ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.7

An Elaborated Review on Steganography Techniques

RajandeepKaur[1], Rajneesh Narula[2]
M. Tech Student[1], Assistant Professor[2]
Department of IT & CSE
Adesh Institute of Engineering & Technology, Faridkot, India

Abstract:
Data hiding techniques are very important for the timely growth of intensive transfer of multimedia content and private communications. The Steganography is the art of hiding information in the cover image that can be used to transfer data and information from one source to other. It hides the existence of the message so that the information is transferred in a secret way. Steganography is possible in digital images also. Many different carrier filescan be used, like digital images which are commonly used nowadays. The concept of hiding the secret message can be done with the help of many steganography techniques like LSB, PVD, etc. Various applications have different requirements and accommodate various methods with advantages as well as disadvantages. This paper intends to provide a review of image Steganography, its uses,and techniques. It also attempts to identify the requirements of a good Steganography algorithm and briefly reflects on which Steganography techniques are more suitable for which applications.

Keywords: Steganography, PVD, Frequency Domain, Spatial domain, LSB method.

I. INTRODUCTION

Since the developmentof theInternet, the mostimportant factor in transferring of the information is the security of information. Steganography is the art and science of invisible communication. It is accomplished by hiding information in other information, thus hidingthe existence ofthe information. Steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing"[1] defining it as "covered writing". In the image Steganography, the information is hidden in images which are generally available on internet.

The idea and practice of information hiding comes from history. The Greek historian Herodotus writes of a Nobleman, Histaeus, who needs to communicate with his son-in-law in Greece, has shaved the head of one of most trusted slave and tattooed the message onto the slave's scalp. When the slave's hair grew back he sends slave with the hidden message and when slave reaches to the destination again he shaved his scalp andretrieve the message [2]. In the Second World War, the new data hiding technique which is known as the Microdot technique was greatly used. In this the information, like photographs, was reduced in sizeuntil it was the size of atyped period (full stop mark). It was extremely difficult to detect a hidden information; a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [3]. Nowadays Steganography is implemented on computers with digital data being the carriers and networks being the high-speed delivery channels. Bothe the fields move in different directions, Steganography's intent is to hide the existence of the message, while cryptography scrambles a message in such a way that it cannot be understood[11].

Steganography and cryptography are techniques used to protect information fromunwanted parties but neither technology alone is perfect. Once the presence of hidden information is revealed or suspected, the reason of Steganography is mostly finished. The strength of Steganography increases by combining it with cryptography.

II. STEGANOGRAPHIC DOMAINS

The Steganography has been categorized into two main categories:
(i) Spatial domain Steganography: Spatial domain Steganography describes the use of pixel gray levels and their color values directly for encoding the message bits. It mainly includes LSB Steganography and Bit-Plane Complexity Slicing (BPS) algorithm. Spatial domain is more generally used because of the high capability of hidden information and the easy realization by a human.
(ii) Transform domain Steganography: The secret information is embedded in the transform coefficients of the cover image. Examples of transform domain Steganography are Discrete Cosine Transform, Discrete Fourier Transform, and Discrete Wavelet Transform.

III. STEGNOGRAPHY

Steganography is used for wide range of organisations such as defence organizations for safe communication of secret information, intelligence agencies, in smart identity cards (HID) where personal details are embedded in the photograph itself for copyright control of materials, medical imaging where patient's details are embedded within theimage providing protection of information and reducing transmission time.

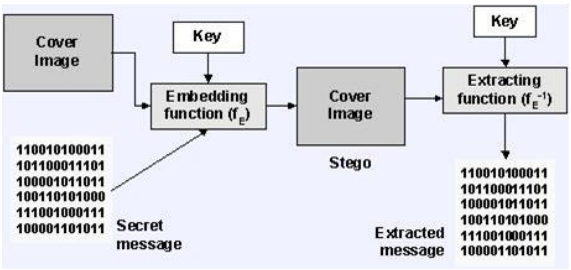

Figure.1. the basic Steganography Model

The model for Steganography shows the basic process involved in Steganography which consists of Cover Image, Secret Message, and Key. Cover Image is also known as cover-object, in which message is embedded and serves to Comparison of different techniques for Steganography in images hide the presence of the message. The Secret Message can be any type of data (plain text, cipher text or another image) that the sender wishes to remain confidential. Key is known as stego-key, which ensures that only recipient who knows the key, the corresponding decoding key will be able to recover themessage from a cover-object. The cover-object with the object secretly embedded message is then called the stego-object [4]. Recovering message from astego-object requires thecover-object itself and acorresponding decoding key if an objectstego-key was used during the information encoding process.

