International Journal of Research in Advent Technology, Vol.3, No.3, March 2015
E-ISSN: 2321-9637

A Survey on Steganography using Multimedia Files

P. Selvigrija (Assistant Professor)
Department of Computer Science and Engineering,
Christ College of Engineering and Technology, Puducherry, India
grijapst@gmail.com

E. Ramya (Student)
Department of Computer Science and Engineering,
Christ College of Engineering and Technology, Puducherry, India
ramya_0629@pec.edu

Abstract—Steganography is a type of secrete communication that hides the secrete information. It deals with the different ways of hiding/embedding the secrete information such as text, image, audio or video files inside another multimedia files with the help of private key. The hidden information is termed as secrete file and the file in which the secrete file is hidden is termed as cover file. The file represents the multimedia files such as text, image, audio or video. The obtained embedded file is said to be stego file. In this paper, the various steganographic techniques used for hiding the secrete file inside the cover file have been discussed.

Keywords—Steganography, Multimedia files, Cover file, Secrete file, Embedding.

I. INTRODUCTION

Steganography derives from the Greek word, “Steganos”, which means coated or secret, and, “Graphy” means that writing or drawing [1] [9]. On the best level, steganography is hidden writing, whether or not it consists of invisible ink on paper or copyright data hidden in an audio file. Today, steganography is most frequently related to information hidden with different information in an electronic file. This can be typically done by replacing that least necessary or most redundant bits of information within the original file [10]. Wherever Cryptography scrambles a message into a code to obscure its meaning, steganography hides the message entirely.

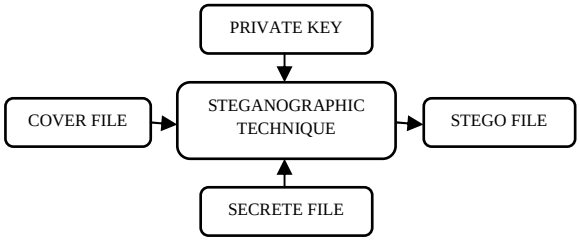

Fig.1. Block Diagram of Steganography

II. HISTORY OF STEGANOGRAPHY

Since man first started communication over written messages, the necessity for secrecy was in high demand. Within the past, messages may simply be intercepted and since there have been no secrecy devices; the third party was able to browse the message. This all modified throughout the time of the Greeks, around five hundred B.C., once Demaratus initial used the technique of Steganography. Steganography is that the use of activity a message thus it's sort of a message doesn't exist in any respect. Demaratus was a Greek national, lived in Persia as a result of he was banished from Balkan state. Whereas in Persia, he witnessed Xerxes, the leader of the Persians, build one in all the best service fleets the globe has ever far-famed. Xerxes was aiming to use this fleet to attack Balkan state during an onset. Demaratus still felt a love for his motherland and then determined he ought to warn Balkan state regarding the key attack. He knew it might be onerous to send the message over to Balkan state while not it being intercepted. This can be once he came up with the concept of employing a wax pill to cover his message. Demaratus knew that blank wax tablets can be sent to Balkan state while not anyone being the wiser. To cover his message, he scraped all the wax off from the pill exploits solely the wood from beneath. He then scraped his message into the wood and once he finished, recovered the wood with the wax. The wax coated his message and it gave the impression of it absolutely was simply a blank wax pill. Demaratus’ message was hidden and then he sent this to Balkan state. The hidden message was never discovered by the Persians and with success created it to Balkan state. Thanks to this message, Balkan state was able to defeat the incursive Persian force. The opposite techniques used for activity info in past day’s square measure clean-shaven head technique, clear ink technique and through coddled egg.

Pliny the Elder discovered that the “milk” of the thithymallus plant could easily be used as a transparent ink. If you wrote a message with the milk, it soon evaporated and left virtually no residue. It appeared as if the message completely erased. But

once the milk completely dried, and was heated, it would begin to char and turn a brown colour. So, this message could be written on anything that was not too flammable, which made it quite convenient. The reason it turned brown was because the milk was loaded with carbon and when carbon is heated, it tends to char.

Another technique used was the grille system. This technique involved strategically placing letters within a seemingly ordinary text. The secret message was sent and then the receiver was only able to see the secret message by using a special grille. The grille was just a slab of wood that would fit over the message. The slab had holes in it at the spots where the strategically placed letters would be. The letters would then spell out the secret message. This technique was effective due to the fact that the person trying to intercept the message would not be able to decode it unless they had the correct slab. This was also one of the major downfalls. Both parties needed to agree on the type of slab to use. To make it more secure, I am sure that one grille was not used very often. Not only did the parties have to agree on the right grille, but if the receiver's grille was lost or broken, the message again would be unreadable and thus useless.

