IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 06, pp. 2569-2573, June, 2016

Research Article

VARIOUS METHODS OF VIDEO STEGANOGRAPHY

[1]Souma Pal and [2,*]Prof.Samir Kumar Bandyopadhyay

[1]Research Scholar, Department of Computer Science and Engineering, University of Calcutta, India
[2]Professor Department of Computer Science & Engineering, University of Calcutta, Kolkata, West Bengal, India

ARTICLE INFO

Article History:

Received 15th March 2016
Received in revised form
24th April 2016
Accepted 19th May 2016
Published online 30th June 2016

Keywords:

Steganography,
Digital watermarking,
Least Significant Bit,
Discrete Wavelet Transform,
Discrete Cosine Transform.

ABSTRACT

In recent days, security is a big threat in the transmission medium due to the development of the Internet and multimedia contents such as audio, image, video etc. For transmitting secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. Video Steganography is the process of hiding some secret information inside a video. The addition of this information to the video is not recognizable by the human eye as the change of a pixel colour is negligible. In this paper, a review on various video steganography techniques has been presented.

Copyright©2016, Souma Pal and Prof.Samir Kumar Bandyopadhyay. *This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.*

INTRODUCTION

Steganography is the art and science of embedding hidden information in such a way that no one, apart from the sender and intended recipient, identifies the existence of the message into the cover file. Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different invisible information. This hidden information can be plain text, cipher text, audio or even images. In a computer-based audio Steganography system, secret messages are embedded in digital audio. The secret message is embedded by slightly altering the binary sequence of the sound Existing audio Steganography software can embed messages in WAV, AU, and even MP3 audio files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images because human air is very perceptible to noise. These methods range from rather simple algorithms that insert information in the form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide message.

Cryptography on the other hand scrambles a message into a code to obscure its meaning, these two secret communication technologies are used separately or together—for example, by first level encrypting a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of secret communication, and as regulations are created by governments to limit uses of encryption so the importance of steganography becomes prominence day by day. In this paper we combine the concept of cryptography and steganography. In first level the message is encrypted by using a pattern matching algorithm and in second level the message is secretly hidden into a cover file.

To perform the pattern matching algorithm a 28 bit sequence array has been employed in such a way that all possible combination of a four bit sequence is present there. The target string is also converted into binary sequence. In next level each four sequence of the target string is searched from the pattern matching array and instead of sending the target string directly we have send its identified location. This methodology increases the level of encryption in a well manner. For sending purpose the conventional LSB method has been used. Main advantages of LSB coding is that it allows a huge volume of data given in audio or text format to be encoded and data are found in the receiving end in loss-less way. The message is decrypted in the receiving side in a loss less way.

***Corresponding author: Prof.Samir Kumar Bandyopadhyay,**
Professor Department of Computer Science & Engineering, University of Calcutta, Kolkata, West Bengal, India.

Finally the quality of the proposed method is measured with respect to two parameters Mid Square Error and Signals to Noise Ratio, The experimental result illustrates that the stego signal generated by proposed method are perceptually indistinguishable from the original cover file. A video can be viewed as a sequence of still images. Data embedding in videos seems very similar to images. However, there are many differences between data hiding in images and videos, where the first important difference is the size of the host media. Since videos contain more sample number of pixels or the number of transform domain coefficients, a video has higher capacity than a still image and more data can be embedded in the video. Also, there are some characteristics in videos which cannot be found in images as perceptual redundancy in videos is due to their temporal features. Here data hiding operations are executed entirely in the compressed domain. On the other hand, when really higher amount of data must be embedded in the case of video sequences, there is a more demanding constraint on real-time effectiveness of the system. The method utilizes the characteristic of the human vision's sensitivity to color value variations. The aim is to offer safe exchange of color stego video across the internet that is resistant to all the steganalysis methods like statistical and visual analysis. This paper provides overview of various Video Steganography schemes.

Literature Reviews

Image based and video based steganography techniques are mainly classified into spatial domain and frequency domain based methods. The former embedding techniques are LSB, matrix embedding etc. Two important parameters for evaluating the performance of these system are capacity and imperceptibility. Capacity refers to the amount of data that can be hidden in the cover medium so that no perceptible distortion is introduced. Imperceptibility or transparency represents the invisibility of the hidden data in the cover media without degrading the perceptual quality by data embedding (Lee and Chen, 2000). Security refers to an unauthorized person's inability to detect hidden data. To enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision, tri-way pixel-value differencing (TPVD) algorithm is used for embedding (Ko-Chin Chang *et al.*, 2008). Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later (Hartung and Girod, 1998; Bin Liu *et al.*, 2008). The other, tries to embed data directly in compressed video stream. The problem of the former is how to make the embedded message resist video compression. But because the video basically exists in the format of compression, the research of the latter is more significant.

In audio steganography, the weakness of the Human Auditory System (HAS) is basically used to hide information in the audio file. Because the human auditory system has more precision than Human Visual System (HVS), that's why audio, steganography is more challenging than image steganography.
The lists of methods that are commonly used to perform audio steganography are works in two domain, time domain or frequency domain. Some popular method are given below (Rahim *et al.*, 2014; Balgurgi *et al.*, 2012; Malviya *et al.*, 2012; Bandyopadhyay *et al.*, 2008).

