions. So, steganalysis has to be performed on the basis of different kinds of anomalies detected in the statistical properties of the images. A steganographic system is considered as broken by an algorithm if the algorithm can decide whether a given image contains a secret message or not. Even if the actual hidden message remains undiscovered, just the proof of its mere presence in the image makes steganalysis successful. Steganalysis finds its use (Nissar and Mir, 2010) in computer forensics, cyber warfare, tracking criminal activities over the internet and gathering evidence for investigations particularly in case of anti-social elements.

The rest of the section gives a brief description of steganography and steganalysis. Section 2 of the paper explains various targeted steganalysis techniques which are then comparatively analysed in Section 3. Finally, Section 4 gives the possible scope and directions of future research in this domain. Lastly, Section 5 presents the concluding remarks of the paper and the associated future work.
1.1 Components of a steganographic system

Although the origin of steganography is found long back, its modern formulation is explained in terms of the \textit{Prisoner’s Problem} proposed by Simmons (1983), where two inmates, Alice and Bob wish to communicate secretly to plan their escape from the prison. Warden Wendy examines all of their communication and is determined to throw them in solitary confinement if she suspects any covert communication (Chandramouli et al., 2003) taking place. The process of inserting the hidden information into another medium is called embedding. The carrier object in which the hidden information is to be embedded into is called a cover-object and the object which is carrying the hidden information is called a stego-object.

Thus hiding information into a medium requires following elements (Provos and Honeyman, 2003):

1. the cover-object (C) in which the secret message will be embedded
2. the secret message (M), which is the information to be hidden into the cover-object
3. the steganographic algorithm (A) which will be used for message embedding and extraction
4. a secret-key (K) may be used to hide and unhide the message
5. the stego-object (S) which will contain the embedded secret message

In a steganographic system, the input to A is C, M and K and the output is S at the site of the message sender and the input to A is K and output is M at the site of the receiver of the secret message as shown in Figure 1. Whenever Alice wants to send a secret message to Bob, she does so by embedding the message M into cover object C using a steganographic algorithm A and a secret key K which is known by only Alice and Bob. The stego object S thus formed is then sent to Bob after being checked by the warden Wendy. Wendy uses steganalysis techniques for distinguishing between a cover-image and a stego-image. She remains unaware of the secret communication is taking place if she is unable to differentiate between the stego-object S and the cover-object C. Bob then uses the key K and the same algorithm A to extract the secret message M.

\textbf{Figure 1} A steganographic system
1.2 Digital image steganography

All digital file formats like text, images, audios, videos or protocol can be used for steganography, but the formats with high degree of redundancy are the most suitable ones. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display (Currie and Irvine, 1996). Images are most suitable for being cover objects for steganography as large amount of redundant bits are present in the digital representation of an image and they are too commonly used for conveying information over the internet. It is generally considered that greyscale images are more suitable than colour images for hiding data (Fridrich et al., 2001) because the disturbance of correlations between colour components may easily reveal the trace of embedding. Greyscale images use eight bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. Digital images with a high amount of visual complexity serves as a better cover image as slight changes in them introduced due to embedding becomes visually unnoticeable.

Image steganography techniques can be classified into two broad categories – spatial or image domain techniques and transform or frequency domain techniques. Steganography in the spatial domain involves embedding a message directly into the intensity of the pixels, while that in the transform domain involves first transforming the image and then embedding the message into it. Embedding in the least significant bit (LSB) plane of an image is the most widely used spatial domain steganography technique. This technique makes use of the fact that the LSBs in an image could be thought of as random noise and changes to them would not have any effect on the appearance of the image. Although the image seems unchanged visually after the LSBs are modified, there is a change in the statistical properties of the image. The embedding rate is measured in bits per pixel (bpp).

Spatial Domain steganography is one of the conventional techniques capable of hiding large secret message in a cover image without introducing many perceptible distortions (Bender et al., 1996). Its implementation is also very simple. It works by replacing the LSBs of randomly selected pixels in the cover image with the secret message bits. The selection of pixels may be determined by a secret key. Many steganographic tools using this technique, such as Steghide, S-tools and Steganos are available on the internet. There are predominantly two types of steganography in the spatial domain. They are LSB replacement and LSB matching. In LSB replacement, the LSB bit plane is replaced with the secret message data represented in binary form, i.e., the LSB are simply flipped if it is not same as the message bits. Whereas, in LSB matching (Li et al., 2009; Mielikainen, 2006; Sharp, 2001), instead of replacing the LSBs of the cover image pixels, LSB matching adds or subtracts them by 1 if they do not match the message bits, in other words, the pixel value is increased or decreased so as to match the bit of the message that is to be hidden. Embedding rate is 1 bpp for both the types of steganography. LSB replacement technique introduces some anomalies in the histogram of the image, this makes it detectable. LSB matching technique is more difficult to detect. Another type of spatial domain steganography is prediction error-based steganography (Wu and Tsai, 2003). In order to maintain image visual quality, secret data should be hidden in complex areas of the image. To evaluate the local complexity, the pixel prediction error can be used. The larger the prediction error, the more obvious is the local fluctuation. Data can be hidden into the prediction errors. The neighbouring pixel of the
current pixel can be used to predict its value and thus their difference can be considered as a kind of prediction error.

Embedding in the transform domain category mainly makes use of the redundancies in the discrete cosine transform (DCT) domain, which is used in JPEG compression. Embedding in DCT domain is simply done by altering the DCT coefficients, for example by changing the LSB of each coefficient. Although changing the DCT coefficients will cause unnoticeable visual artifacts, they do cause detectable statistical changes. Some transform domain algorithms also use discrete Fourier transform (DFT) and discrete wavelet transform (DWT). Some popular frequency domain steganographic algorithms are JSteg, JPHide, F5, OutGuess and so on. JSteg and JPHide are two classical frequency domain tools that utilise the technique of LSB embedding. JSteg embeds secret message bits into a cover image by replacing the LSBs of non-zero quantised DCT coefficients with them. JPHide uses the same technique but the DCT coefficients are selected randomly. F5 works by decreasing the absolute value of DCT coefficients by 1 if needed to be modified. OutGuess embeds secret message bits along a random walk into the LSBs of the quantised DCT coefficients while skipping 0’s and 1’s. After embedding, corrections are made to the coefficients that are unmodified to make the global DCT histogram of the stego image match that of the cover image.