III. RELATED WORKS

Kousik Dasgupta, J.K. Mandal and Paramartha Dutta [1] proposed a Hash based Least Significant Bit (LSB) technique for embedding secret information in the LSB of the cover frames. The eight bits of the secret information is divided into 3, 3 and 2 and embedded into RGB pixel values of the cover frames respectively. Then the hash function is used to select the position for inserting in the LSB bits. The Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Image Fidelity (IF) are measured.

Swathi .A and S.A.K. Jilani [2] used LSB technique for hiding information inside the cover video. Here the information will be embedded based on the stego key. Key is used in the form of polynomial equations with different coefficients. By using this, the capacity of embedding bits into the cover image can be increased.

Ronak Doshi, Pratik Jain and Lalit Gupta [3] provided a detailed explanation on different approaches towards implementation of Steganography using Multimedia files such as text, image, audio and video. They also explained the Steganalysis process. Steganalysis is the process of identifying the hidden message by an unauthorized person. Steganalysis process in Steganography is similar to Cryptanalysis process in Cryptography.

Rohit G Bal and Dr. P Ezhilarasu [4] used Ahadow Derivation and Quantization technique for hiding secrete information inside a vide file. They also proposed several solutions for colour image pixels that reveals the secrete image without loss and preserves the cover image using quantization.

Hamdy M Kelash, Osama F Abdel Wahab, Osama A. Elshakankiry and Hala S El-sayed [5] proposed a Steganography algorithm based on colour histograms for embedding data into video sequences directly. Their goal is to decrease the faded pixels in each frame in order to increase the embedding capacity.

Hemant Gupta and Setu Chaturvedi [6] proposed an advanced approach for dynamic data protection using LSB and hybrid approach. They proposed a method for replacing one or two or three LSB of each pixel in video frame and apply Advanced Encryption Standard (AES). They also performed calculations on PSNR and Correlation Factor for Original and embedded image.

Anwar H Ibrahim and Waleed M Ibrahim [7] proposed the existing Steganographic technique for hiding Text message in picture using Robet, Canny, Sobel, Perwitt and Log algorithms. The embedding is done by various techniques using Matlab. After analyzing the results they found that the canny method shows the better result in embedding and extraction in all the text given.

Krati vyas and B. L. Pal [8] proposed the LSB method that hides the secrete message based on searching about the identical bits between the secret messages and image pixels values. The proposed method was compared with the LSB benchmarking method directly in the least two significant bits of the image pixels.

Deepak Kumar Sharma and Astha Gautham [9] used Hash function method to hide data in video. They first separated the frames of video into RGB components and then used double hash function technique to select the pixel from row and column. They also used quadratic probing technique for solving the problem when collision occurs.

Vipula Madhukar Wajgade and Dr. Suresh Kumar [10] proposed a method for the data hiding which is based on video steganography. They have used the AES algorithm to make the steganography more secure and robust. They also used SHA – 1 for generating secrete key.

IV. TYPES OF STEGANOGRAPHIC TECHNIQUES

Secret data is hidden within all types of cover information. The subsequent formula provides a very generic description of the items of the steganographic process:

Cover medium + Hidden information + Stego key = Stego medium

In this context, the cover medium is that the file in which we are going to hide the hidden information, which can even be encrypted using the stego key. The resultant file is that the stego medium (which can, in fact be identical variety of file because the cover medium). There are four in which during which steganography has been implemented:

1. Text.
2. Images.
3. Audio files.
4. Video files.

1. Steganography in Text:

Steganography in text file are often done through the subsequent techniques:

i. Line-shift coding
ii. Word-shift coding
iii. Feature coding

i. Line-shift coding:

In this methodology, text lines are vertically shifted to encode the document unambiguously. Encoding and decoding will usually be applied either to the format file of a document, or the bitmap of a page image. By moving each second line of document either 1/300 of an inch up or down, it had been found that line-shift coding worked significantly well, and documents may still be fully decoded, even once the tenth photocopy.

However, this methodology is perhaps the foremost visible text coding technique to the reader. Also, line-shift encoding is often defeated by manual or automatic activity of the quantity of pixels between text baselines. Random or uniform re-spacing of the lines will harm any tries to decipher the codeword.

However, if a document is marked with line-shift coding, it's significantly tough to get rid of the encoding if the document is in paper format. Every page can have to be compelled to be rescanned, altered, and reprinted. This is often sophisticated even additional if the written document may be a photocopy, because it can then suffer from effects like blurring, and salt-and-pepper noise.

ii. Word shift coding:

In word-shift coding, code words are coded into a document by shifting the horizontal locations of words among text lines, whereas maintaining a natural spacing appearance. This encoding also can be applied to either the format file or the page image bitmap. The method, of course, is barely applicable to documents with variable spacing between adjacent words, like in documents that are text-justified. As a results of this variable spacing, it's necessary to possess the original image, or to a minimum of grasp the spacing between words within the un-encoded document.

