Analysis of Modern Steganographic Techniques

Remya Unnikrishnan
unnikrishnan.remya@gmail.com

ABSTRACT
Steganography is the science that involves communicating the secret data in an appropriate multimedia carrier e.g. image, audio and video files. In this paper we have made an analysis of modern steganographic algorithms that are edge adaptive i.e. which can embed most of the secret data in edge areas while leaving the smoother regions as they are. Based on certain design criteria’s such as security against RS steganalysis, invisibility (visually and statistically), embedding scheme etc, the algorithms have been evaluated. Our analysis explores the strengths and weaknesses of the modern steganographic techniques which will enable us to design a better steganographic algorithm.

KEYWORDS
Image Steganography, Pixel-value differencing (PVD), Least significant bit based steganography (LSB), steganalysis.

1.INTRODUCTION
Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have their own respective strong and weak points. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. On the other side, steganalysis aims to expose the presence of hidden secret messages in those stego media. If there exists a steganalytic algorithm which can guess whether a given media is a cover or not with a higher probability than random guessing, the steganographic system is considered broken.

The rest of the paper is organized as follows Section 2 gives a literature survey on certain modern steganographic schemes highlighting its strengths and weaknesses. Section 3 analysis the different schemes based on certain design criteria’s. Finally concluding remarks are given.

2.LITERATURE REVIEW

2.1 HIDING BEHIND CORNERS: USING EDGES IN IMAGES FOR BETTER STEGANOGRAPHY (HBC) [1]
Certain digital techniques do not take into account the cover’s original information thereby they leave certain marks on the stego image. Here they have avoided this by taking the cover’s original information. The earlier techniques achieved this goal by providing the user both the original cover image and the stego image during the data retrieving process which is not secure. Two algorithms are used here based on using image filters to determine the effective hiding places they are: FilterFirst and BattleSteg. Both the algorithms have various strengths and weaknesses.

The strengths of FilterFirst are that it eliminates the need to provide any extra information such as original image, yet ensures that the same pixels are used for hiding and retrieval, it is more difficult to identify the steganographic images but much easier to retrieve the hidden information. It is also very effective in hiding information. Whereas the weaknesses of FilterFirst are that it is not secure, as an attacker can repeat the filtering process, it is also much easier to retrieve the hidden information once the stego-image is identified.

The Strengths of BattleSteg are that it requires a password to retrieve the message. Its weaknesses are that there is no random seed so it is impossible to know where to place the shots and also it is possible for BattleSteg to never have a hit.

2.2 HIDING SECRET MESSAGE IN EDGES OF THE IMAGE (RELSB) [2]
Here a new least significant bit embedding algorithm for hiding secret messages in nonadjacent pixel locations of edges of images is proposed. Here the messages are hidden in regions which are least like their neighboring pixels i.e. regions that contain edges, corners, thin lines etc so that an attacker will have less suspicion of the presence of message bits in edges, because pixels in edges appear to be much brighter or dimmer than their neighbours. Edges can be detected by edge detection filters.

. For a 3x3 window Laplacian edge detector [14] has the following form.

$$D=8x_5-(x_1 + x_2 + x_3 + x_4 + x_6 + x_7 + x_8 + x_9)$$  (1)

where $x_1, x_2, x_3, x_4, x_6, x_7, x_8$ and $x_9$ are the pixel values in a sliding 3x3 window scanning from the top left to bottom right with center pixel value $x_5$. D will become positive when the center pixel x is brighter is brighter than its neighbours and vice versa. One common disadvantage of LSB embedding is that it creates an imbalance between the neighbouring pixels causing the value of D to change. Here this imbalance is avoided by flipping the gray-scale values among 2i-1, 2i and 2i+1. This ensures that the new value
of D after LSB embedding is not different from the old value of D before embedding.

The various strengths of this scheme are that an attacker will have less suspicion to the presence of message bits in edges because pixels in edges appear to be either much brighter or dimmer than their neighbours and it is also secure against blind steganalysis. In order to ensure that the neighbouring pixels in the window are not changed by Laplacian edge detectors, we apply the edge detection filter in a non-overlapping window only. It also limits the length of the secret message to be embedded.

