Survey and Analysis of Current methods of Steganography

Madhulina Das¹, Samir Kumar Bandyopadhyay²

¹, ² Department of Computer Science and Engineering, University of Calcutta, India

Abstract - Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. In order to address this Information Security, Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. This paper is a tutorial review of the steganography techniques appeared in the literature.

Keywords: Digital image steganography; spatial domain; frequency domain; adaptive steganography;

I. INTRODUCTION

Steganography is an art of secret communications. Steganography means to conceal messages existence in another medium. Its techniques are in use from hundreds of years. Digital Steganography is the technique of securing digitized data by hiding it into another piece of data. Today, in digital age the easy access to any form of data such as audio, videos, images and text make it vulnerable to many threats [1].

Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis.

1.1. Steganography in Digital Mediums

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security. It can be shown in Figure 1.

![Steganographic Process](image)

Cover image  +  Secrete image (it can be data also)  →  Stego image

Fig1: (Steganograhpic Process)

@IJMTER-2015, All rights Reserved 527
I.1.1. **Image Steganography**: Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

1.1.2. **Network Steganography**: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP *etc*., where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields [2].

1.1.3. **Video Steganography**: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

1.1.4. **Audio Steganography**: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or *etc* for steganography.

1.1.5. **Text Steganography**: General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code [3] and *etc* is used to achieve information hiding.

II. **OBJECTIVE OF STEGANOGRAPHY**

The main goal of steganography is to communicate securely in a completely undetectable manner [4] such that no one can suspect that it exist some secret information. The data can be copied for purpose of copyright violation, tampered with or illegally accessed without the knowledge of owner. Therefore, the need of hiding secret identification inside different types of digital data is required such that owner can prove copyright ownership; enhancing robustness of image search engines and smart IDs (identity cards) where individuals’ details are embedded in their photographs.

Other objective are video-audio synchronization, companies’ safe circulation of secret data, TV broadcasting, TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network traffic of particular users) [3], and also checksum embedding [11].

III. **HISTORY OF STEGANOGRAPHY**

The standard and concept of “What You See Is What You Get (WYSIWYG)” which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a steganographer as it does not always hold true. A thorough history of steganography can be found in the literature [3,5 , 6]. The word steganography is originally derived from Greek words which mean “Covered Writing”. It has been used in various forms for thousands of years. In the 5th century BC Histaiaicus shaved a slave’s head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [3, 5, 6, 7]. In the recent history with the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone “digital”. One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh [8], who proposed a method which resembles embedding into the 4 LSBs (least significant bits). They examined image downgrading and contamination which is known now as image-based steganography. Embedding hidden messages in video and audio files is also possible. Examples exist in [9] for hiding data in music files, and even in a simpler form such as in Hyper Text Mark up Language (HTML), executable files (.EXE) and Extensible Markup Language (XML) [10].
IV. Methods of steganography

Steganography methods can be classified into six categories.

4.1 Substitution

A general framework showing the substitution method is highlighted in Fig 2.

Jung and Yoo [12] down-sampled an input image to \( \frac{1}{2} \) of its size and then used a modified interpolation method, termed the neighbour mean interpolation (NMI), to up-sample the result back to its original dimensions ready for embedding. For the embedding process the up-sampled image was divided into 2x2 non-overlapping blocks as shown in Fig. 3. Potential problems with this method are:

- the impossibility of recovering the secret bits without errors, owing to the use of \( \log_2 \), which is also used in the extraction that produces floating point values, and
- since in the 2x2 blocks, the leading value (i.e., block(1,1)) is left unaltered, thus this would lead to the destruction of the natural strong correlation between adjacent pixels which would advertise a non-natural process involvement.
Chi-Kwong Chan and L.M. Cheng [13] proposed a data hiding scheme by simple LSB substitution by applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived. Experimental results show that the stego-image is visually indistinguishable from the original cover-image.