The following may be a straightforward example of however word-shifting may work. For every text-line, the most important and smallest areas between words are found. To code a line, the most important spacing is reduced by an explicit quantity, and therefore the smallest is extended by identical quantity. This maintains the line length, and produces very little visible modification to the text. Word-shift coding ought to be less visible to the reader than line-shift coding, since the spacing between adjacent words on a line is commonly shifted to support text justification. However, word-shifting also can be detected and defeated, in either of two ways.

If one is aware of the rule utilized by the formatter for text justification, actual spaces between words may then be measured and compared to the formatter's expected spacing. The variations in spacing would reveal encoded information.

A second methodology is to require two or more clearly encoded, uncorrupted documents and perform page by page pixel-wise distinction operations on the page images. One may then quickly obtain word shifts and therefore the size of the word displacement. By replacing the shifted words back to the original spacing made under the formatter, or simply applying random horizontal shifts to any or all words within the document not found at column edges, an attacker may eliminate the encoding. However, it's felt that these ways would be long and careful.

iii. Feature coding:

A third methodology of coding information into text suggested is known as feature coding. This is often applied either to the bitmap image of a document, or to a format file. In feature coding, certain text options are altered, or not altered, depending on the codeword. As an example, one may encode bits into text by extending or shortening the

upward, vertical end lines of letters like b, d, h, etc. Generally, before encoding, feature randomization takes place. That is, character end line lengths would be randomly prolonged or shortened, then altered once more to encode the particular information. This removes the chance of visual decoding, because the original end line lengths wouldn't be well-known. Of course, to decode, one needs the original image, or at least a specification of the modification in pixels at a feature.

Due to the frequently high variety of options in documents which will be altered, feature coding supports a high quantity of information encoding. Also, feature encoding is essentially indiscernible to the reader. Finally, feature encoding is often applied on to image files that leave out the necessity for a format file. When making an attempt to attack a feature-coded document, it's fascinating that a strictly random adjustment of end line lengths isn't a very robust attack on this coding methodology. Feature coding is often defeated by adjusting every end line length to a set value. This could be done manually, however would be conscientious. Though this method is often machine-controlled, it can be created tougher by variable the actual feature to be encoded. To even additional complicate the difficulty, word shifting could be utilized in conjunction with feature coding, as an example. Efforts like this could place enough impediments within the attacker's way to build his job troublesome and long.

2. Steganography in Image:

The most common approaches to information concealing in images are:

i. Least significant Bit (LSB)
ii. Masking and Filtering

i. Least significant bit (LSB) insertion:

It is a standard, straightforward approach to embedding information in a very cover file. Sadly, it's vulnerable to even a small image manipulation. changing an image from a format like GIF or BMP, that reconstructs the original message specifically (lossless compression) to a JPEG, that doesn't (lossy compression), then back may destroy the data hidden within the LSBs. to cover a picture within the LSBs of every byte of a 24-bit image, you'll store 3 bits in every pixel. If you compress the message to be hidden before you embed it, you will hide an oversized quantity of data. To the human eye, the ensuing stego-image can look similar to the cover image. As an example, the letter A is often hidden in 3 pixels (assuming no compression). The original formation information for 3 pixels (9 bytes) could also be:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000011. Inserting the binary value for A within the 3 pixels would lead to:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The underlined bits are the only 3 actually modified within the eight bytes used. On average, LSB needs that solely 0.5 the bits in a picture be modified. We can hide information within the least and second LSB and still the human eye wouldn't be able to recognize it.

ii. Masking and filtering:

Masking and filtering techniques, typically restricted to 24-bit and gray-scale images, hide information by marking an image, in a very manner just like paper watermarks. Watermarking techniques could also be applied without concern of image destruction owing to lossy compression as a result of their additional integrated into the image. Visible watermarks don't seem to be steganography by definition. The distinction is primarily one in all intent. Ancient steganography conceals information; watermarks extend information and become an attribute of the cover image. Digital watermarks could embrace such information as copyright, license or ownership. In steganography, the item of communication is that the hidden message. In digital water-marks, the item of communication is that the cover.