1.3 Classification of steganalysis techniques

Steganalysis can be broadly classified into two classes: \textit{signature steganalysis} and \textit{statistical steganalysis}. The division is based on whether the signature of the steganography technique or the statistics of image is used to identify the presence of concealed messages in images embedded using steganography. Based on its area of application, it can be further divided into specific methods and universal methods. \textit{Specific or targeted techniques} are those which target a particular steganographic algorithm. \textit{Blind or universal techniques} are those which are independent of the steganographic algorithm used. Both approaches have their own advantages and disadvantages. A steganalysis technique specific to an embedding method would give very good results when tested only on that embedding method, and might fail on all other steganographic algorithms.

On the other hand, a steganalysis method which is independent of the embedding algorithm might perform less accurately overall but still provide acceptable results on new embedding algorithms. The functionality of targeted steganalysis techniques may be limited by the image format. By studying and analysing the embedding algorithm, the statistical changes that might occur can be found out based on which it may be shown whether an image contains any secret information or not. As these methods concentrate on specific steganographic algorithms, they give highly accurate results but they may not be extended to attack steganographic algorithms other than the ones they target. A blind steganalysis technique is designed to work on all types of embedding techniques and image formats. A blind algorithm is trained to find out the difference in the statistical properties of pure and stego image. The machine running the blind algorithm is trained on a large image database. Blind techniques are usually less accurate than targeted ones, but can be applied on a large-scale basis to break various algorithms. The main focus of this paper is to study and analyse various specific (targeted) steganalysis techniques in spatial domain.
1.4 Different approaches to steganalysis

A steganalyser can attempt an attack using a suitable approach among the following:

1. **Visual attacks**: this attack is done by analysing the images visually, like considering the bit images and trying to find the difference visually in those single bit images.

2. **Structural attacks**: the format of data file often changes as the data to be hidden is embedded, identifying these characteristic structural changes can detect the existence of image, for example, in palette-based steganography the palette of image is changed before embedding data to reduce the number of colours so that the adjacent pixel colour difference should be very less. This shows that groups of pixels in a palette have the same colour which is not the case in normal images.

3. **Statistical attacks**: in these types of attacks the statistical analysis of the images by some mathematical formulas is done and the detection of hidden data is done based on these statistical results. Generally, the hidden message is more random than the original data of the image thus finding the formulae to know the randomness reveals the existence of data.

1.5 Types of steganalysis attacks

Steganalysers can perform attacks in several ways, for example, they may just detect the presence of hidden data or may detect and extract the hidden data, some may just try to destroy the hidden data after finding their existence or some may even try to replace the hidden data with other data by finding the exact location where and how the data had been hidden originally. This gives way to the categorisation of attackers as Active attacker and Passive attacker. An active steganalyser only detects the presence of hidden message without causing any harm to it. A passive steganalyser attempts to destroy the hidden message (Anderson and Petitcolas, 1998) or manipulates it.

Steganalysis attacks are classified into six main categories (Johnson and Jajodia, 1998) based on information available to the attacker. They are:

1. **Stego-only attack**: only the stego-image is available for analysis.

2. **Known cover attack**: the original cover-image and stego-image are both available.

3. **Known message attack**: at some point, the hidden message becomes known to the attacker. Analysing the stego-image for patterns that correspond to the hidden message may be beneficial for future attacks against that system. Even with the message, this may be very difficult and may even be considered equivalent to the stego-only attack.

4. **Chosen stego attack**: the steganography tool (algorithm) and stego-image are known.

5. **Chosen message attack**: the steganalyser generates a stego-image from some steganography tool or algorithm from a chosen message. This goal in this attack is to determine corresponding patterns in the stego-image that may point to the use of specific steganography tool or algorithms.

6. **Known stego attack**: the steganography algorithm is known and both the original and stego-image are available.
1.6 Goals of any image steganalysis technique

From the user’s point of view, steganalysis must meet the following requirements (Ziou and Jafari, 2014):

1. detection of the presence or confirmation of the absence of a hidden message in a given image
2. identification of the steganographic technique used to embed the message
3. estimation of features of the hidden message, such as length and location
4. extraction of the hidden message
5. anticipation of new and unknown steganographic techniques.

From the designer’s point of view, fulfilling such requirements implies that a steganalysis method can be characterised by its accuracy, universality, and expressiveness. Accuracy means detection, identification, and estimation with minimum error even in the case of a short message length. Universality relates to the ability of detecting a hidden message for a large set of steganography techniques and image types. Expressiveness is the ability of a steganalysis method to explain the embedding. It is an extremely challenging task to make a steganalysis technique which perfectly detects secret messages of any length, hidden using any embedding algorithm in any type of cover image. So, an algorithm which fairly detects the presence of hidden messages inside images with a high amount of accuracy can be considered to be reliable.

