Steganography Techniques: A Review

Mr.Pravin R. Kamble
Department Of Computer Science & Engineering
Sanjeevan Engineering & Technology Institute,
Panhala, Kolhapur,MS, India, Pin-416201

Mr.Prakash S. Waghamode
Department Of Computer Science & Engineering
Sanjeevan Engineering & Technology Institute,
Panhala, Kolhapur,MS, India, Pin-416201

Mr.Vilas S Gaikwad
Department Of Computer Science & Engineering
Sanjeevan Engineering & Technology Institute,
Panhala, Kolhapur,MS, India, Pin-416201

Mr.Ganesh B. Hogade
Department Of Computer Science & Engineering
Sanjeevan Engineering & Technology Institute,
Panhala, Kolhapur,MS, India, Pin-416201

***Abstract*- Steganography is a useful technique for hiding data behind the carrier file such as image, audio, video etc. and that data securely transfer from sender to receiver. The cryptography is also another technique which is used for the protecting information. The Combining encryption methods of cryptography and steganography enables the user to transmit information which is masked inside of a file in plain view. This will provide more security to transferring data.**

This paper provides a general overview of Steganography techniques in which Text, Image Audio and Video Medias used for the information hiding behind channels. Also the Cryptography will be applied on the information for the better security.

Keywords: Image Steganography, Audio Steganography, Video Steganography, Spatial domain and Transform domain.

I. INTRODUCTION

The Steganography is an ancient art of hiding information. It refers to the science of “invisible” communication. The cryptography is used for secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer.

The process of steganography technique can be defined into 4 categories such as Text, Image, Audio and Video. In text steganography text files are used to hide data. Here in this system the confidential data can be of any format like text, audio, video or image. The cover is a file in which the data is hidden is at ext file.Technique used to achieve confidentiality is LSB (Least Significant Bit) i.e. modifying least significant bit of the cover file. In image steganography image files like Bit Map Picture (BMP), PNG (Portable Network Graphics), JPEG (Joint Picture Expert Group), TIFF (Tagged Image File Format) etc. are used to hide data. Technique used to achieve confidentiality are LSB (Least Significant Bit), spread spectrum etc. In audio steganography sound files like AVI (Audio Video Interleaved), MPEG (Moving Picture Expert Group), FLV (Flash Video) etc. are used to hide data. Techniques used to achieve confidentiality are LSB, spread spectrum etc. The best format is wave format since the reading of the bits of data is easier in wave file, also the compression is good in wave files and the distortion of data is very less in wave files. In video steganography video files like AVI, MVI, DAT etc. are used to hide data. Techniques used to achieve confidentiality are LSB, spread spectrum, ecliptic curve method etc. It is worth to mention that the major role in 9/11’s bomb blast in United State (US) played through the use of video steganography.

II. TYPES OF STEGANOGRAPHY

A. IMAGE STEGANOGRAPHY

The image steganography is used to hide a secret message inside an image. The most widely used technique to hide secret bit inside the LSB [2] of the cover image. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24 bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel [16] in this way we can use more secret bit to hide dat in it.

In image steganography image files like BMP, PNG, JPEG, TIFF, GIF etc. are used to hide data. Technique used to achieve confidentiality is LSB, spread spectrum etc. In Spatial Domain Embedding steganography algorithm [6] is based on modifying the least significant bit layer of images. This technique makes use of the fact that the least significant bits in an image could be thought of random noise and changes to them would not have any effect on the image. The message bits are permuted before embedding, this has the effect of distributing the bits evenly, thus on average only half of the LSB will be modified. Popular steganographic tools based on LSB embedding vary in their approach for hiding information. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or instead of just changing the last bit they increment or decrement the pixel value.

Another category of steganography techniques is Transform Domain technique in which a number of algorithms have been proposed [5]. Transform Domain Methods hide messages in significant areas of cover image which makes them more robust to attacks, such as compression, cropping, and some image processing, than the LSB approach. Most of the work in this category has been concentrated on making use of redundancies in the DCT (Discrete Cosine Transform) domain, which is used in JPEG compression. But there have been other algorithms which make use of other transform domains such as the frequency domain. Embedding in DCT domain [6] is simply done by altering the DCT coefficients, for example by changing the least significant bit of each coefficient. One of the constraints of embedding in DCT domain is that many of the 64 coefficients are equal to zero, and changing to many zeros to non-zeros values will have an effect on the compression rate. That is why the number of bit one could embed in DCT domain, is less that the number of bits one could embed by the LSB method. Also the embedding capacity becomes dependent on the image type used in the case of DCT embedding, since de- pending on the texture of image the number of non-zero DCT coefficients will vary.