Vijay Kumar Sharma, Vishal Shrivastava [14] proposed another substitution method. The proposed algorithm embedded MSB of secret image in to LSB of cover image. In this n LSB of cover image, from a byte is replaced by n MSB of secret image, the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived. Experimental results show that the stego-image is visually indistinguishable from the original cover-image when n<=4, because of better PSNR which is achieved by this technique.

(Chang et al., 2002) [15] (Thien et al., 2003) [16] proposes that LSB substitution is the most commonly used method directly replacing the LSBs of pixels in the cover image with secret bits to get the stego-image. LSB substitution algorithm is the simplest scheme to hide message in a host image. It replaces the least significant bit (LSB) of each pixel with the encrypted message bit stream. Authenticated receivers can extract the message by deciphering the LSB of every pixel of the host image with a pre-shared key. Since only the least significant bit of pixels is altered, it is visually imperceptible by human. The capacity of the algorithm is 1 bit per pixel.

Samir Kumar Bandyopadhyay et.al [17] proposed a genetic algorithm. Using the proposed Genetic Algorithm, message bits are embedded into different bits of the pixel grey level values, resulting in increased robustness. The robustness would be increased against those attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well. Proposed a Genetic Algorithm approach to make the bit insertion technique more robust by inserting message bits in
different bit level of the pixel grey level values. The layers are selected in pseudo – random method thereby making it more robust against steganalytic attack. The proposed Genetic approach minimises the effect of bit updation on image grey value thereby reducing the risk the statistical stego attack. Moreover only the stego image is sent to the reciever end thereby reducing chances of suspicion.

4.2 Transform Domain

Basically there are many kinds of power level transforms that exist to transfer an image to its frequency domain, some of which are Discrete Cosine Transform, KL Transform and Wavelet Transform.

Gurmeet Kaur and Aarti Kochhar [18] have compare the DCT and DWT method. This paper presents a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. The experimental results show that the algorithm has a high capacity and a good invisibility as compare to DCT. Moreover PSNR of cover image with stego-image shows the better results in comparison with existing Steganography approaches.

DCT

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

$$T(pq) = \alpha(p) \alpha(q) \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F(mn) \cos \left( \frac{\pi(2n+1)q}{2M} \right) \cos \left( \frac{\pi(2n+1)p}{2N} \right)$$

where,

$$0 \leq q \leq N - 1$$

$$0 \leq p \leq M - 1$$

$$\alpha(p) = \begin{cases} \frac{1}{\sqrt{M}}, & p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \leq p \leq M - 1 \end{cases}$$

$$\alpha(q) = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \leq q \leq N - 1 \end{cases}$$

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

DCT is used extensively with video and image compression e.g. JPEG lossy compression. Each block DCT coefficients obtained from Eq. (3) are quantized using a specific Quantization Table (QT).

DWT

Figure 4 describes the typical scenario when using DWT. The image to which DWT is applied gets split up into 4 regions LL, LH, HL, and HH respectively. Of these regions LL region holds the visually more significant data whereas HH region holds the visually less significant data. On application of DWT to the carrier image, the high frequency components get separated from low frequency components which help us to achieve a convenient space to embed our message into it.

![Figure 4 Scenario using DWT](image)

The embedding capacity can be further improved by applying the second level of DWT to LL region which is generated after applying DWT to the entire carrier image. This generates four more regions, namely the LL1, LH1, HL1, and HH1 regions. Of these regions, the LL1 region now contains visually
the most significant details whereas LH1, HL1, HH1 are still acceptable to be replaced. Hence we have successfully tried replacing these regions and the distortion in the carrier image is very low, typically not observable to human eye unless magnified using computing techniques.

![Second Level DWT](image)

Hemalatha S et.al [19] provides a novel image steganography technique to hide both image and key in color cover image using Discrete Wavelet Transform (DWT) and Integer Wavelet Transform (IWT). There is no visual difference between the stego image and the cover image. The extracted image is also similar to the secret image. This is proved by the high PSNR (Peak Signal to Noise Ratio) value for both stego and extracted secret image. The results are compared with the results of similar techniques and it is found that the proposed technique is simple and gives better PSNR values than others.

