AN OVERVIEW OF HIDING INFORMATION USING STEGANOGRAPHY METHODS WITH CRYPTOGRAPHY

Maheshwari A[1*], Padma S[1], Shrivastava D P[2], Dimitrios A. Karras[3], Phyu Phyu Khaing[4]

[1]Department of Computer Applications, K.S.Rangasamy college of Arts and Science College, Tiruchengode, India.

[2]Higher Colleges of Technology UAE.

[3]National and Kapodistrian University of Athens, Greece.

[4]University of Computer Studies, Mandalay, Myanmar.

ABSTRACT:

The art of hiding a secret message and transmitted to a receiver known as Steganography. So, that eavesdropper cannot find the content of message. The main aim of Steganography is unauthorized person cannot access the message. So, the information can be transmitted from sender to receiver without any detection by hackers. Cryptography technique in which plaintext is encrypted to the ciphertext. The original text encrypted to an unreadable format that cannot be accessed by normal users. Steganography used along with cryptography to enhance privacy in transmitting data. In this paper, several Steganographic techniques were discussed. Steganography technique includes text, image, audio, and video.

Text Steganography, in this technique the secret message that has to be sent is hidden inside another cover text file. The hidden text file is transmitted from sender to receiver. Image steganography, commonly used technique in which the image or a message hidden inside another cover image by altering some color change in the image using LSB(Least Significant Bit) and transmitted from sender to receiver ,difficult for human eye to detect those changes. Audio Steganography, in this technique the secret message or audio that has to be sent is hidden inside another cover audio file and transmitted from sender to receiver. Video Steganography, secret message or video that has to be sent is hidden inside another cover video file and transmitted from sender to receiver.

Keywords: Steganography, Crptography, Secret message, plaintext, ciphertext.

INTRODUCTION:

Today security is needed for internet applications to transmit the data. Data security is provided through Steganography and Cryptography. Steganography and cryptography used simultaneously to secure data which implement more privacy in sending data.[Pratiksha Sheti,V.Kapoor].The greek word "Stegno" means cover and graphia means "writing". So, Steganography which is known as "covered writing"[1]. Steganography and Crptography seem similar. Cryptography means "Secret writing" converts a text to an unreadable format so that it cannot be read by the normal user. Steganography, the secret message that has to be transmitted is hidden inside text, image, audio and video. So, that hackers cannot find them easily.[Pratiksha Sheti,V.Kapoor].When a hacker tries to find the secret message by breaking the steganographic technique it is useless for them because before using Steganographic technique the message were encrypted using Cryptography[2]. AES Algorithm used to encrypt the message [Pratiksha Sheti,V.Kapoor].

Steganography consist of two materials, message and the carrier. Secret data to be hidden known as message and the material are the mode that is used to send the message known as carrier [3]. Various types of Steganographic methods were available. In this paper we were going to discuss about some of the Steganographic techniques.Fig.1 depicts the categories of Steganographic techniques [4].

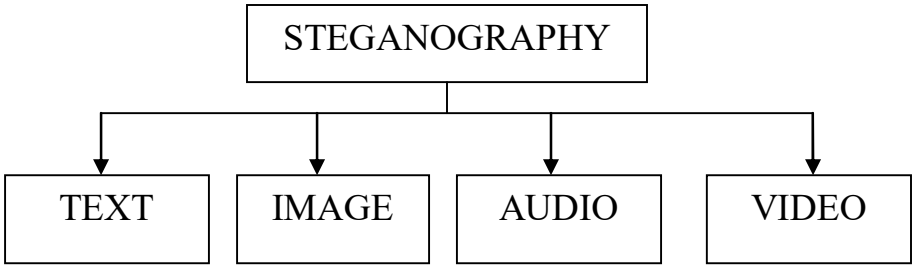

Fig.1 Categories of Steganographic techniques

STEGANOGRAPHIC TECHNIQUES:

Initially the text is encrypted using Crptography. AES [Advanced Encryption Standard] Algorithm with 128 bit, used to encrypt the text [5] then Steganographic techniques were applied on the text.