IV. PRINCIPLES OF STEGANOGRAPHY

The secret payload is embedded inside the cover object(image, audio or text) in encrypted format by using a hiding algorithm and it sent to a receiver over a network. The receiver after receiving of the message then decrypted the message by applying the reverse process to the cover data and reveals the secret data [4].

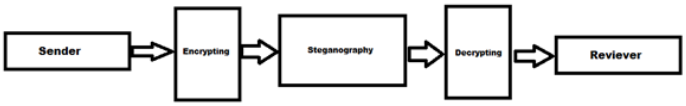

Figure.2. the principle of Steganography

Steganography algorithm tries to save the properties of the original image. A suitable image, called as cover/ carrier, can be selected from the internet or directly captured using a high-resolution camera. The secret message is then inserted into the cover image using the suitable algorithm, in such a way that does not change the original image according to human vision. The result is a new image, the stego-image, which does not look different than the original image.

V. TYPES OF STEGNOGRAPHY

Steganography can be used for almost all digital image formats, but the formats those are with a high degree of redundancy are more suitable. Redundancy is defined as the bits of an object that provide accuracy much greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be alteredwithout the alteration being detected easily [4]. There are four categories of fileformats that can be used for Steganography shown in fig. 3.

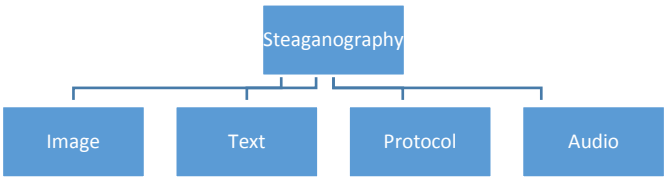

Figure.3. Types of Steganography

Since images are quite a popular cover or carrier objects used for Steganography. In the domain of digital images different image file formats exist for example .jpg, .bmp., .gif, etc.

VI. SPATIAL DOMAIN METHOD

In spatial domain scheme, the secret messages are embedded directly in the cover image. The most widely used and simplest Steganography method is the least significant bit (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding [6]. Least significant bit (LSB) Replacement is a common, simple approach to embedding information in a cover image. The least significant bit (8 bit) of some or all of the bytes inside an image is replaced with a bit of the hidden message in a selected part of the cover image. When using a 24-bit image, a bit of each of the red, green and blue color can be used, since they are each represented by a byte. It allows to store 3 bits in each pixel. The image of 800 X 600 pixel, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [10].

For example, 3 pixels grid for of a 24-bit image can be as follows:

(00101101 00011100 11011101)
(10100111 11000101 00001101)
(11010010 10101101 01100011)

When the binary number 10110110, is embedded into the least significant bits of this part of the image.

The resulting grid is as follows:

(00101101 00011100 11011101)
(10100111 11000100 00001101)
(11010011 10101100 01100011)

The number was embedded into the first 8 bytes ofthegrid, from these only the 3 underlined bits needed to be changed according to the secret message which is embedded. Mostly, half ofthe bits in an image are required to bemodified to hide a secret message using the maximum cover size. Since there are 256 intensities of colour of each pixel, by changing the LSB of a pixel, it results in small changes in the intensity of the colours. These changes cannot be identify by the human eye, thus the message is successfully hidden in image.

Figure.4. the cover image and the stego-image

VII. HIDING GRAY IMAGES USING BLOCKS TECHNIQUE

Internet is growing wider and also the channels for communication. Security of digital media is a great issue due to the fast pace of internet. The hiding of a message will reduce the possibility of detection of the real secret message. This method allows us to hide gray image in one another. In this method the cover is divided into blocks ofequal sizes, Each blocksize issame as that size of the embedding image[4]. Compare each pixel in embedding image with all the corresponding pixels in the blocks of the cover image i.e. pixel (i ,j) in the embedding image iscompared with the pixel (i, j) in all blocks of cover image. Best pixel is selected which is the pixel that gives minimumdifference between it and the pixelto embed. For Example, if pixel (i,j) to embed has a value 254, and corresponding pixels values are: 248, 230, 249, 252, 255,260, 270, and 262 (assume

cover is divided into 8 blocks). Then the pixel with value 255 will be selected to embed 254.