B. AUDIO STEGANOGRAPHY

The sender embeds secret data of any type using a key in a digital cover file to produce a stego file, in such a way that an observer cannot detect the existence of the hidden message. Fig.2 shows at the other end, the receiver processes the received stego-file to extract the hidden message [13]. This flow diagram is same for image/video steganography except cover media.

In many schemes a method of audio steganography based on modification of least significant bits (LSB) the audio samples in the temporal domain or transform domain have been proposed. Some of these methods employ LSB technique and combine it with other techniques such as error diffusion, minimum error replacement (MER) and temporal masking effect. Another method embeds covert messages in the LSB of wavelet transform and recently in the integer transform. The main objectives of the LSB based schemes are to raise payload or the maximum amount of the information to be embedded and to prevent audio quality degradation. The best format is wave format since the reading of the bits of data is easier in wave file, also the compression is good in wave files and the distortion of data is very less in wave files. There are many methods in audio steganography some of them discussed as below.

Using LSB coding technique the modification in least- significant bit is possible, as modifications will usually not create audible changes to the sounds [3]. Another method involves taking advantage of human limitations. It is possible to encode messages using frequencies that are inaudible. Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion [16]. In Phase coding technique the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. The basic Spread Spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. The SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal.

C. VIDEO STEGANOGRAPHY

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. The video steganography is nothing but a combination of image and audio steganography [13].

III. LITRATURE SURVEY

Chan and Cheng (2003) [1] proposed the hiding data in images by simple LSB Substitution method. In that paper optimal pixel adjustment process (OPAP) is used for the enhancing the Stego image quality obtained by the simple LSB substitution method. OPAP is used for the checking the embedding error between original image and Stego image. This method applied on grayscale images in which 2-4 bits of original cover image pixels are used for the secret data bits embedding. The quality of image calculated from the PSNR of the image.

Zlii, Yang and Xian (2003) [2] has proposed LSB Steganography Detection Algorithm Gradient Energy-Flipping Rate detection (CEFR). From the analysis of the variation of the gradient energy, LSB Steganography in color and grayscale image, the secret message embedded in the target image is detected, and the length of the embedded message is estimated. This method conclude that when embedding rate>0.05 bits per pixel, detect the presence of secret message and the embedding length estimation error is constraint within 10%. This method applied on spatial LSB domain steganography.

Sutaone and Khandare (2004) [3] has proposed random insertion LSB for image Steganography. This method convert message in to ASCII binary equivalent and spread out the message in to the carrier image seemingly random manner with the external secrete key. This method also provides both Steganography and cryptography together.

Ru, Zhang, Huang (2005) [4] proposed a steganographic tool Steghide which is useful for detecting messages hidden in WAV files. In this paper a linear predictor was used for the magnitude of wavelet sub band coefficients to extract significant statistics features, and employing support vector machines to detect the existence of hidden messages. Wavelet decomposition used to analyze the signals on multi resolution. Linear predictor used to capture the faint changes of relation between neighbor samples caused by embedding.

Mohammad Shirali-Shahreza and M. Hassan Shirali-Shahreza (2007) [5] this paper introduce Text steganography concept which offers a new method for secret exchange of information through SMS by using and developing abbreviation text steganography. This method applies on Nokia- N71 mobile phone. The cryptography is also used for the sending encrypted message. The SMS-Texting language is a combination of abbreviated words used in SMS. This algorithm uses the full word for hiding bit 0 and the abbreviated form for hiding bit 1.This method can also use on other devices such as Pocket PC and PDA's. Also this method can be implemented on desktop PCs using SMS gateway for sending and receiving SMS messages. A small amount of information can be hidden in this method.

Pooyan and Delforouzi (2007) [6] proposed LSB-based Audio Steganography Method Based on Lifting Wavelet Transform. The encrypted covert data is embedded into the wavelet coefficients of host audio signal. They calculate hearing threshold in wavelet domain. Then according to this threshold data bits are embedded in the least significant bits of lifting wavelet technique is reformed to increase the robustness coefficients. Inverse lifting wavelet transform is applied to modified coefficients to construct stego signal in time domain. Haar wavelet transform was used.

Yang, Weng, Wang (2008) [7] proposed the new adaptive LSB technique using Pixel Value differencing with spatial LSB domain technique. It gives high embedding capacity and imperceptible Stego image. This method is used to distinguish between edge areas and smooth areas. The edge areas are used for the higher embedding capacity for data hiding .This technique comes under the spatial domain image processing and this method applied on grayscale images. The quality of stegoimages calculated from the peak signal to noise ratio (PSNR).