2 Related research on specific steganalysis techniques

2.1 Chi-square attack

It is one of the earliest known steganalysis methods, which was proposed by Westfeld and Pfitzmann (1999). This approach is specific to the steganographic technique in which the LSBs of the pixels are flipped according to the bits of the hidden message. The technique shows that due to the use of LSB replacement algorithm, statistical characteristics known as pairs of values (POVs) are formed in the histogram of the image under analysis. After embedding, the total number of occurrence of two members of certain POV remains same. Figure 2 shows the mappings between pixels of an 8-bit greyscale image with 256 grey values after undergoing LSB replacement technique. C represents the cover image and S represents the stego-image; in other words, the cover image after embedding secret data into it. For $0 \leq k \leq 127$ in an 8-bit greyscale image, a pixel of value $2k$ in C, after embedding may either remain $2k$ in S or change to $2k + 1$. Similarly, a pixel whose value is $2k + 1$ in C, after embedding may either remain $2k + 1$ in S or change its value to $2k$. Thus, in general, these even-odd pixel pairs form the set $\{2k, 2k + 1 | 05 \leq k \leq 127\}$ and is called PoVs.
Figure 2  Mappings between grey values

\[
C \rightarrow S \\
0 \rightarrow 0 \\
1 \rightarrow 1 \\
2 \rightarrow 2 \\
3 \rightarrow 3 \\
\vdots \\
254 \rightarrow 254 \\
255 \rightarrow 255
\]

This concept of pair wise dependencies is exploited to design a statistical Chi-square test to detect the hidden messages (Westfeld and Pfitzmann, 1999; Fridrich and Goljan, 2002). Westfeld and Pfitzmann (1999) say that it is uncommon for the frequency of pixel value \(2k\) to be nearly equal to pixel value \(2k + 1\) in an image that has not been embedded with information. Thus, the chi-squared attack was designed to detect these nearly equal PoVs in images to find out the probability of embedding using first order statistics. The test proceeds as follows:

For an 8-bit greyscale test image, the frequencies of each grey value are classified into following two sets

\[
\begin{align*}
x(k) &= \text{frequency}(2k), \\
y(k) &= \text{frequency}(2k + 1), \quad \text{for } 0 \leq k \leq 127
\end{align*}
\]

And, the theoretically expected frequency of grey values \(2k\) and \(2k + 1\) is

\[
z(k) = (x(k) + y(k))/2.
\]

Now, the chi-squared statistic with \(n - 1\) degree of freedom is then calculated as:

\[
\chi^2_{n-1} = \sum_{i=0}^{127} \frac{(x_i - z_i)^2}{z_i}, \quad \text{where } z_i = \frac{x_i + y_i}{2}
\]

The probability density function \(F(u)\) for the image is given as follows:

\[
F(u) = \frac{1}{2^{n-1} \Gamma\left(\frac{n-1}{2}\right)} e^{-\frac{u^{2n-2}}{4}}
\]

Now, the probability of embedding \(p\) is calculated by integrating the density function with the chi-squared statistic value as its upper limit as follows:

\[
p = 1 - \int_0^{\chi^2_{n-1}} F(u) \, du
\]

or

\[
p = 1 - \frac{1}{2^{n-1} \Gamma\left(\frac{n-1}{2}\right)} \int_0^{\chi^2_{n-1}} e^{-\frac{u^{2n-2}}{4}} \, du
\]

This \(p\) gives the probability of embedding in the test image. The reported results show that this method reliably detects sequentially embedded messages.
2.2 RS steganalysis

A more sophisticated technique RS steganalysis (regular and singular group) is presented by Fridrich et al. (2001) for detection of LSB embedding in colour as well as greyscale images. This technique utilises sensitive dual statistics derived from spatial correlations in images. The image is divided into disjoint groups of fixed shape. Within each group noise is measured by the mean absolute value of the differences between adjacent pixels. Each group is classified as regular or singular, depending on whether the pixel noise within the group is increased or decreased after flipping the LSBs of a fixed set of pixels within each group using a mask. The classification is repeated for a dual type of flipping. Theoretical analysis and experimentation show that the proportion of regular and singular groups, form quadratic curves, which are used for determining the amount of message, embedded using the LSB method. According to this method, a discrimination function $f$ and a flipping operation $F$ is used to define three types of pixel groups for the image, namely $R$, $S$ and $U$ as follows:

- Regular groups: $G \in R \iff f(F(G)) > f(G)$  
- Singular groups: $G \in S \iff f(F(G)) < f(G)$  
- Unusable groups: $G \in U \iff f(F(G)) = f(G)$

where $G$ denotes the different disjoint groups of pixels.

Then the LSB flipping embedding is done using the flipping operation $F$.

The number of regular groups for mask $M$ is denoted as $RM$ (percent of all groups). Similarly, $SM$ denotes the relative number of singular groups. According to Fridrich et al. (2001), $RM + SM \leq 1$ and $R_{-M} + S_{-M} \leq 1$, holds for the negative mask. The statistical hypothesis of this method is that in a typical image, the expected value of $RM$ equals that of $R_{-M}$, and the same is true for $SM$ and $S_{-M}$ or

$$RM \approx R_{-M} \quad \text{and} \quad SM \approx S_{-M}$$

Now an RS-diagram is drawn for the groups $RM$, $R_{-M}$, $SM$, $S_{-M}$. Figure 3 shows the RS diagram as depicted by Fridrich et al. (2001) in their paper.

**Figure 3** RS-diagram of an image taken by a digital camera

Note: The x-axis is the percentage of pixels with flipped LSBs, the y-axis is the relative number of regular and singular groups with masks $M$ and $-M$, $M = [0 \ 1 \ 1 \ 0]$. 
These four curves are estimated and their intersection is calculated using extrapolation. The curves are seen to change from perfectly linear to curve.

The root $x$ is found out from the quadratic equations of the curves obtained, and is substituted in the following formula

$$p = x/(x-1/2),$$

where $p$ is the embedded message length.

### 2.3 Sample pair analysis method

Sample pair analysis (SPA) method was given by Dumitrescu et al. (2003) inspired by the work of Fridrich et al. (2001) and is a generalised case of methods given in (Dumitrescu et al., 2002; Dumitrescu and Wu, 2002). This technique detects the existence of hidden messages that are randomly embedded in the LSB of natural continuous-tone images. Here it has been investigated that the statistics of sample pairs of signal is highly sensitive to LSB embedding. The technique is based on a finite state machine whose states are selected multisets of sample pairs called trace multisets. The behaviour of trace multisets under LSB embedding operation is modelled by a finite state machine. The structure of this finite state machine is used to establish quadratic equations that estimate the length of embedded messages in terms of cardinalities of trace multisets. The technique precisely measures the length of embedded message, even when the hidden message is very short relative to the size of image.