In Prosanta Gope et. al.’s article [20], the authors introduce an enhanced JPEG steganography along with a suitable encryption methodology using a symmetric key cryptographic algorithm. The JPEG cover image is broken into 8 x 8 blocks of pixel. DCT is applied to each block and quantization is done and data is encrypted using a new encryption method which uses CRC checking.

In S. Arivazhagan et. al.’s work [21] the authors propose a method that works in the transform domain and attempts to extract the secret almost as same as the embedded one, maintaining minimal changes to cover image by using techniques like median maintenance, offset & quantization. A modified approach for embedding color images within color images is proposed and it overcomes the limitations in embedding. Arnold Transform is applied on the secret image to increase robustness. This transformed image is then split into the three Colour planes R, G, B and are subjected to DWT individually, converted to bit stream and then concatenated to be embedded in the cover image which is also subjected to DWT.

### 4.3 Spread Spectrum

Spread spectrum communication describes the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by modulating the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. SSIS works by storing a message as Gaussian noise in an image. At low noise power levels, the image degradation is undetectable by the human eye, while at higher levels the noise appears as speckles or “snow.” The process consists of the following major steps, as illustrated in figure 6:

1. Create encoded message by adding redundancy via error-correcting code.
2. Add padding to make the encoded message the same size as the image.
3. Interleave the encoded message.
4. Generate a pseudorandom noise sequence, n.
5. Use encoded message, m using advanced encryption standard (AES) to modulate the sequence, generating noise, s.
6. Combine the noise with the original image, f. Recover the hidden message. A filter is used to extract the noise from the stego image, resulting in an approximation of the original image. The better this filter works the fewer errors in the extracted message.

Tanmay Bhattacharya et.al [22] proposed a DWT based Steganographic technique. Cover image is decomposed into four sub bands using DWT. Two secret images are embedded within the HL and HH sub bands respectively. During embedding secret images are dispersed within each band using a pseudo random sequence and a Session key. Secret images are extracted using the session key and the size of the images. In this approach the stego image generated is of acceptable level of imperceptibility and distortion compared to the cover image and the overall security is high.

4.4 Statistical
Statistical steganography techniques utilize the existence of “1bit” steganographic schemes, which embed one bit of information in a digital carrier. This is done by modifying the cover in such a way that some statistical characteristics change significantly if a “1” is transmitted. Otherwise the cover is left unchanged, so the receiver must be able to distinguish unmodified covers from modified ones.

In order to construct a l(m)bit stego-system from multiple “1bit” stego system, a cover is divided into l(m) disjoint blocks B1,..,Bl(m). A secret bit, mi, is inserted into the ith block by placing a “1” into Bi if mi=1. Otherwise, the block is not changed in the embedding process. The detection of a specific bit is done via a test function which distinguishes modified blocks from unmodified blocks:

\[
f(B_i) = \begin{cases} 
1 & \text{block } B_i \text{ is modified in the embedding process} \\
0 & \text{otherwise}
\end{cases}
\]

The function f can be interpreted as a hypothesis-testing function; we test the null-hypothesis “block Bi was not modified” against the alternative hypothesis “block bi was modified”. Therefore we can call the whole class of such steganography systems Statistical Steganography. The receiver successively applies f to all cover-blocks bi in order to restore every bit of the secret message.
In Chin-Chen Chang et al.’s article [23] a new approach to wet paper codes using random linear codes of small co-dimension is used which improves embedding efficiency is proposed. To prevent from attack, the selection channel should not be publicly available even in any partial form. A possible remedy is to select it according to some side information that is in principle unavailable to the attacker (e.g.) random or that cannot be well estimated from the stego image. Steganography with non shared selection channels requires codes for memories with defective cells also called wet paper codes. This paper provides a new tool for steganography a coding method that empowers the steganographer with the ability to use arbitrary selection channels while substantially decreasing the number of embedding changes. The algorithm combines wet paper codes with matrix embedding arbitrary selection channels and improved embedding efficiency using random linear codes of small co-dimension. In Tomas Filler et al.’s work [24], the authors propose a practical methodology for minimizing additive distortion in steganography with general embedding operation which is more flexible and easy. Syndrome-Trellis Codes (STC) are used to improve the security of the system. STC divides the samples into different bins (binning) which is a common tool used for solving many information-theoretic and also data-hiding problems. The proposed method can be used in both \textit{spatial & transform domain}. A proper distortion function is chosen which makes statistical detection difficult. Once the steganographer specifies the distortion function, the proposed framework provides all tools for constructing practical embedding schemes. The distortion function or the embedding operations need not be shared with the recipient.