VIII. TRANSFORM DOMAIN METHOD

The transform domain Steganography technique is used for hiding a huge amount of data and provides high security, a good invisibility and no loss of secret message. The goal behind it is to hideinformation in frequency domain byaltering magnitude of all of discrete cosine transform (DCT) coefficients of cover image. The 2-D DCT converts image blocks from spatial domain to frequency domain. The cover image is divided into nonoverlapping blocks of size 8×8 and applies DCT on each of blocks of the cover image using forward DCT [7].

IX. JPEG IMAGE STEGANOGRAPHY TECHNIQUE

Originally it was thought thatSteganography would not bepossible to use with JPEG imagessince they used lossy compression methods which resulted in few parts of the image data being modified. One of the main characteristics of Steganography is that the information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be damaged. Even if the user could somehow keep the message saved and correct it would be difficult to embed the message without the changes beingnoticed because of the quick compression applied. The properties of the compression algorithm have been manipulatedin order to develop asteganographic algorithm for JPEGs[10]. One of the properties of JPEG is exploited to make the changes to the image to make it unnoticeable to the human eye. During the DCT transformation part of the compression algorithm, rounding errors occur in the coefficient data that are not noticeable and understandable. Although this property is what classifies the algorithm as being lossy, this property can also be used to hide messages. It is neither feasible nor possible to embed the message in an image that uses lossy compression since the compression would destroy all information in the process. So, it is important to recognize that the JPEG compression algorithm is actually divided into lossy and lossless stages. The quantization and the DCT phase form part of the lossy stage, whereas the Huffman encoding used to further compress the data is lossless. Steganography takes place between these two stages. Using the same principles of LSB insertion the message can be embedded into the least significantbits ofthe coefficients beforeapplying theHuffman encoding. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain.

X. SPREAD SPECTRUM IMAGE STEGANOGRAPHY TECHNIQUE

The Spread Spectrum Image Steganography (SSIS) is adata hiding/ secret communicationsteganographic technique which uses digital imagery as a cover signal. Spread spectrumprovides theability tohide asignificant quantity of information bitswithin digital images while avoiding detection by an intruder. The message after transfer is recovered with lowest error probability due the use of error control coding. Spread spectrum image steganography payload is, at a minimum, an order of magnitude greater thanof existing watermarking techniques. Furthermore, the original image is not needed to extract the hidden message. The proposed receiver need only a key in order to reconstruct the secret message. The existence of the hidden information is virtually undetectable by human or computer analysis. At last, SSIS provides resiliency to transmission noise, like in a wireless environment and low levels of compression.

XI. EVALUATION

The most important requirement is thata Steganographic algorithm has to be imperceptible. Below criteria has been proposed for imperceptibility of an algorithm:

1) Invisibility- The invisibility of a Steganographic algorithm is prime requirement. The strength of Steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised [8].

2) Payload capacity- Watermarking, needs to embed only asmall amount of copyright information, Inotherhand Steganography requires sufficient embedding capacity [9]. More the data to be hidden more better the technique.

3) Robustness against statistical attacks – Statistical Steganalysis is the practice of detecting hidden information byapplying statisticaltestsoncover image. Many Steganographic algorithms leave a "signature" when embedding information that can be easily detected through statistical analysis.

4) Robustness againstimage manipulation – While being transmitted the image may undergo changes by an active attacker in an attempt to get hidden information. Image manipulation, such as cropping or rotating, can be performed on the image. This may destroy the hidden message. It is required for Steganographic algorithms to be robust against malicious cracking attempts on the image.

5) Independent of file format – The most powerfulSteganographic algorithms thus possess the ability to embed information in any type of file. The work efficiently with each available file formats.

6) Unsuspicious files – This requirement includes all characteristics of aSteganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by an attacker.