The proposed algorithm random edge LSB (RELSB) embedding uses least significant bit embedding at random locations in nonadjacent edge pixels of the image.

2.3 ADAPTIVE DATA HIDING IN EDGE AREAS OF IMAGES WITH SPATIAL LSB DOMAIN SYSTEMS (AE-LSB) [3]

Here a new adaptive least-significant bit (LSB) steganographic method based on pixel-value differencing (PVD) [7] is proposed. The difference value of two consecutive pixels estimates how many secret bits to be embedded into the two pixels. Pixels located in the edge areas are embedded with more secret bits than that located in smooth areas. The range of difference values is adaptively divided into lower level, middle level, and higher level. Both the pixels in the pair are embedded by the \( \kappa \)-bit LSB substitution method. Depending upon the range which the value belongs to the value is adaptive and will change. The readjusting phase ensures that the two consecutive pixels belong to the same level both before and after embedding.

It is based on the concept that edge areas can tolerate a larger number of changes than smooth areas. The range \([0, 255]\) of difference values is divided into different levels i.e. lower level, middle level and higher level. A higher level will use a larger value of \( \kappa \) modified LSB substitution method. For extracting data exactly, the difference values before and after embedding must belong to the same level.

This scheme provides more capacity and better quality than the PVD [7] and improved version of PVD (IPVD) [8]; it also has a characteristic of imperceptibility. The relative attacks to either destroy or detect the embedding information are not given here.

2.4A HIGH QUALITY STEGANOGRAPHIC METHOD WITH PIXEL-VALUE DIFFERENCING AND MODULUS FUNCTION [4]

In this paper a new method has been devised by which the falling-off-boundary problem can be avoided by using the pixel-value differencing and modulus function. Here first the difference value of the two consecutive pixels is computed and then their remainder is calculated by the modulus operation.

The secret data is embedded into the two pixels by modifying their remainder.

The hiding capacity of the two consecutive pixels depends upon the difference value taken i.e. lesser the difference value smoother the area, so only less secret data can be embedded and vice versa.

The various strengths of this scheme are that it can greatly reduce the visibility of the hidden data than the PVD method. Since this scheme uses the remainder of the two consecutive pixels it is more flexible, it can solve the falling-off-boundary problem by readjusting the remainder of the two consecutive pixels, highly secure against RS steganalysis [9].

Since in this technique the selection of pixel pair is mainly dependent on a PRNG, the modified pixels will be spread around the whole stego image, many smooth regions will get altered.

2.5 EDGE ADAPTIVE IMAGE STEGANOGRAPHY BASED ON LSB MATCHING REVISITED (EA-LSBMR) [5]

In most of the existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator the relationship between the image content and the size of the secret message is not considered. Therefore most of the smooth or flat regions would get contaminated even at a low embedding rate.

In this steganographic technique, the LSB matching revisited image steganography (LSBMR) [6] is expanded and an edge adaptive scheme is proposed where the embedding regions are selected according to the size of the secret message and the difference between two consecutive pixels in the cover image. For lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. As the embedding rate increases more edge regions would be adaptively released by adjusting just a few parameters.

The flow diagram of the data embedding stage is shown in Fig.1. First some parameters are initialized which are then used for region selection and data preprocessing. Then the capacity of the selected region is checked against the secret message to be embedded, if the region selected is enough for embedding the data then the data is embedded. Else again parameters have to be revised and then again region selection and capacity estimation have to be done.

The absolute difference between two adjacent pixels is the criterion for region selection, and LSBMR [6] is used as the data hiding algorithm.

The strengths of this scheme are that for lower embedding rates only the sharper edge regions are used for hiding data and it would not leave any obvious visual artifacts in the LSB planes of the stegos. As the embedding rate increases more edge regions would be adaptively released by adjusting just a few parameters. Certain parameters are selected here which may be different for different image content and secret message. These parameters are kept as side information in a predetermined area of the image. Hence extracting of the data is easier as shown in Fig.2.
Fig.1. Data Embedding

Fig.2. Data Extracting

The main advantages of this scheme when compared with the other schemes are that both the visual quality and security of the stego images is improved.