3. Steganography in Audio Files:

Audio steganography embeds the secret message into the music files having formats. The different ways are:

i. LSB coding
ii. Phase coding
iii. Spread spectrum
iv. Parity coding
v. Echo hiding

i. LSB coding:

Least significant Bit (LSB) coding is that the easiest way to embed information in a very digital audio file. By substituting the least significant bit of every sampling purpose with a binary message, LSB coding permits for an oversized quantity of information to be encoded.

ii. Phase coding:

Phase coding addresses the disadvantages of the noise-inducing strategies of audio steganography. Phase coding depends on the very fact that the phase parts of sound aren't as perceptible to the human ear as noise is. Instead of introducing perturbations, the technique encodes the message bits as phase shifts within the phase spectrum of a digital signal, achieving an unperceivable encoding in terms of signal-to-perceived noise ratio.

iii. Spread spectrum:

In the context of audio steganography, the essential spread spectrum (SS) technique tries to spread secret information across the audio signal's frequency spectrum the maximum amount as attainable. This can be analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the complete sound file. However, in contrast to LSB coding, the SS technique spreads the secret message over the sound file's frequency spectrum, employing a code that's independent of the particular signal. As a result, the final signal occupies a bandwidth in way over what's really needed for transmission.

Two versions of SS will be employed in audio steganography: the direct-sequence and frequency-hopping schemes. In direct-sequence SS, the key message is displayed by a constant known as the chip rate and so modulated with a pseudorandom signal. It's then interleaved with the cover-signal. In frequency-hopping SS, the audio file's frequency spectrum is altered in order that it hops quickly between frequencies.

iv. Parity coding:

Instead of breaking a signal down into individual samples, the parity coding technique breaks a signal down into separate regions of samples and encodes every bit from the key message in a very sample region's parity bit. If the parity bit of a specific region doesn't match the key bit to be encoded, the method flips the LSB of 1 of the samples within the region. Thus, the sender has a lot of an alternative in encoding the secret bit, and also the signal are often modified in a very additional unnoticeable fashion.

v. Echo hiding:

In echo hiding, data is embedded in a very sound file by introducing an echo into the discrete signal. Just like the spread spectrum methodology, it too provides benefits in that it permits for a high information transmission rate and provides superior strength in comparison to the noise causing strategies.

To hide the information with success, three parameters of the echo are varied: amplitude, decay rate, and offset (delay time) from the original signal. All three parameters are set below the human hearing threshold that the echo isn't simply resolved. Additionally, offset is varied to represent the binary message to be encoded. One offset value represents a binary one, and a second offset value represents a binary zero.

4. Steganography in Video files:

Video Steganography may be a technique to cover any kind of files in any extension into a carrying Video file. The use of the video based steganography is more eligible than totally different transmission files because of its size and memory needs. Videos are the set of images. Video is the electronic medium for the recording, repetition and broadcasting of moving visual pictures. The typical variety of still pictures per unit of your time of video is twenty four frames per second.

V. CONCLUSION

Though Steganography isn't enforced in wider ways in which however it can be the most effective security tool. the most drawback of today's world is to secure their information confidentially; the techniques used presently aren't thought of the most effective which may solely get replaced by Steganography.The various techniques have been discussed for hiding the multimedia files in another multimedia files such as text, image, audio or video files. These techniques provide security to the secret files in different ways. The intruders will feel difficult to guess which technique has been used for hiding one file inside another file.

REFERENCES

[1] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB"), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[2] A. Swathi and Dr. S.A.K. Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal of Computational Engineering Research (IJCER), Vol. 2, Issue 5, September 2012.

[3] Ronak Doshi, Pratik Jain and Lalit Gupta, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 6, November-December 2012.

[4] Rohit G Bal and Dr. P. Ezhilarasu, "An Efficient Safe and Secured Video Steganography using Shadow Derivation", International Journal of

Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.

[5] Hamdy M. Kelash, Osama F. Abdel Wahab, Osama A. Elshakankiry and Hala S. El-sayed, "Utilization of Steganographic Techniques in Video Sequences", International Journal of Computing and Network Technology, Sys. 2, No. 1 Pg. 17-24, January 2014.

[6] Hemant Gupta and Setu Chaturvedi, "Video Steganography through LSB Based Hybrid Approach", International Journal of Computer Science and Network Security, Vol. 14, No. 3, March 2014.

[7] Anwar H. Ibrahim and Waleed M. Ibrahim, "Text Hidden in Picture Using Steganography: Algorithms and Implications for Phase Embedding and Extraction Time", International Journal of Information Technology & Computer Science (IJITCS), Vol. 7, No. 3, February 2013.

[8] Krati vyas and B. L. Pal, "A Proposed Method in Image Steganography to improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 3, Issue 1, January 2014.

[9] Deepak Kumar Sharma and Astha Gautam, "An Approach to hide Data in Video using Steganography", International Journal of Research in Engineering and Technology (IJRET), Vol. 3, Issue 4, April 2014.

[10] Vipula Madhukar Wajgade and Dr. Suresh Kumar, "Enhancing Data Security using Video Steganography", International Journal of Emerging Technology and Advanced Engineering (IJETAC), Vol. 3, Issue 4, April 2013.