The cover image is partitioned into horizontally adjacent pixel pairs and $P$ is the set of all pixel pairs. The sets $X$ and $Y$ of $P$ are defined as:

1. $X$ is a set of pairs $(u, v) \in P$ such that $v$ is even and $u < v$ or $v$ is odd and $u > v$.
2. $Y$ is a set of pairs $(u, v) \in P$ such that $v$ is even and $u > v$ or $v$ is odd and $u > v$.

Statistically, $|X| = |Y|$ for natural images. $Z$ is a subset of pairs $(u, v) \in P$ such that $u = v$.

$Y$ is further divided into two subsets $W$ and $V$ such that $W$ is a set of pairs in $P$ of the form $(2k, 2k + 1)$ or $(2k + 1, 2k)$ and $V = Y - W$. Then, $P = X \cup W \cup V \cup Z$, where $X$, $W$, $V$, $Z$ are called primary sets.

Now message is embedded into the LSBs of the pixel values. Given a pixel pair, there are four situations:

1. 00 – both $u$ and $v$ remain unmodified.
2. 10 – only $u$ is modified.
3. 01 – only $v$ is modified.
4. 11 – both $u$ and $v$ are modified.

The possible state transition diagram for the sets of the image after embedding is shown in Figure 4.
Figure 4  State transition diagram for sets $X$, $V$, $W$, $Z$ due to LSB flipping

![State transition diagram](image)

Figure 5  The 8 trace subsets of the set $C_{m,n}$

![Trace subsets diagram](image)

For each modification pattern $\pi \in \{00, 10, 01, 11\}$ and each primary set $A \in \{X, V, W, Z\}$, $f(\pi, A) = f(\pi, P)$, then,

1. $f(00, P) = (1 - p/2)^2$
2. $f(10, P) = f(01, P) = p/2(1 - p/2)$
3. $f(11, P) = (p/2)^2$.

Here, $p$ is the embedded message in bits divided by the total number of pixels. The fraction of the pixels modifies by the LSB embedding is $p/2$. $X'$, $V'$, $W'$, $Z'$ are the sets $X$, $V$, $W$ and $Z$ after embedding. The following equations are thus obtained:

- $|X'| = |X|(1 - p/2) + |V'| p/2$
- $|V'| = |V|(1 - p/2) + |X| p/2$
\[ |W| = |W|(1 - p + p^2/2) + |Z| p(1 - 1/2) \]

Solving the equations the value of \( p \) is obtained, which gives the embedded message length.

### 2.4 Triples analysis

Ker (2005) proposed a steganalysis method for spatial domain embedding, placing the older method (Dumitrescu et al., 2003) into a common context and providing new and more powerful detectors. This technique is a generalisation of the sample-pairs method to include three tuples of pixels and detects the presence of hidden message, hence estimating its length. It is also observed in Ker (2005) that triples analysis maintains superior performance when the cover images are JPEGs which have been reduced in size. For generalising, \( g \) -tuples of sample values are considered, for arbitrary \( g \). The steps that follow are determining the probabilities of transition between trace subsets, hypothesising a value for \( p \), inverting the formula to express the cardinalities of the cover image trace subsets in terms of those of the stego-image, using a model for cover images and solving for \( p \) optimally. Triples analysis is the analysis involving case of \( g = 3 \) which makes the number of sub multisets \( 2^3 \), i.e., 8. Figure 5 shows the 8 trace subsets of the set \( C_{m,n} \) as in Ker (2005). Subsets connected by an edge are related by the flipping of the LSB of exactly one sample in the 3-tuple. Experimental results show that this method is a highly sensitive detector.

### 2.5 Pixel value differencing attack

The pixel value differencing (PVD) method was originally proposed to hide secret messages into 256 grey-valued images (Wu and Tsai, 2003). It can embed larger amount of data without much degradation in the image quality and thus are hardly noticeable by human eyes. It is based on the fact that human eyes can easily observe small changes in the grey values of smooth areas in the image but they cannot observe relatively larger changes at the edges areas. PVD uses the difference of each pair of pixels to determine the number of message bits that can be embedded into that pixel pair. Pixels around an edge area will have larger differences whereas pixels at a smooth area will have smaller differences. The larger the difference, the more the bits that can be embedded into that pixel pair.

The PVD method is not very sensitive to straightforward histogram analysis as compared to LSB. However, by drawing the histogram for the differences of pixel pairs, variations before and after embedding can be clearly observed. In Zhang and Wang (2004), the authors presented an analysis of the changes in the histogram of the pixel difference due to embedding secret data in a cover image using PVD. Sabeti et al. (2007) utilised chi-square steganalysis to identify the existence of data embedded by PVD or by its enhanced version PVD+LSB (Wu et al., 2005; Yang et al., 2007). They generate a substitute image which is created from the pixel-pair difference vector of the stego-image. Then, they applied chi-square steganalysis on the substitute image to detect the presence of embedded data.
2.6 Analysis of adjacent pixel pairs

A method of steganalysis based on analysis of adjacent pixel pairs was proposed by Shreelekshmi et al. (2011). This technique is based on the fact that the neighbouring pixels of a pixel in an image mostly have same colour values, which change with embedding. But embedding does not change pixel values arbitrarily. These transitions in the adjacent pixel pairs are analysed in this technique. \( P \) is the set of vertically or horizontally adjacent pixel pairs of the test image. Figure 6 shows the transition in \( P \) due to embedding in an 8-bit greyscale image.

