A Survey Paper on Image Steganography for Secure Communication Techniques

Pragnesh Prajapati[1] Hardik Kadia[2]
[1,2]Department of Computer Engineering
[1,2]Merchant Engineering College, Basna

Abstract— 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 respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

Key words: steganographic techniques, grafia

I. INTRODUCTION

Steganography is art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information.

The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning"writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images.

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated . The strength of steganography can thus be amplified by combining it with cryptography.

Two other technologies that are closely related to steganography are watermarking and fingerprinting . These technologies are mainly concerned with the protection of intellectual property, thus the algorithmshave different requirements than steganography.

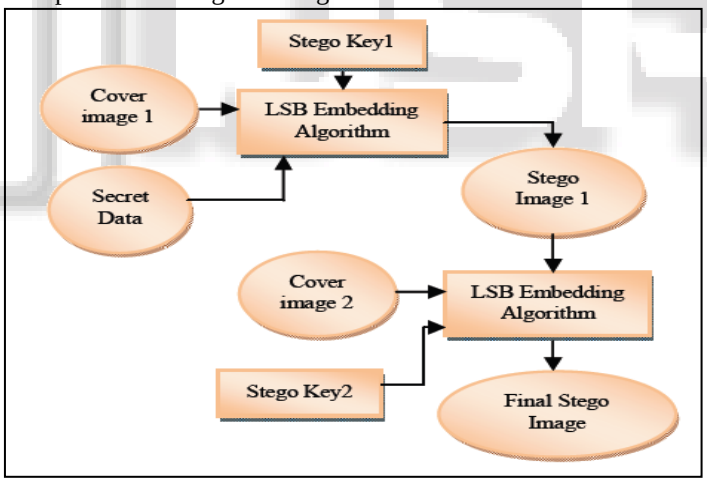

Fig. 1: Data Hiding Process

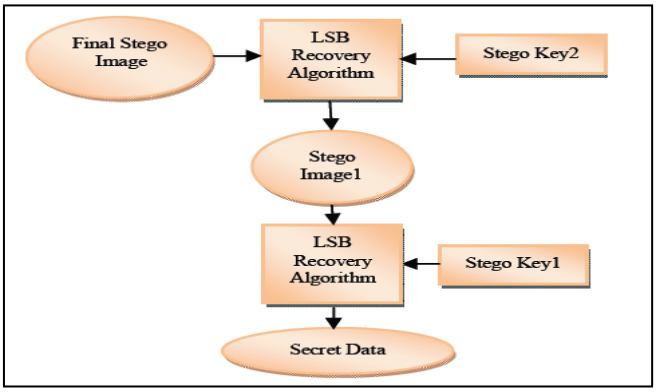

Fig. 2: Data Extraction Process

II. TYPES OF STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [11]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [5]. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.Figure shows the four main categories of file formats that can be used for steganography.

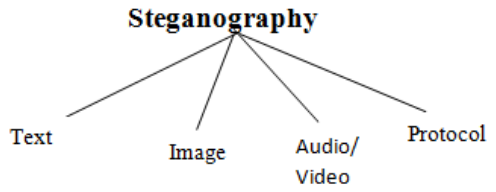

Fig. 3: Categories of Steganography

III. IMAGE STEGANOGRAPHIC TECHNIQUE

A. *Spatial Domain Methods:*

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are:

1) Least significant bit (LSB)
2) Pixel value differencing (PVD)
3) Edges based data embedding method (EBE)
4) Random pixel embedding method (RPE)
5) Mapping pixel to hidden data method
6) Labeling or connectivity method
7) Pixel intensity based method
8) Texture based method
9) Histogram shifting methods

B. *Transform Domain Technique:*

This is a more complex way of hiding information in image. Various algorithms and transformations are used on the image to hide information in.. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions. Transform domain techniques are:

1) Discrete Fourier transformation technique (DFT).
2) Discrete cosine transformation technique (DCT).
3) Discrete Wavelet transformation technique (DWT).
4) Lossless or reversible method (DCT).
5) Embedding in coefficient bits.

C. *Distortion Techniques:*

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit .The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a "1." otherwise, the message bit is a "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.

D. *Masking and Filtering:*

These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

IV. CONCLUSION & FUTURE

In this study, we analyzed image Steganography using LSB approach is simple and very famous technique. LSB Approach provides large message/ image data capacity and also provides better PSNR ratio compare to other technique. But problem is that provide no more robustness against brute force attack and Histogram Analysis. While image Steganography in Frequency Domain technique provide randomize insertion of secret message with high capacity, high PSNR Ratio and good invisibility. Such as using DCT, DWT, IWT etc. And also provide more robustness against brute force attack and Histogram Analysis.

V. FUTURE EXTENSION

Gain better result and improve PSNR ratio of Final Stego Image. Using Huffman Encoding increases the embedding capacity and Security. It provides one type of authentication, as any single bit change in the Huffman coded bit stream, Huffman table is unable to decode.

REFERENCES

[1] .“A Survey of Image Steganography Techniques” by Mehdi Hussain and Mureed Hussain, May 2013.
[2] “Some New Methodologies for Image Hiding using Steganographic Techniques” by Rajesh Kumar Tiwari and Gadadhar Sahoo.
[3] “Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain “J. K. Mandal and Debashis Das by IJIST,July 2012
[4] ”A Steganography Algorithm for Hiding Image In Image By Improved lsb Substitution by Minimize Detection “by vijay kumar sharma , vishal shrivastava, february 2012.
[5] “Dual Image Steganography for Communicating High Security Information” Ketki Thakre, Nehal Chitaliya,ISSN,July 2014
[6] “An Overview Of Image Steganography” by T. Morkel , J.H.P. Eloff M.S. Olivier.
[7] “Steganography Using Least Signicant Bit Algorithm” by Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav,May-2012.
[8] “Edge Adaptive Image Steganography Based on LSB Matching Revisited” by Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member, IEEE, June-2010.
[9] “A detailed look at Steganographic Techniques and their use in an Open Systems Environment” by Bret Dunbar, SANS Institute,january-2002.
[10] “Edge Adaptive Image Steganography Based on LSB Matching Revisited “Weiqi Luo, Member,Fangjun Huang, and Jiwu Huang,IEEE,June 2010
[11] “Digital Image Steganography:Survey and Analysis of Current Methods”Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt,March,2010.
– Books
[12] Rafael C. Gonzalez, Richard “ Digital Image Processing ”.