1. TEXT STEGANOGRAPHY:

Text format altering or altering only certain characteristics of text elements, Steganography can be achieved. The main aim of the technique is to use encoding methods that are used to develop alterations they were reliably decodable but difficult to read by a normal reader. Reliable decoding and minimum visible change becomes conflicting. Sometimes, it becomes challenge in designing a document marking techniques. Document content and page layout were described by a computer file which is a document format file, using standard format description language such as Tex, @off etc. From this format file text that has been generated [5]. Different approaches of text Steganograph were illustrated with three techniques other than forms an exhaustive list of document masking technique. These three can be used separately or used jointly. Each technique has its advantage.

A. Line-Shift coding:

To encode the document, the position of the text lines was shifted vertically for altering the document. The technique of encoding can applied to the format file or bitmap of page image. The code that is embedded may be derived from bitmap or format file. The decoding may be done without the original image which has uniform line spacing between lines within a paragraph.

B. Word-Shift coding:

To encode the document, the position of the text line was shifted horizontally for altering the document, in a specific order. In this technique encoding may be applied to a format file or bitmap of page image. In the format file or bitmap file decoding is applied. This technique is useful only if the document that have different space between adjacent words. Varying space in the document is used when the document has justification in whitespace. Due to this varying size, decoding requires the original message spacing requires in an un-encoded document.

C. Feature Encoding:

Format file or a bitmap image document, this coding technique is applied. Depending on the codeword the image is examined for chosen text features with the features altered, or not altered. The original message required for decoding or important features of the pixel is needed. Numerous text features were available here we use the text to be alter upward, vertical endlines- that is the top of letters, b, d, h, etc. Endlines

were altered by shortening or extending their length to one or more pixel but the endline feature is not changed [6].

Another form of text Steganography defined by Chapman et al. In this method natural language is used to write and cover the secret message [7].

2. IMAGE STEGANOGRAHY:

Nowadays messages or image hidden inside another cover image becomes popular technique. In newsgroup or World Wide Web images with secret messages can be spread easily. German Steganographic expert Niles Niels provos, researched the use of steganography in newsgroup, detects the hidden message inside the image that were posted on the web by creating a scanning cluster. After checking one million images, but no hidden message were found. So, the use of Steganographic technique seem to be limited.

Without modifying the visible properties of the image, the message can be hidden by altering the "noisy" areas with many color variations. LSB (Least Significant Bit) used to make alterations in the image. Cover image has been taken as a source and it is masked, filtered and transformed. On the different type of image file these technique can be used in different degree for successful alteration.

A. Least Significant Bit:

Least Significant Bit (LSB) is a simple approach for embedding message in a cover image. In the deterministic sequence, this simplest Steganography technique used to embed the bits of a message directly into a least significant bit plane of a cover image. Amplitude of change seem to be small when modulating the least significant bit, it does not results in a human-perceptible difference [8].A proper cover image is necessary to hide a secret message into it. The reason is there is a chance of information loss while hiding the message in a image as stated by loss compression algorithm. When we use a 24-bit color image 3 bit can be used to store in each pixel of red, green and blue color.

Consider an example, the grid has3 pixels of 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)
(11001000 00100111 11101001)
The results shown below when the character A with binary value 10000001,is inserted in the above grid.
(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

In this example, there is need to change only three bits to insert a new character successfully. In a maximum cover size of an image only half of the bits have to be changed to hide a message as an average. Human visual system (HVS) cannot recognize this small modification made to the least significant bit. So, the message can be hidden effectively [2].

Least significant bit of third color remains without any change. Correctness of 8 bits which were embedded in these pixels can be used for checking. Also be known as "Parity Bit".

B. Masking and Filtering:

It takes a different approach to hide image usually it is restricted to 24-bit or greyscale image. This technique is similar to Paper Water Mark; it creates a marking in a image. For example the parts of image were modified by luminance. Visible properties of the image can be changed by masking but in a way the human eye cannot notice the anomalies. Masking use the visible aspects of image, it is robust than LSB modifications in order with compression, cropping and also includes different types of image processing. Images were embedded inside the visible parts of an image but at the "noise" level, makes it to be more suitable than LSB modification when compression algorithm like were JPEG used [2].

C. Transformation:

Discrete Cosine transformation is a more complex way of hiding a secret message inside a message. In JPEG Compression algorithm, to transform successive 8*8 pixel block of image into 64 DCT coefficients. Discrete Cosine Transformation (DST) is used. The following pseudo algorithm used for transformation [2].