Based on the transitions due to embedding the technique (Shreelekshmi et al., 2011) partitions \( P \) into \( C_0, C_1, C_2, C_3, \ldots, C_{2^m-1} \). Each \( C_m \geq 1 \) is further partitioned to \( X_{2m-1}, Y_{2m} \) and \( Y_{2m+1} \) and \( C_0 \) to \( D_0 \) and \( Y_1 \). The transitions due to embedding are confined between blocks of each \( C_m \) and cardinalities of these blocks change with embedding. Generally,

\[
|X_{2m-1}| \geq |X_{2m}| = |Y_{2m}| \geq |Y_{2m-1}|
\]

**Figure 6** Transition in \( P \) due to embedding

Hence, due to embedding, \( |X_{2m-1}| \) decreases and \( |Y_{2m+1}| \) increases. \( |X_{2m}| \) and \( |Y_{2m}| \) increase/decrease depending on their initial value. At 100% embedding, all these cardinalities become equal. The decrease/increase in \( |X_{2m-1}| \) \( / \) \( |Y_{2m+1}| \) are quadratic when difference between \( |X_{2m-1}| \) \( / \) \( |Y_{2m+1}| \) is large. The decrease/increase in \( |X_{2m}| \) and \( |Y_{2m}| \) is linear.

When \( |C_m| \) is small, \( |X_{2m-1}| \approx |X'_{2m-1}| \), it is known that \( |Y_{2m+1}| \approx |X_{2m-1}| \). Thus, we have, \( |Y_{2m+1}| \approx |X'_{2m-1}| \). Since \( |C_{m-1}| \) is an invariant with embedding,

\[
|X_{2m-3}| \approx (|X'_{2m-3}| + |X'_{2m-2}| + |Y'_{2m-2}| + |Y'_{2m-1}|) - (|X'_{2m-2}| + |Y'_{2m-2}| + |Y_{2m-1}|)
\]

\[
|Y_{2m-3}| \approx |X_{2m-3}| - (|X'| + |X'_2| + |Y'_2| + |Y'_3|) - (|X'_2| + |Y'_2| + |Y_1|)
\]

\[
|Y_1| \approx |X_1|
\]

\[
|D_0| \approx (|D_0| + |Y_1|) - |Y_1|
\]
We know $|D_0| \approx |D_0| (1 - p(1 - p/2)) + 2n(p(1 - p/2))$.

The above quadratic equation is then solved to get $p$, the amount of hidden message. Throughout this paper, the name AAPP attack is used to refer to this method.

### 2.7 Tri-way pixel value differencing steganalysis

Zaker and Hamzeh proposed a steganalysis method for attacking tri-way pixel value differencing (TPVD) steganography, based on differences of pixel difference histogram (Zaker and Hamzeh, 2011). The TPVD steganography (Chang et al., 2008) is a modified version of PVD steganography which aims to increase the capacity of PVD by embedding secret bits in different edge directions of an image whereas the original PVD technique embeds data into the edge areas of the image that are only in one direction. TPVD embeds data in horizontal, vertical and diagonal edges of the image simultaneously, along with preserving the image qualities. Since TPVD also embeds secret bits in difference values between two adjacent pixel pairs, probabilistic distribution of difference values which have been altered due to embedding can be considered as valuable statistical information for attacking TPVD.

The TPVD steganalysis method introduced a new steganalytic measure named Growing Anomalies whose value has a linear relationship with the secret message rate. For this, firstly, the extraction of the difference values of a test image suspected to be altered during TPVD embedding. Secondly, those values are compared with the histogram values of that image after embedding additional secret bits into it using TPVD embedding. The first step of TPVD steganalysis is called the preprocessing step. In this step, the image is divided into blocks of size 2 × 2. Branch conditions are checked to find whether to perform TPVD or PVD on that block. The difference of pixel values are calculated for each block and stored in the vector $D$. Figure 7 (Zaker and Hamzeh, 2011) shows the block diagram of the preprocessing phase.

---

Figure 7  Block diagram of preprocessing phase

---

The second step is the analysing phase. In this step the difference of adjacent bars in the histogram of the $D$ vector is calculated by the formula:

$$DD(i) = \Delta H(i) = H_D(i) - H_D(i-1); \quad (-255 < i \leq 255)$$
Then, an additional amount of secret data is embedded in $\theta\%$ of difference values and its $DD'$ value is calculated similarly as $DD$:

$$DD'(i) = \Delta H'(i) = H'_D(i) - H'_D(i-1)$$

It is shown in (Zaker and Hamzeh, 2011) that as the embedding rate $\theta$ increases, these $DD'(i)$ values decreases till they get zero for 100% embedding. On the other hand, $DD'(i)$ values which are at the boundary of ranges, increases as the embedding rate increases. Growing anomalies are the sum of elongated bars in $DD$ diagram, i.e., the sum of differences at the beginning of each range whose index is $k$. It can be calculated as:

$$Growing\ anomalies = \sum_{k=1}^{K} DD(u_k)$$

where $K$ = number of ranges. Growing anomalies for the test image Lena (Figure 8) is shown in Figure 9.

**Figure 8** Lena (512 × 512)

**Figure 9** Growing anomalies for test image Lena as more secret message is embedded into it (see online version for colours)

Growing anomalies saturates to a constant value after embedding in all possible pixel difference values. Hence, more amount of embedding will not cause any change in its value. This property is utilised in this steganalysis technique to find out the initial secret message rate (SMR) which is calculated as:

$$SMR = \frac{Growing\ anomalies\ of\ test\ image\ (P(0))}{Growing\ anomalies\ after\ embedding\ 100\%\ additional\ secret\ message\ into\ the\ test\ image\ (P(1))}$$
The value of SMR identifies whether the test image is cover image or stego image. Figure 10 shows the block diagram of TPVD steganalysis.

**Figure 10** Block diagram of TPVD steganalysis

2.8 **Boundary pixel steganography attack**

Chiew and Pieprzyk (2010) proposed a steganalytic method to detect messages hidden in a black and white (binary) image using boundary pixels steganography (Liang et al., 2007). This method is referred as BPS attack in this paper. It derives the 512 pattern histograms from the boundary pixels as the distinguishing statistic; the histogram difference is then computed to determine the changes in them due to embedding. Lastly, a histogram quotient is proposed to estimate the length of the embedded message. Boundary pixel steganography hides the secret information along the edge areas in the binary image where the white pixels meet the black ones. These pixels are called boundary pixels.

