**ABSTRACT**

The paper describes short survey on different steganography techniques for an image in spatial and transform domains and steganalysis techniques for hide the secret message. The strong and weak points of these techniques are mentioned briefly so that researchers who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. One can develop a better steganography technique by analyzing the contemporary steganalysis techniques.

**KEYWORDS:** Discrete wavelet transform (DWT), Discrete cosine transform(DCT), Integer wavelet transform(IWT), Least significant bits(LSB), Pixel value differencing(PVD), Gray level modification(GLM).

**INTRODUCTION**

Steganography is a process that hide the secret information or message into a cover media. Cover media can be a image or a audio or video file. There are two main steganography techniques: Spatial Domain and Transform Domain. Spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as “simple systems”.

The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format. Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods hide messages in more significant areas of the cover image, making it more robust. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression. In the next sections steganographic algorithms will be explained in categories according to image file formats and the domain in which they are performed.

**STEGANOGRAPHY TECHNIQUES**

Spatial Domain Steganographic Method

a) LSB Technique

Steganography software hide information by replacing only the least significant bits (LSB) of an image with bits from the file that is to be hidden. One of the most common techniques used in steganography. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

**Example of Lsb:**

<table>
<thead>
<tr>
<th>Pixels:</th>
<th>Secret message:</th>
<th>Result:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10101110 11101001 10101000)</td>
<td>01000001</td>
<td>(10101110 11101001 10101000)</td>
</tr>
<tr>
<td>(10100010 01011000 11101001)</td>
<td></td>
<td>(11011000 10000111 01011001)</td>
</tr>
<tr>
<td>(11011000 10000111 01011001)</td>
<td></td>
<td>(11011000 10000111 01011001)</td>
</tr>
</tbody>
</table>

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the...
cover-object, but the cover-object is degraded more, and therefore it is more detectable.

B) **Gray level modification method** [8]

- Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM Steganography uses the concept of odd and even numbers to map data within an image.
- A set of pixels are selected based on a mathematical function from a given pixel. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

C) **Data Hiding by PVD** [8]

- The pixel-value differencing (PVD) method segments the cover image into non-overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding.
- This Steganography method is based on image layers. This method divides the host image into each block and embeds the corresponding secret message bits into each block using the layers which are made by binary representation of pixel values. It then performs a search on the rows and columns of the layers for finding the most similar row and column of the layers for finding the most similar row or column. The location of row/column and its differences from secret message is then marked by modifying the minimum number of bits in the least significant bits of the blocks.

**TRANSFORM DOMAIN STEGANOGRAPHIC METHOD**

A) **DCT based Data Hiding** [10]

- DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It can separate the image into high, middle, and low frequency components.
- In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks.

B) **Discrete Wavelet Transform Technique (DWT)** [5]

- Scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighbouring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed.
- The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image. Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighbouring pixels and then store the sum on the top and the difference on the bottom.
- Repeat this operation until all the columns are processed. Finally, we will obtain sub-bands denoted as LL, HL, LH, and HH respectively.
- Integer wavelet transform has been derived from using lifting scheme. IWT results the coefficients in terms of integers. Therefore this transform is used for LSB based embedding.
- In general, Low Frequency (LF) and High Frequency (HF) components are generated by averaging and differencing methods respectively.

C) **IWT (Integer wavelet transform)** [1]

- Integer wavelet transform has been derived from using lifting scheme. IWT results the coefficients in terms of integers. Therefore this transform is used for LSB based embedding.
- In general, Low Frequency (LF) and High Frequency (HF) components are generated by averaging and differencing methods respectively.
- Haar wavelet transform is a basic wavelet transform among wavelet family. Integer wavelet transform has been derived using lifting scheme. IWT results the coefficients in terms of integers.
- Therefore this transform is used for LSB based embedding. In general, Low Frequency (LF) and High Frequency (HF) components are generated by averaging and differencing methods respectively. First level decomposition of an image gives Approximation (LL), Horizontal (LH), Vertical (HL) and Diagonal (HH) coefficients. LL coefficients are more sensitive than the remaining coefficients, so the embedding is done in all the sub-bands except LL sub-band. Since LH, HL and HH coefficients contain edge information more information can be embedded in these coefficients.
CONCLUSION
The paper describes a short survey on different types of steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image in spatial domain. The strong and weak points of these techniques are mentioned briefly so that researchers who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. The next plan is to develop a steganography technique that is robust to different types of attacks and the majority of contemporary steganalysis techniques fail to detect the presence of secret messages.

REFERENCES
16. Satish Singh Verma, Ravindra Gupta, Gaurav Shrivastava” A Novel Technique for Data Hiding in Audio Carrierby Using Sample Comparison in DWT Domain”