A Review of Security and Data Hiding Techniques

Abhishek Kumar, Anuranjan Misra

Abstract- Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. There are different types of steganography techniques each have their strengths and weaknesses. In this paper, we review the different security and data hiding techniques that are used to implement a steganography such as LSB, ISB, MLSB.

Keyword:- LSB, ISB, MLSB, Steganography

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. But it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is defined by Markus Kahn as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". The objectives of Steganography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data.

II. STEGANOGRAPHY

Steganography is a Greek word which means concealed writing. The word “steganos” means “covered “ and “graphial “ means “writing” . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. But today’s most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data

A) Types of Steganography

1. Text Steganography: It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. These methods are i) Format Based Method; ii) Random and Statistical Method; iii) Linguistics Method.

2. Image Steganography: Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

3. Audio Steganography: It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

4. Video Steganography: It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

5. Network or Protocol Steganography: It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used.

B) Framework of Steganography

Steganography is comprised of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message within a cover Work, and is the most carefully constructed process of the two. A great deal of attention is paid to ensuring that the secret message goes unnoticed if a third party were to intercept the cover Work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end. The entire process of steganography can be presented graphically as shown in Fig 1.

Revised Version Manuscript Received on August 20, 2015.

Mr. Abhishek Kumar, M.Tech Student, Department of Electronics and Communication, Noida International University, Delhi National Capital Region Noida, India.

Dr. Anuranjan Misra, Professor & Head, Department of Computer Science and Engineering, Noida International University, Delhi National Capital Region Noida, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

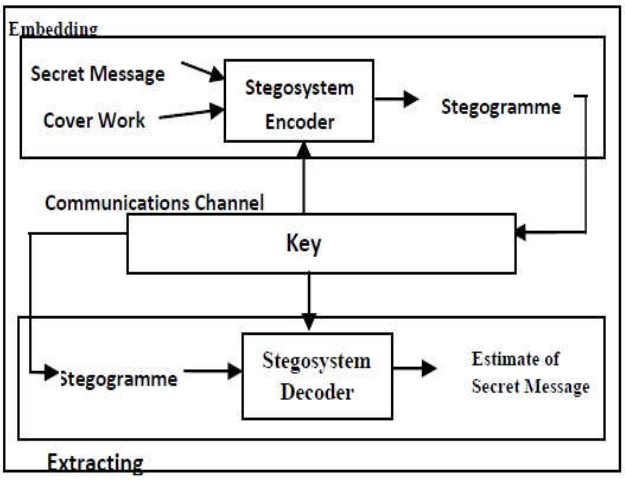

Fig 1 Process of Steganography Two inputs required for the embedding process are secret message and the cover work that is used to construct a stegogramme that contains a secret message.

The inputs are passed through the stego-system encoder to embed the message within an exact copy of the cover work. The stego-system requires a key which is also used at the extraction phase. The resulting output from the stego-system encoder is the stegogramme that contains the secret message. This stegogramme is then sent over some communications channel along with the key that was used to embed the message. Both the stegogramme and the key are then fed into the stego-system decoder where an estimate of the secret message is extracted [9].

III. IMAGE STEGANOGRAPHY

The most cover media used for steganography is image. The reason is that the large amount of redundant data present in the images can be easily altered to hide secret messages inside them without attracting attention to human visual system (HVS).

A. Image Definition

A computer image is an array of points called pixels which are represented as light intensity. The pixels are displayed horizontally row by row. The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel [1]. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour [1].

1) ***Color Table:*** In a 24-bit color scheme each pixel is represented by 3 bytes, each byte representing the intensity of the 3 primary colors Red Green and Blue respectively. Each of these 3 colors has a value that can range from 0 to 255. 0 means the color is not active and 255 means a full amount of color.

Pixels with the following values make specific colors:

255 0 0 is red
0 255 0 is green
0 0 255 is blue
0 0 0 is black
255 255 255 is white

Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours [1]. The RGB values for each pixel are stored in a color table. Each entry has a value for the row and a value for red, green and blue. Each pixel has a color associated with it stored in the color table. The pixel contains a value that corresponds to the row in the color table that contains the REB value for that pixel. The first number is the row number that the pixel references to get its corresponding color. The second number is the value for red, the third number is the value for green and the fourth number is the value for blue.