Boundary pixels are defined (Liang et al., 2007) as the pixels having at least one neighbouring pixel with different intensity. For example, a white (black) pixel will be called as boundary pixel if it has at least one among its four neighbouring pixel black (white), as black and white are the only possible colours in a binary image. But every boundary pixel is not eligible for embedding, rather, if the currently evaluated boundary pixel satisfies the following two conditions then only it is considered eligible for embedding:

\[ \text{a} \quad \text{out of the four neighbouring pixels, at least two unmarked (unevaluated) neighbouring pixels are present having two different pixel values} \]

\[ \text{b} \quad \text{if any marked (evaluated) neighbouring pixel is present, its four neighbouring pixels must also satisfy the first criterion.} \]

After finding out the pixels eligible for embedding, the message is embedded to the pixels. Whenever the message bit does not match the value of the pixel, it is simply overwritten by the message bit, otherwise it is left unaltered. After embedding, visual distortions are minimal and the image does not show any salt and pepper noise. But a closer look at the image reveals small pixel-wide notches and protrusions nearby the boundary pixels. In Chiew and Pieprzyk (2010), it is shown that for a pixel, a certain pixel pattern can be formed together with its eight neighbouring pixels. The 512 pattern histogram \( H(J) \) gives the frequency of occurrence of each pattern in the given test image \( J \).

\[ H = \{ h_i | 1 \leq i \leq 512 \}. \]
The frequency of occurrence \( h_i \) for the \( i^{th} \) pattern is given by

\[
h_i = \sum_{k=1}^{M} \delta(i, p(k))
\]

where \( p(k) \) denotes the \( k^{th} \) pattern in the given image, \( M \) is the total number of patterns in the given image and \( \delta \) is the Dirac delta function (i.e., \( \delta(u, v) = 1 \) if \( u = v \) and 0 otherwise). Now, due to embedding, the inter pixel correlation gets disturbed and thus reflects in pattern changes and the histogram flattens, in other words, some of its local maxima may decrease and local minima may increase. The histogram difference is then calculated to capture the flatness of the 512 pattern histograms. The histogram difference is the bin-wise absolute difference between the 512 pattern histograms for two images, one being the given test image and the other the same image but 100% re-embedded with random secret data with the same embedding algorithm.

The histogram \( H' = \{h'_i | 1 \leq i \leq 512\} \) represents the second image histogram, where \( h'_i \) is the corresponding frequency of occurrence for the \( i^{th} \) pattern in the same image that has been 100% re-embedded with random message. The histogram difference is calculated as

\[
HD = \{ |h_i - h'_i| | 1 \leq i \leq 512 \}
\]

The histogram quotient \( hq \) is calculated by performing matrix right division on \( HD \) by \( H \), i.e.,

\[
hq = HD/H
\]

Using linear interpolation, the constant of proportionality \( c \) is obtained such that \( hq \approx c \times l \), where \( l \) is the message length which is then calculated from \( l = hq/c \).

3 Comparative analysis

This section provides a comparative analysis of the techniques explained in Section 2 on the basis of some parameters. These parameters are explained in the first part of this section, following which two tables are provided which give a brief overview of the performance and characteristics of the various steganalysis methods. The last part of this section gives the analysis of the steganalysis methods based on the tabular data presented.

3.1 Parameters for comparison

The parameters used for the comparative analysis of various steganalysis methods are as follows:

1. **Steganographic algorithm**: this parameter explains which specific steganographic algorithm the steganalysis method under consideration is capable of successfully attacking.

2. **Type of steganalysis attack**: this parameter defines the type of steganalysis attack that is followed by the steganalysis method under consideration. It can be any one...
among the ones described in Section 1.5, i.e., stego only attack, known cover attack, known message attack, chosen stego attack, chosen message attack or known stego attack. A successful steganalysis method which is stego-only attack type can be called strongest among all the other attack types and it can be called weakest if it is known stego attack type.

3 Cover image type: this parameter describes which type of cover image is suitable for successfully attacking using the steganalysis method under consideration. The image can be a greyscale image or colour image. The image compression can be either lossy compression type or lossless compression type. A steganalysis method which successfully attacks both colour and greyscale images is better.

4 Amount/rate of embedding: this parameter explains the amount or rate of pixels that should be embedded with secret data in order that the steganalysis method accurately detects its presence in the stego-image.

5 Maximum estimation error: this parameter gives the maximum percentage of error obtained when the steganalysis technique is applied on a set of test images. The lower the value of this parameter, the better is the algorithm.

6 Detection accuracy: this parameter categorises the accuracy of secret message detection of the steganalysis techniques based on their performance on a huge database of images. The values of this parameter relates to the maximum estimation error parameter. The possible values of this parameter are HIGH, MEDIUM and LOW. For a particular algorithm this value is relative to other steganalysis algorithms to which this algorithm is compared. HIGH represents minimum error rate in detection of secret message, thus making the method most reliable among others. The method marked LOW has maximum error rate of detection, thus, is the least reliable method as compared to the rest. MEDIUM value, as the name suggests, lies between HIGH and LOW.

7 Information obtained: this parameter explains what type of information is obtained after applying the steganalysis method to the stego-image. A steganalysis method can detect information like the probability of embedding, the length of message embedded, the embedding rate or whether the image is a stego-image or not.

8 Statistical changes detected: this parameter explains what type of statistical changes are detected, by the steganalysis method, in the properties of the image. The changes that are detected are brought about in the image as a result of a steganographic algorithm applied to it.

9 Case of failure: this parameter defines the case for the failure (if any) of the steganalysis method. It is the condition for which the method does not work correctly as required.