Kim, Jung and Yoo (2008) [8] proposed A high capacity data hiding using PVD and LSB Replacement Method. This method calculates the difference value between two consecutive pixels. The LSB substitution method is used when the difference value is small (i.e smooth areas) and PVD is used when it is large (i.e edge areas) of cover image pixels. The pixels belong to the edge areas could embed more data than the smooth area of image thus LSB substitution is used to embed more data on smooth area without distortion to the human visual system. This method is useful for the grayscale images.

Garay, Medina, Rivera and Ponomaryov (2008) [9] proposed a steganographic communication channel using mp3 and wave audio signals. It uses Direct Sequence Spread Spectrum (DSSS) to insert confidential information in MP3 and WAV audio digital signals. Filtering, re-sampling, noise addition, echo addition and MPEG compression were used to evaluate the proposed algorithm.

Bhattacharya, Das, Bandopadhya and Kim (2009) [10] proposed a security model for the Text steganography. The model combines cryptography, steganography and along with that an extra layer of security has been imposed in between them. This extra layer of security changes the format of normal encrypted message and the security layer followed by it embeds the encrypted message behind a multimedia cover object. It gives privacy and secrecy by using cryptography and steganography resp. Two secret keys are used. This algorithm is useful for the color images, audio and video covers Medias.

Yang, Sun and Guang Sun (2009) [11] proposed a high capacity data hiding scheme using adaptive LSB substitution technique. This technique focuses on to avoid abrupt changes in image edge areas, as well as to achieve better quality of the Stego-image. This scheme exploits the brightness, edges, and texture masking of the host image to estimate the number k of LSBs for data hiding. The method proposed a human visual system (HVS) and LSB substitution, which obeys the concept that the edges cannot tolerate great change. The method was applied on the 512 × 512 grayscale image.

Bhaumik, Choi, Robles, and Balitanas (2009) [12] proposed a data hiding and extraction procedure for high resolution Audio Video Interleave (avi) videos. The main intention of this method is to provide proper protection on data during transmission. Accuracy of the correct message output that extract from source can estimated by using tools for comparison and statistical analysis.

Elsadig, Kiah, Zaidan and Zaidan (2009) [13] proposed LSB insertion method on video images or frames. This method considers the digital image file as separate frames and changing the output image displayed on each video frame by hidden data that does not visually change the image. The result was successful on extracted set of video frames.

Dao, Bai and Yu (2009) [14] proposed A High Bit rate Information Hiding Algorithm for Video in Video. Experimental result shows that the host video which is embedded numerous auxiliary information have little visually quality decline. Peak Signal to Noise Ratio (PSNR) of host video only degrades 0.22dB in average, while the hidden information has a high percentage of survives and keeps a high robustness in H.264/AVC compression, the average Bit Error Rate (BER) of hiding information is 0.015%. This technique will be very useful in captioning, picture-in-video, speech-in-video etc. it enhances the efficiency of multimedia information.

Mozo, Obien, Rigor, Rayel, Chua and Tangonan (2009) [15] proposed a Video Steganography using FLV. In this method FLV file extension used because of its simple file structure, its relatively small size compared to other video file formats, and its popularity in video-hosting websites. The FLV file size changes when a file is hidden but the picture and sound quality of the FLV with the embedded data is perfectly maintained. This would allow doctors and medical personnel to embed multiple medical records such as electrocardiogram signals, ultrasound files, medical prescriptions, urinalysis, and many more medical files into a single video file (flv).

Kim,Cheng and Young Yoo (2009) [16] proposed A New Steganography Scheme based on an Index-color Image. This method first divides the secret data into several parts based on the number of colors in the cover image, and then embeds secret data into the cover image. The cover image can be recovered easily without loss. This technique can be applied to BMP, gif and PNG image formats which use the index-color technique.

Luo, Huang and Jiwu Huang (2010) [17] proposed edge based LSB Matching Revisited image steganography algorithm. In that embedding region selected from the size of the secret message and the difference between two consecutive pixels in the cover image. Lower embedding rates, only sharper edge regions are used while keeping the other smoother regions as they are. This algorithm applied on grayscale images which gives higher visual quality and better security. This method will be applied on audio/video steganography in the spatial or frequency domains.

Nikoukar (2010) [18] proposed an Image steganography Method Based on RGB (Red/Green/Blue) color Image. In this technique BMP file format images are used which performs least variations in the cover images. Every pixel in BMP file contain 24bits - R, G, B channels in which one is pixel indicator and remaining two are used to hide the data. Secret key and randomization technique are used for selection of number of bits used and color channel that are used. Data detection is more difficult than the previous technique.