The weaknesses of this scheme is that the pixel modification rate is higher than that of AE-LSB [3] and this paper does not evaluate the security for JPEG images due to JPEG incompatibilities [15].

3. ANALYSIS OF STEGANOGRAPHIC TECHNIQUES

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Embedding scheme</strong></td>
<td>Difference between pixel &amp; its neighbours and uses LSB replacement</td>
<td>Least significant bit embedding at random locations at non adjacent pixel locations.</td>
<td>Difference between pixel &amp; its neighbours</td>
<td>Pixel difference and modulus function</td>
<td>Pixel difference for region selection and LSBRM is data hiding algorithm</td>
</tr>
<tr>
<td><strong>LSB replacement style asymmetry</strong></td>
<td>Present</td>
<td>Absent</td>
<td>Absent</td>
<td>Absent</td>
<td>Absent</td>
</tr>
<tr>
<td><strong>Security against RS Steganalysis</strong></td>
<td>Not secure</td>
<td>Secure</td>
<td>Not secure</td>
<td>Secure</td>
<td>Secure</td>
</tr>
<tr>
<td><strong>Utilisation of Edge areas</strong></td>
<td>Utilized fully</td>
<td>Cannot make full use</td>
<td>Cannot make full use</td>
<td>Cannot make full use</td>
<td>Utilized fully</td>
</tr>
<tr>
<td><strong>Pixel or pixel pair selection</strong></td>
<td>Mainly depends on a PRNG</td>
<td>Mainly depends on a PRNG</td>
<td>Mainly depends on a PRNG</td>
<td>Mainly depends on a PRNG</td>
<td>Relationship between the image content and size of the secret message</td>
</tr>
<tr>
<td><strong>Invisibility</strong></td>
<td>Visually highly invisible</td>
<td>Visual and statistical differences b/w cover and stego image</td>
<td>Visual and statistical differences b/w cover and stego image</td>
<td>Visual and statistical differences b/w cover and stego image</td>
<td>Highly invisible both visually and statistically</td>
</tr>
</tbody>
</table>
The various aspects which were used for analysis are embedding scheme, LSB replacement style asymmetry, security against RS steganalysis, utilization of edge areas, pixel/pixel pair selection and the average rate of modification. From the analysis we get to know that only HBC [1] will first embed the secret bits into edge regions as far as possible while keeping the smooth regions as they are, but it is vulnerable to RS steganalysis due to LSB replacement style asymmetry. RELSB [2] performs data hiding on the center pixels by detecting the edges and is also secure against blind steganalysis. The disadvantage with this scheme is that embedding capacity is relatively low. AE-LSB [3] provides better capacity but is vulnerable to attack by RS steganalysis [9]. The average modification rate of the pixels is the least i.e. the average payload capacity of each single pixel is the largest among the other schemes, so only fewer pixels need to be modified at the same embedding rate. But here the less smooth regions would get contaminated due to its lesser modification rate. PVD with modulus function [4] reduces the visibility of the hidden data than the PVD method and it is also secure against RS steganalysis. EA-LSBMR [5] utilizes the edge areas fully so is both visually and statistically invisible. It is also secure against RS steganalysis. From the analysis we have done in TABLE 1 we can arrive at the conclusion that only HBC [1] and EA-LSBMR [5] utilizes the edge areas fully. But HBC [1] is vulnerable to RS steganalysis [9] and sample pair analysis [13] since it just modifies the LSBS and so LSB replacement style asymmetry is present. EA-LSBMR [5] provides both visual and statistical invisibility against steganalysis like [9]-[13].

**CONCLUSION**

From the above analysis we have seen that HBC [1] even though utilizes the edge areas fully is insecure against RS steganalysis as it just modifies the LSBS. PVD with modulus function [4] provides lesser distortion to the stego image than the other PVD methods but doesn’t utilize the edge areas fully so is not visually invisible than EA-LSBMR [5]. The average rate of pixel modification is the least for AE-LSB [3] compared with the other schemes. But this can lead to contamination of the less smooth areas. EA-LSBMR [5] is both visually and statistically invisible utilizing the edge areas fully when compared with the other methods.

The research to devise a strong steganographic method is a continuous process. By such analysis we can arrive at a strong steganographic algorithm in the coming days.

**REFERENCES**