Table 1 compares the methods of Section 2 on the basis of the first five parameters explained in this section, namely the steganographic algorithm, type of steganalysis attack, cover image type, amount/rate of embedding and detection accuracy. Table 2 lists out the statistical changes detected in the test image as a result of embedding which helps in steganalysis of the method, the information obtained from the test image after applying the steganalysis algorithm to it and the cases when the steganalysis methods fail to perform as desired.
## Table 1  
Comparison table for various steganalysis algorithms

<table>
<thead>
<tr>
<th>Steganalysis algorithm</th>
<th>Steganographic algorithm</th>
<th>Type of steganalysis attack</th>
<th>Cover image type</th>
<th>Amount/rate of embedding</th>
<th>Maximum estimation error</th>
<th>Detection accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chi-square attack</td>
<td>LSB replacement steganography</td>
<td>Chosen stego</td>
<td>Colour/greyscale</td>
<td>High*</td>
<td>12.9%</td>
<td>LOW</td>
</tr>
<tr>
<td>RS steganalysis</td>
<td>LSB replacement steganography</td>
<td>Chosen stego</td>
<td>Colour/greyscale</td>
<td>&gt;0.005 bpp</td>
<td>11.38%</td>
<td>LOW</td>
</tr>
<tr>
<td>SPA method</td>
<td>LSB replacement steganography</td>
<td>Known stego</td>
<td>Colour</td>
<td>Any</td>
<td>8.6%</td>
<td>MEDIUM***</td>
</tr>
<tr>
<td>Triples analysis</td>
<td>LSB replacement steganography</td>
<td>Known stego</td>
<td>Lossy (JPEG)</td>
<td>Low**</td>
<td>7.8%</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>PVD attack</td>
<td>PVD steganography</td>
<td>Chosen stego</td>
<td>Greyscale</td>
<td>Any</td>
<td>9.2%</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>AAPP steganalysis</td>
<td>LSB replacement steganography</td>
<td>Chosen stego</td>
<td>Lossless</td>
<td>Any**</td>
<td>8.3%</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>TPVD steganalysis</td>
<td>Tri-way PVD steganography</td>
<td>Chosen stego</td>
<td>Greyscale</td>
<td>&gt;10%</td>
<td>7.43%</td>
<td>HIGH</td>
</tr>
<tr>
<td>BPS attack</td>
<td>Boundary pixel steganography</td>
<td>Chosen stego</td>
<td>Binary</td>
<td>Any</td>
<td>8.04%</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

Notes: *100% embedding gives best results, 50% gives average results.  
**Better results when embedded message is small.  
***Gives highly inaccurate results for few images.

### 3.2 Analysis

It is clear from Table 1 that chi-square attack (Westfeld and Pfitzmann, 1999) gives best results when the test image is fully embedded with secret message, in other words, all the pixels of the test image are embedded with secret bits. But its results are not reliable for very low amount of embedded message. Chi-square attack can be applied only when the message has been sequentially embedded into the image. However, this method was later generalised to detect randomly scattered messages (Nissar and Mir, 2010). Chi-square attack cannot reliably detect how much data is embedded in an image that contains intrinsic noise. The test may give false positives even for images that contain absolutely no embedded data. This makes this method’s detection accuracy, LOW.

RS steganalysis (Fridrich et al., 2001) is more reliable than chi-square method (Westfeld and Pfitzmann, 1999). Both the techniques attack an image in which embedding is done using LSB replacement method, i.e., flipping of the LSBs if they do not match the secret message bits. RS steganalysis is better than chi-square method as the former can attack even if the secret message is embedded non-sequentially whereas the latter one fails in such case. But RS steganalysis will fail if the secret message is embedded in the cover image at a rate less than 0.005 bpp. This method is prone to errors and it also gives extreme outliers yielding highly unreliable results (Bohme, 2005).
makes the detection accuracy of this method LOW. Both these methods (Westfeld and Pfitzmann, 1999; Fridrich et al., 2001) can be applied to colour as well as greyscale test images.

### Table 2

<table>
<thead>
<tr>
<th>Steganalysis algo</th>
<th>Statistical changes detected</th>
<th>Information obtained</th>
<th>Case of failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chi-squared attack</td>
<td>PoV formation</td>
<td>Probability of embedding</td>
<td>Fails if data is embedded in the noisy part of image and if message is embedded non-sequentially</td>
</tr>
<tr>
<td>RS steganalysis</td>
<td>The proportion of regular and singular groups form curves quadratic in the amount of message embedded</td>
<td>Embedding rate</td>
<td>Fails if embedding rate is less than 0.005 bpp</td>
</tr>
<tr>
<td>SPA method</td>
<td>Change in cardinalities of trace submultisets of pixels</td>
<td>Length of embedded message</td>
<td>Fails if size of the corresponding subsets before and after embedding remain same</td>
</tr>
<tr>
<td>Triples Analysis</td>
<td>A feature vector, calculated on pixel groups.</td>
<td>Length of embedded message</td>
<td>Fails if embedded message size is large</td>
</tr>
<tr>
<td>PVD steganalysis</td>
<td>Step effect is observed in the histogram of the image</td>
<td>Probability of embedding</td>
<td>Fails if blocks of pixels are defined according to a secret key in the algorithm.</td>
</tr>
<tr>
<td>AAPP steganalysis</td>
<td>Transitions in adjacent pixel pairs</td>
<td>Length of embedded message</td>
<td>When embedding is done in active regions of the image.</td>
</tr>
<tr>
<td>TPVD steganalysis</td>
<td>Growing Anomalies feature derived from differences of Tri-way pixel difference histogram</td>
<td>Secret message rate</td>
<td>Gives inaccurate results if embedding is less than 10% of the image</td>
</tr>
<tr>
<td>BPS attack</td>
<td>Pixel-wide distortion near Boundary pixels</td>
<td>Length of embedded message</td>
<td>Fails if the image has a very high degree of randomness</td>
</tr>
</tbody>
</table>

SPA method, PVD attack and BPS attack can perform accurately no matter what the percentage of embedding is there in the test image, but these three support different test image formats. SPA method supports colour images whereas PVD attack supports greyscale images. The sample pair analysis technique precisely measures the length of embedded message. This method is marginally more accurate than the RS steganalysis method (Fridrich et al., 2001). It fails when the size of corresponding trace submultisets, before and after embedding, remains the same. SPA method detects even very small messages accurately but sometimes it gives highly inaccurate results for some images. This is the reason that in spite of giving highly accurate results most of the time; its detection accuracy is marked as MEDIUM in Table 1. Also, the fact that it requires the cover image of the test image for its process of detection makes it less practical.