Wei, Guo and Wang (2010) [19] proposed method on Advanced Audio Coding (AAC) and MPEG-2 and MPEG-4 the audio format are used. Encryption takes place on hidden data and then encoded into AAC bit stream. This method use Huffman and differential coding for encoding each bit of the hidden data as the parity of the number of bits. AAC is a lossy compression encoding scheme for digital audio, which achieves better sound quality than MP3 at the same bit rate.

Djebbar, Ayad, Hamam and Meraim (2011) [20] proposed A perfect audio Steganographic technique aim at embedding data in an imperceptible, robust and secure way and then extracting it by authorized people. This paper presents a review of the current state of art literature in digital audio steganography techniques and approaches. The Audio steganography methods Low bit encoding, Echo hiding, Magnitude spectrum, Phase spectrum, Tone insertion, Spread spectrum, Cepstral domain, Wavelet coefficients, Codebook Modification, Bit stream hiding etc. was introduced.

Gadicha1 (2011) [21] proposed audio wave steganography method that reduces embedding distortion of the host audio and message bits are embedded into 4th LSB layers, resulting in increased robustness against noise addition. This method introduces smaller error during watermark embedding. If the 4th LSB layer is used, the absolute error value ranges from 1 to 4 Quantization Signal, while the standard method in the same conditions causes constant absolute error of 8 Quantization Signal. LSB coding method introduced the average power of noise is smaller i.e. 9.31db.

The table 1 shows the various methods of steganography applied on text, image, audio and video carriers. Some methods used cryptography concept for security. In recent research of steganographic techniques tells us that there are lots of methods was invented which is related with audio/video steganography. Video steganography are more useful than image and audio steganography because all algorithms of image and audio steganography can be applied on video.

Table 1. Steganography Methods

Steganography Methods	Additional Cryptography	Carrier Format	Message supported	Authors
LSB Substitution	No	Grayscale image	Text	Chan and Cheng (2003)
Random insertion LSB	Yes	Grayscale image	Text	Zlii, Yang and Xian (2004)
Text steganography	Yes	SMS	Text	Shahreza and Shahreza (2007)
LSB-based Audio Steganography	No	Audio signal	Text	Pooyan, Delforouzi (2007)
Spatial LSB domain technique	No	Grayscale image	Text	Yang, Weng, Wang and Sun (2008)
PVD and LSB Replacement Method	No	Grayscale image	Text	Kim, Jung and Yoo (2008)
Audio Steganography	No	Using MP3 and WAV audio signals	Text	Garay, Medina, Rivera and Ponomaryov (2008)
Text steganography	Yes	Color image (audio/video)	Text	Bhattacharya, Das Bandyopadhyay and Kim (2009)
adaptive LSB substitution	No	Grayscale image	Text	Yang, Sun and Sun (2009)
Video steganography	No	AVI videos	Text	Bhaumik, Choi, Robles and Balitanas (2009)
LSB insertion method on video images	No	Video file	Video files	Kiah , Zaidan and Zaidan (2009)
Video in video steganography	No	Video file	Video file	Dao, Bai and Yu (2009)

Video steganography	No	FLV file	Text	Mozo, Obien, Rigor, Rayel, Chua and Tangonan (2009)
LSB Matching Revisited	No	Grayscale image	Text	Luo, Huang and Huang (2010)
Image steganography	Yes	RGB color Image	Text	Nikoukar (2010)
Audio steganography	No	Advanced Audio Coding (AAC), MPEG-2, MPEG-4	Text	Wei, Guo and Wang (2010)
Audio wave steganography	No	Audio/ Video	Text	Gadichal (2011)

IV. DISCUSSION AND RESEARCH SCOPE

After reviewing the various papers in area of steganography it is found that -

It is observed that most of the Steganography techniques are suitable to hide text as massage only and not able to hide any binary message. Many image Steganography techniques are only for gray scale images but not applicable for color image. In comparison with video and audio as carrier, there are many Steganography techniques for image but very few are for audio and video. Image Steganography techniques are used for video Steganography but there is need of performance improvement in term of security, hiding capacity, visual quality and attack analysis. The video and audio steganography are good for storing large amount of message than other Steganography techniques.