IV. STEGANOGRAPHY TECHNIQUES

A) Spatial Domain: In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories: i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labelling or connectivity method vii) Pixel intensity based.

i) LSB: this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

ii) BPCP: In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data

iii) PVD: In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

B) Spread Spectrum: The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it become difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication

C) *Hide & Seek(The Sequential Approach):* The simplest form of image steganography is the method known as Hide & Seek [9] which replaces the LSBs of pixel values with the bits from the message bit stream.

The algorithm is so straightforward that it does not require a key to be implemented. This makes things a lot simpler to program and exchange the secret, it does mean that the security lies solely in the algorithm. If a key were used, then it might still be impossible for the adversary to decode the

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

hidden message, as the key would usually index the manipulated regions of the image.

Encoding

Algorithm 1 The encoding process of the Hide & Seek algorithm in sequential mode.

1: for i = 1, ..., l(m) do
2: p = LSB(ci)
3: if p ≠ mi then
4: ci = mi
5: end if
6: end for

The algorithm works by taking the first pixel of the image ci and obtaining its LSB value. This is typically achieved by calculating the modulus 2 of the pixel value. This will return a 0 if the number is even and a 1 if the number is odd, which effectively tells us the LSB value.

We then compare this value with the message bit mi that we are trying to embed. If they are already the same, then we do nothing, but if they are different then we replace ci with mi. This process continues till there are values in m that need to be encoded.

Decoding

As the encoder replaced the LSBs of the pixel values in c in sequence, the order is already known that should be used to retrieve the data. Calculate the modulus 2 of all the pixel values in the stegogramme s, and reconstruct m as mi'.

Algorithm 2 The decoding process of the Hide & Seek algorithm in sequential mode

1: for i = 1, ..., l(s) do
2: mi'=LSB(si)
3: end for Run

the loop for l(s) instead of l(m). If a key were used, it would probably reveal this information, but instead simply retrieve the LSB value of every pixel. When converted this to ASCII, the message will be readable up to the point that the message was encoded.

V. CONCLUSION

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. The simpler systems can be used in such a way that they make life harder for the steganalyst, simply by embedding shorter messages. Short messages create a shorter bit-stream, which in turn requires less bit-flips to embed. With fewer modifications made to an image, it is much harder to spot a difference between the stegogramme and a clean version of the same image. It is still highly likely that a complete steganographic system might employ cryptographic measures as a safety-net to protect the content of the message in the event that the steganography is broken. In these years, LSB is the most widely used technique for steganography. Some researchers have also used the techniques like water marking, distortion technique, spatial technique, ISB, MSB in their work and provided a strong means of secure information transmission. In further research we are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

REFERENCES

1. Owens, M., A discussion of covert channels and steganography, SANS Institute, 2002
2. ohnson, N.F. & Jajodia, S., Steganalysis of Images Created Using Current Steganography Software, Proceedings of the 2nd Information Hiding Workshop, April 1998
3. Venkatraman, S., Abraham, A. & Paprzycki, M., Significance of Steganography on Data Security, Proceedings of the International Conference on Information Technology: Coding and Computing, 2004
4. Lee, Y.K. & Chen, L.H., High capacity image steganographic model, Visual Image SignalProcessing, 147:03, June 2000
5. Reference Guide: Graphics Technical Options and Decisions, http://www.devx.com/projectcool/Article/19997
6. Johnson, N.F. & Jajodia, S., Exploring Steganography: Seeing the Unseen, Computer Journal, February 1998
7. Bender, W., Gruhl, D., Morimoto, N. & Lu, A., Techniques for data hiding, IBM Systems Journal, Vol 35, 1996
8. Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., Information Hiding – A survey, Proceedings of the IEEE, 87:07, July 1999
9. Philip Bateman, Image Steganography and Steganalysis, August 2008
10. Marvel, L.M., Boncelet Jr

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.