### 4.5 Distortion

Distortion techniques require the knowledge of the original cover in the decoding process. Sender applies a sequence of modifications to a cover in order to get a stego-object, she chooses this sequences of modifications in such a way that it corresponds to a specific secret message she wants to transmit. Receiver measures the difference to the original cover to reconstruct the sequence of modifications applied by sender which corresponds to the secret message.

In many applications, such systems are not useful, since the receiver must have access to the original covers. If anyone also has the access to them, she can easily detect to cover modifications and has evidence for a secret communication. If the embedding and extraction functions are public and do not depend on a stego-key, it is also possible for that person to reconstruct the secret message entirely. Throughout this section we will therefore assume that original covers can be distributed through a secure channel.

An early approach to hiding information is in text. Most text-based hiding method are of distortion type(i.e. the arrangement of words or the layout of a document may reveal information). One technique is done by modulating the positions of lines and words which will be detailed in the next subsection. Adding spaces and “invisible” characters to text provides a method to pass hidden information.

In D.P.Gaikwad et al.’s paper [25] the authors propose image restoration technique in steganography. The image is blurred before hiding the message image using special point spread function and randomly generated key. Sequential LSB embedding in the R plane is done in this project. The number of rows and columns of the message image is encrypted in the first row of the cover image. Before inserting, the original message image is blurred using the specific PSF (Point Spread Function). The parameters used for blurring with PSF are used as keys during deblurring. The secret key values are sent through a secure channel (Tunnelling). The secret image is recovered using the two keys and a third key, which is randomly generated and depends on the content of the hiding message.

In Hamid.A.Jalab et al.’s paper[26], a new information hiding system is presented using distortion. The aim of the proposed system is to hide information (data file) within image page of execution file (EXEfile) to make sure changes made to the file will not be detected by universe and the functionality of
the exe.file is still functioning after hiding process. Meanwhile, since the cover file might be used to identify hiding information, the proposed system considers overcoming this dilemma by using the execution file as a cover file.

In M.B.Ould MEDENI et.al.’s article [27], the authors use error correcting codes in steganographic protocols. An optimal code is one that makes most of the maximum embeddable (MLE). The method referred to as matrix encoding requires the sender and recipient to agree in advance on a parity check matrix \( H \). The cover medium is processed to extract a sequence of symbols \( _{\_} \), which is modified into \( s \) to embed the message \( m \). \( s \) is sometimes called the stegodata, and modifications on \( s \) are translated on the cover-medium to obtain the stego-medium. Relation between steganographic algorithms and error correcting codes are discussed.

4.6 Cover Generation
A cover generation method actually creates a cover for the sole purpose of hiding information. Spam mimic is an excellent example of a cover generation method. Cover generations have heavy and complexity process for algorithms compression with other techniques. This point due to delay time for finished (hiding or extract) process option. Example Automated Generation of English Text. Use a large dictionary of words categorized by different types, and a style which describes how words of different types can be used to form a meaningful sentence. Transform message bits into sentences by selecting words out of the dictionary which conforms to a sentence structure given in the style source.

Vivek sampat et. al. [28] propose an advanced system of audio steganography, which generates a personalized cover dynamically for hiding data within itself. An attempt has been made to make the generated cover meaningful by keeping in mind the concept of musical scales during the generation process.

Some Steganographic applications generate a digital object only for the purpose of being a cover for secret communication [29],[30].

V. CONCLUSION
Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. More restrictions on the use of privacy-protecting technologies are not very unlikely, especially in this period of time with great anxiety of terrorist and other attacks.

REFERENCE