Input: message, cover image
Output: Steganographic image containing the message.
while data left to embed do
  get next DCT coefficient from cover image
  if DCT 6=0 and DCT 6=1 then

get next LSB from message
replace DCT LSB with message bit
end if
insert DCT into Steganographic image
end while

3. AUDIO STEGANOGRAPHY:

In a corresponding audio file secret message is embedded into a digitized audio signal which results in slight modification of a binary sequence in the audio. Number of audio Steganographic techniques were available here a brief introduction for some of them were given.

A. LSB Coding:

Quantification technique used after sampling technique used to convert analogy signals into a digital binary sequence. Binary sequence of LSB in each sample of digitized audio file is replaced with binary equivalent of the secret message to be hidden in this technique.

B. Phase Coding:

Phase change in audio signal cannot recognized by Human Auditory System (HAS) as it is easy to recognize noise in the signal. This fact is exploited by the phase coding method. Secret message bit is encoded as phase shifts in phase spectrum of digital signal. Inaudible encoding is achieved through Signal-to-noise ratio.

C. Spread Spectrum:

In this technique two approaches were used

1. Direct Sequence Spread Spectrum (DSSS)
2. Frequency Hopping Spread Spectrum (FHSS)

In telecommunication, DSSS technique is used as modulation technique. Because with other spectrum the transmitted signal takes up more bandwidth than a information signal that is modulated. It multiplies the data that is being transmitted by a “noise” signal [9].

D. Echo hiding:

In this technique the secret message that is embedded into a cover audio signal as “echo”. Amplitude, decay rate and offset are the three parameters of echo cover signal. These parameters were used to represent the message from original signal that is varied to represent encoded secret binary message. Those signals were set below the threshold value of Human Auditory System (HAS). So, it is not easily recognized by human.

4. VEDIO STEGANOGRAPHY:

Images, sounds were embedded into a video file. Message can be hidden inside another cover video file [10]. In this video Steganography technique sender sends the video to the receiver by embedding secret message into it. “Keys” were used as optional while sending those video to the receiver. The secret key can send to the receiver to resolve the hidden message.

CONCLUSION:

Various Steganographic techniques were discussed. From all those technique Image Steganography is commonly used technique. Text Steganography in which scarcity of text files limits its usage. Audio Steganography in this technique it is possible for a normal user to find any change in the audio. Video Steganography and Image Steganography were used to encrypt decrypt the original message.

REFERNCES:

1. Sara Khosravi, Mashallah Abbasi Dezfoli, Mohammad Hossein Yektaie, A new steganography method based HIOP (Higher Intensity Of Pixel)algorithm and Strassen's matrix multiplication, Journal of Global Research in Computer Science, Vol. 2, No. 1, 2011.
2. Robert Krenn, Steganography and steganalysis, Internet Publication, March 2004. Available at: http://www.krenn.nl/univ/cry/steg/article.pdf
3. Christian Cachin, Digital Steganography, Encyclopedia of Cryptography and Security, 2005.
4. Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, Data Hiding Through Multi Level Steganography and SSCE, Journal of Global
5. Prathiksha sethi, V.Kapoor, A Proposed Novel Architecture for Information Hiding in Image steganography by using Genetic Algorithm and Cryptography, Procedia Computer Science 87(2016) 61-66.
6. J.T. Brassil, S. Low, N.F. Maxemchuk, and L. O’Gorman, "Electronic Marking and Identification Techniques to Discourage Document

7. M.Chapman, G. Davida, and M. Rennhard, “A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography”,Proceedings of the Information Security Conference, October 2001, pp. 156-165.
8. Mohamed Amin, Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd Rozi (2003) Information hiding using steganography Project Report. Available at: http://eprints.utm.my/4339/1/71847.pdf
9. Direct-sequence spread spectrum (DSSS), Frequency-hopping spread spectrum (FHSS) Wikipedia, the free encyclopedia, GNU Free Documentation License http://en.wikipedia.org/wiki/Frequencyhopping_spread_spectrum.
10. Yadav, Pooja, Nishchol Mishra, and Sanjeev Sharma. "A secure video steganography with encryption based on LSB technique." In 2013 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-5. IEEE, 2013.