Spatial domain Steganography techniques are easy for attacks so they need to combine with external security such as cryptography. Some Spatial Domain Steganography techniques are based on secret key so secrecy of key is required to provide externally. There is a research scope in making image, audio and video steganography techniques parallel to improve their embedding and extraction processes speedy. Particularly in image and video there is more scope to do a parallelism and also improve hiding capacity. At the same time, attack analysis process should also parallelize to minimize the time of steganalysis.

V. CONLUSION

Paper present the review of all existing steganographic methods for data hiding inside the text, image, audio and video channels. Some steganographic methods need to improve security by using cryptography against attacks. Image and audio steganography both techniques are useful for the video stegnography to increase the hiding capacity of secure data inside the carrier fie. The parallelization of steganography technique is an important task in steganographic area to increase the processing speed of the steganoghraphic algorithm.

The various steganographic techniques such as image, audio and video steganography need to be focused on hiding capacity, detectability, Level of Visibility and robustness against malicious and unintentional attacks.

ACKNOWLEDGMENT

We express our sincere thanks to the all authors, whose papers in the area of Steganography.

REFERENCES

[1] Chan K. C, Cheng L. M (2003), "hiding data in images in simple LSB substitution", Journal of pattern recognition, pp.469-474.

[2] Zlii Li,Yang S. A. F. , Xian Y (2003)," A LSB Steganography Detection Algorithm", The 14th IEEE 2003 International Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings.pp.2780-2783.

[3] Sutaone M. S. and Khandare M. V. (2004) ,"Image Based Steganography Using LSB Insertion Technique", pp.146-151.

[4] Ru X. M, Zhang H. J, Huang X (2005), "Steganalysis Of Audio: Attacking The Steghide", Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, pp.3937-3942, pp.18-21.

[5] Shahreza M. S and Shahreza M. H. S (2007) ,"Text Steganography in SMS", International Conference on Convergence Information Technology, pp.2260-2265.

[6] Pooyan M, Delforouzi A (2007) , "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", 2007 IEEE International Symposium on Signal Processing and information technology, pp.600-603.

[7] Yang C. H, Weng C. Y, Wang S. J and Sun H. M (2008), "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497.

[8] Kim K. J, Jung K. H and Yoo K. Y (2008) , "A high capacity data hiding method using PVD and LSB replacement",International Conference on Computer Science and Software Engineering, pp.876-879.

[9] Garay S. H, Medina R. V, Rivera L. V and Ponomaryov V (2008), "Steganographic Communication Channel Using Audio Signals" ,12th International Conference on Mathematical Methods in Electromagnetic Theory, pp.427-429.

[10] Bhattacharya D, Das P, Bandyopadhyay S. K., Kim T (2009) ,"Text Steganography: A Novel Approach ", International Journal of Advance Science and Technology,Vol.3, pp.79-86.

[11] Yang H ,Sun X, Sun G (2009), "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution" Radio Engineering, Vol. 18, No. 4, pp. 509-516.

[12] Bhaumik A. K, Choi M, Robles R. J and Balitanas M. O (2009) , "Data Hiding in Video", International Journal of Database Theory and Application Vol. 2, No. 2, pp.9-16.

[13] Kiah E ,Zaidan B. B and Zaidan A. A (2009) , "High rate video streaming steganography", International Conference on Information Management and Engineering, pp.550-554.

[14] Dao W. S, Bai X. C and Yu Li (2009) , "A High Bitrate Information Hiding Algorithm for Video in Video",World Academy of Science, Engineering and Technology 59, pp. 413-419.

[15] Mozo A. J, Obien M. E, Rigor C. J, Rayel D. F, Chua K. and Tangonan G (2009) , "Video Steganography using Flash Video (FLV)", I2MTC 2009 - International Instrumentation and Measurement Technology Conference Singapore, pp.5-7.

[16] Kim S. M, Cheng Z and Yoo K.Y (2009) , "A New Steganography Scheme based on an Index-color Image", 2009 Sixth International Conference on Information Technology: New Generations, pp.376-381.

[17] Luo W, Huang F and Huang J (2010) , "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 2, pp.201-214

[18] Nikoukar A. A (2010) , "An Image Steganography method with high data hiding Capacity Based on RGB Image", International Journal of Signal and Processing, pp.238-241.

[19] Wei Y, Guo L, Wang Y (2010) , "Controlling Bitrate Steganography on AAC Audio", 2010 3rd International Congress on Image and Signal Processing (CISP2010), pp.4373-4375.

[20] Djebbar F, Ayad B, Hamam H and Meraim K. A (2011) , "A view on latest audio steganography techniques", 2011 international conference on innovations in information and technology, pp.409-414.

[21] Gadicha1 A. B (2011), "Audio Wave Steganography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-5, pp.174-176.