Table .1. Comparison of image Steganography techniques

	Invisibility	Payload capacity	Robustness against statistical attack	Robustness against image manipulation	Independent of file format	Unsuspicious files
LSB in BMP	High	High	Low	Low	Low	Low
LSB in GIF	Medium	Medium	Low	Low	Low	Low
JPEG	High	Medium	Medium	Medium	Low	High
Spread Spectrum	High	Medium	High	Medium	High	High

XII. CONCLUSION

Although only some of the popular image steganographic techniques were discussed in this paper, there exists a

large selection of approachesto hiding information in images. Different image file formats have different methods of hiding messages having different strong and weak features respectively. Whereas one technique lacks in payload capacity, while other lacks in robustness. For example, the patchwork approach has avery high level of robustness againstmosttype of attacks, but it can hidesonly avery less amount of information. The Least significant bit (LSB) technique in both BMP and GIF works efficiently, but these both approaches result in suspicious files that increase the probability of detection when in the presence of a intruder. Thus this paper provides the pros and cons of various steaganography techniques available.

XIII. REFERENCES

[1]. T. Sharp, "An implementation of key-based digital signal Steganography", in Proc. Information Hiding Workshop, Springer LNCS 2137, pp. 13–26, 2001.

[2]. JarnoMielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume: 13, Issue: 5, pp. 285- 287.

[3]. K.M. Singh, L.S. Singh, A.B. Singh and K.S. Devi, "Hiding Secret Message in Edges of the Images", Information and Communication Technology, 2007. ICICT '07, pp. 238-241.

[4]. Jagvinder Kaur and Sanjeev Kumar," Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011

[5]. Lee, Y.K.; Chen, and L.H., "High capacity image Steganographic model", Visual Image Signal Processing, 147:03, June 2008

[6]. Johnson, N.F and Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 2008.

[7]. Blossom kaur1, Amandeep kaur2 andJasdeep singh,"Steganographic approach for hiding image in dct domain" International Journal of Advances in Engineering & Technology, July 2011.

[8]. R.Amirtharajan and R.Akila,"A Comparative Analysisof Image Steganography;" International Journal of Computer Applications (0975 – 8887) ,Volume 2 – No.3, May 2010.

[9]. V. Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz, "Modulo based Image Steganography Technique against Statistical and Histogram Analysis", IJCA Special Issue on"Network Security and Cryptography" NSC, 2011.

[10]. Dumitrescu, S., W. Xiaolinand Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355 - 372.

[11]. Ahn, L.V. and N.J. Hopper, 2004. Public-key steganography. In Lecture Notes in Computer Science. Vol. 3027 / 2004 of Advances in Cryptology - EUROCRYPT 2004, pp: 323–341. Springer-Verlag Heidelberg.

[12]. Pang, H.H., K.L. Tan and X. Zhou, 2004. Steganographic schemes for file system and b tree. IEEE Trans. On Knowledge and Data Engineering, 16:701–713.

[13]. Mittal, U. and N. Phamdo, 2002. Hybrid digitalanalog joint source-channel codes for broadcasting and robust communications. IEEE Trans. on Info. Theory, 48:1082 –1102.

[14]. Pavan, S., S. Gangadharpalli and V. Sridhar, 2005. Multivariate entropy detector based hybrid image registration algorithm. IEEE Intl. Conf. on Acoustics, Speech and Signal Processing, pp: 18-23.

[15]. Moulin, P. and J.A. O"Sullivan, 2003. Information theoretic analysis of information hiding.IEEE Trans. on Info. Theory, 49: 563–593.

[16]. Amin, P., N. Liu and K. Subbalakshmi, 2005.Statistically secure digital image data hiding. IEEE Multimedia Signal Processing MMSP05, China.

[17]. Jackson, J., G. Gunsch, R. Claypoole and G. Lamont, 2004. Detecting novel steganography with ananomaly- based strategy. J. Electr. Image, 13: 860– 870.

[18]. Deshpande Neeta, KamalapurSnehal, Daisy Jacobs "Implementation of LSB Steganography and Its Evaluation for Various Bits" Digital Information Management, 2006 1st International conference.ppt 173-178,2007.

[19]. C.Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2Information Hiding Workshop, vol. 1525, pp. 306-318, 1998.

[20]. F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, "Information Hiding – A Survey", in proceeding of IEEE, pp. 1062-1078, July 1999.