Triples method is vastly superior in every case except for simple uncompressed covers. However, triples estimator gives wildly inaccurate results if the hidden message is long. It is clearly shown in Ker (2005) that the triples estimator is very substantially more accurate than the RS (Fridrich et al., 2001) or sample pair (Dumitrescu et al., 2003)
estimators in case of small hidden messages. It is also shown in Ker (2005) that for embedding rates of 0.02 bpp, the reliability of detection is in case of Triples method is superior to RS (Fridrich et al., 2001) or sample pair methods (Dumitrescu et al., 2003). Triples analysis detects only small messages in test images of lossy compressed colour image formats, e.g., JPEG images. But it requires the cover image of the test image for detecting the message length, making its detection accuracy MEDIUM.

The PVD method is not very sensitive to straightforward histogram analysis as compared to LSB. But applying its enhanced version PVD+LSB (Yang et al., 2007; Shreelekshmi et al., 2011), it can be attacked (Zaker and Hamzeh, 2011). In this method (Zaker and Hamzeh, 2011), a substitute image is generated from the pixel-pair difference vector of the stego-image. Then, they applied chi-square steganalysis on the substitute image to detect the presence of embedded data. This produces a step effect in the histogram of the substitute image. But this PVD attack fails if blocks of pixels are defined according to a secret key in the algorithm. Hence, the detection accuracy of this method is MEDIUM.

AAPP steganalysis can detect messages of any length in lossless image formats example GIF and BMP images, but gives comparatively better results when hidden message is small in length. It is a variant of SPA method, but it is better than the latter for the reason that it does not require the cover image for estimation. The maximum error of secret message length estimation is not more than 10% as per the experimental results of Ker (2005). This makes the detection accuracy of this method HIGH. But this method fails when secret message is embedded cleverly in active regions of the image.

TPVD steganalysis performs accurately only when secret bits are embedded in more than 10% of the total pixels of the test image. It can successfully be applied to greyscale images. TPVD steganalysis has a negligibly low error rate and estimates the secret message rate with average accuracy of 95%. The accuracy of detection is as HIGH as 97% (Zaker and Hamzeh, 2011) when the hidden message occupies more than 10% pixels in the test image. However, this method does not give reliable results for very small messages and fails when the amount of embedding is below 10% in the test image.

The methods having high detection accuracy for colour and greyscale images do not apply well to binary images. BPS attack (Chiew and Pieprzyk, 2010) supports only binary test images and detects with high accuracy. But when the amount of embedding is as high as 80% or more, the amount of pixel-wide notches and protrusions become very high, the estimation is not so accurate. But in this situation, the image becomes highly distorted and has a huge amount of randomness in it which can be easily spotted just as we see it. So, the detection accuracy of this method is HIGH.

4 Future research scopes

The preceding section provides details of various targeted steganalysis algorithms which have evolved over time with respect to their ability of detecting steganography and estimating the length of secret message embedded. It is very difficult for any single steganalysis algorithm to accurately estimate the existence as well as length of hidden message in each and every stego-image it works upon. This makes steganalysis of digital images a very vast area of research. Some of the future scopes of research in this area are listed in this section.
Eliminating the requirements of cover images for detection: instead of using the cover image of the test image for detecting the existence to embedded messages in the test image, techniques which magnify the difference between cover images and stego-images, without requiring the cover images beforehand, can be used. Some such techniques are:

a Calibration – estimating cover image statistics from the test image. As the test image and its actual cover image are statistically related, this technique traces back the cover image by estimating the statistical changes from the test image. Then the difference between the test image and its estimated cover image is used to predict whether the test image is a stego one or a cover image.

b Re-embedding into the test image to find a state when no more data can be embedded and the change in statistics of the test image caused by this indicates the amount of embedding. This technique has been utilised in the two methods explained in Section 2, namely, TPVD steganalysis and BPS attack.

Both these methods can be used together to estimate the cover image and find its differences with the test image and model the differences mathematically to find a differentiating feature which helps in estimating the length of the secret message, if any. Developing new techniques like these to estimate the cover image from the test image can also serve as an extensive area of research.

Ensuring the universality of the steganalysis methods: a steganalysis technique can be said to be universal if it can be applied to any image format. There are only few methods which apply to both colour and greyscale images and the methods that can be successfully applied to colour or greyscale images, fail when applied to binary images. So, the techniques become not only specific towards certain steganography algorithm, but also towards the test image types supported by them. So, extending the scope of images supported by the techniques that are already available might be an active part of research in the future.

Detecting accurately in cases of high randomness: digital images are considered to be best suited for steganography as it has high amount of redundant data which are practically unimportant. High amount of randomness mostly yields high amount of random noise in the image which becomes the cause of failure of many steganalytic techniques such as the chi-square method (Westfeld and Pfitzmann, 1999). Techniques can be developed to reduce the noise of the image along with preserving the embedded secret message bits in the image.

Increasing detection accuracy of an algorithm for both, low as well as high amount of embedding: many algorithms perform extremely well when amount of embedding is low (high) and give extreme outliers as results when the amount of embedding becomes high (low). Research can be carried out in this particular area for improving the detection accuracy, decreasing the maximum error rate and hence, making the technique under consideration more reliable.
5 Conclusions

This paper evaluates various targeted digital image steganalysis techniques and throws light upon their detection accuracy and areas of failure of the techniques. It also provides a glimpse of what the possibilities of research in this field can be. A lot of work has been done over the years in the field of steganalysis of digital images. But with each new day, new and stronger steganographic algorithms are being developed which might be ensuring covert communication over the internet through innocent-to-look digital images. This era of fast growing internet, thus, demands the continuous improvement of already available steganalysis methods and the development of new methods to break the newly developed steganographic algorithms. The future work will be the modification of the existing steganalysis techniques and improving them through techniques mentioned in Section 4 of this paper.

References