LSB coding: Least significant bit coding is the simplest way to embed information in a digital audio file by substituting the least significant bit of each sampling point with a binary message. LSB coding allows for a large amount of data to be encoded (Bin Liu *et al.*, 2008).

Parity coding: In these technique an extra parity bits has been employed with the message so that if there is any change in the message it can be easily identified by the receiver.

Phase coding: Rather than introducing perturbations, 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- noise ratio.

Echo hiding: Echo hiding embeds its data by creating an echo to the source audio. Three parameters of thisartificial echo are used to hide the embedded data, the delay, the decay rate and the initial amplitude. As the delay between the original source audio and the echo decrease it becomes harder for the human ear to distinguish between the two signals until eventually a created carrier sound's echo is just heard as extra resonance.

Spread Spectrum (SS): The Spread spectrum method spreads the secret message over the frequency spectrum of sound file which is independent of the actual signal (Anderson, 1996; Nathan *et al.*, 2011).

Tone Insertion: This technique is based on insertion of lower power tones in the presence of significantly higher ones. The masking effect is a property of human auditory system (HAS) which make any weak speech component imperceptible by listeners in presence of a much louder one. By inserting tones at known frequencies and at low power level, concealed embedding and correct data of the unintentional attacks such as low pass filtering and bit truncation.

Wavelet Coefficient: In this case, the audio steganography is based on discrete wavelet transform (DWT). Data embedding is done in the LSBs of the wavelet coefficients achieving high capacity of 200 kbps in 44.1 kHz audio signal. To improve the embedded data imperceptibility, a hearing threshold is introduced and the data hiding in silent parts of the audio signal is avoided. Data hiding in wavelet domain obtains high embedding rate but data extraction at the receiver side might have some errors.

Day by day to increment the level of encryption some different methodology are incorporate with the above conventional method. Instead of sending the original text message the encrypted version of the text are now embedded with the cover audio file. Modulo operator, XOR operation, gray code converter is the technique generally used to perform the first level encryption. (Datta *et al.*, 2015) Different traditional cryptographic algorithm is directly used for encryption purpose, such as RSA algorithm, AES, DES, MD5 algorithm. Algorithm from different domains is now a day's used in steganography. Genetic algorithm based approach is a technique where a new sample message has been constructed by using alteration, modification and verification and in the receiving end the reconstruction of the message has been done (Hartung and Girod, 1998).(6)

There are lots of methods related to image encryption where a message is secretly hidden within an image. (5) To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in noisy areas that draw less attention—those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

- Least significant bit insertion.
- Masking and filtering.
- Redundant Pattern Encoding.
- Encrypt and Scatter.

Least significant bit (LSB) insertion is a common and simple approach to embed information in a cover file. In this method the LSB of a byte is replaced with an M's bit. This technique works better for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object. On the other hand in frequency domain discrete cosine transformation and other transformation technique has been used. DCT is a lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the form of signal noise, to more powerful methods that exploit sophisticated signal processing techniques to hide information.

Neural network has the super capability to approximation any nonlinear functions. We first extract features of image embedded information, then input them into neural network to get output. Manikopoulos *et al.* (2008) discussed an algorithm that utilises the probability density function (PDF) to generate discriminator features fed into a neural network system which detects hidden data in this domain. A group of scientists at Iowa State University are focusing on the development of an innovative application which they call ''Artificial Neural Network Technology for Steganography (ANNTS)'' aimed at detecting all present Steganography techniques including DCT, DWT and DFT.

Adoption of Neural Network Approach in Maher EI Arbi *et al.* suggested video watermarking based on neural network (Rahim *et al.*, 2013). They propose a novel digital video watermarking scheme based on multi resolution motion estimation and artificial neural network. A multi resolution motion estimation algorithm was adopted to preferentially allocate the watermark to coefficients containing motion. In addition, embedding and extraction of the watermark were based on the relationship between a wavelet coefficient and its neighbour's. A neural network was given to memorize the relationships between coefficients in a 3x3 block of the image. Experimental results showed that embedding watermark where picture content is moving is less perceptible. Further, it showed that the scheme was robust against common video processing attacks.

Guohua Wu el al. (?), suggested Counter propagation Neural Network (CNN) based method for fast audio digital watermark. By making use of the capabilities of memorization and fault tolerance in CPN, watermark is memorized in the nerve cells of CPN. In addition, they adopt a kind of architecture with an adaptive number of parallel CPN to treat with each audio frame and the corresponding watermark bit. Comparing with other traditional methods by using CPN, it was largely improve the efficiency for watermark embedding and correctness for extracting, namely the speed of whole algorithm. The extensive experimental results showed that, we can detect the watermark exactly under most of attacks. This method efficaciously trade off both the robustness and inaudibility of the audio digital watermark.

Different Methods

The effective Steganography should have the following characteristics:

Secrecy: Extraction of hidden data from the host medium should not be possible without the knowledge of the proper secret key used in the extracting procedure.

Imperceptibility: After embedding the data in the medium, it should be imperceptible from the original medium.

High capacity: The maximum length of the hidden message that can be embedded can be as long as possible.

Resistance: The hidden data should be able to survive when the host medium has been manipulated, for example lossy compression scheme.

Accurate extraction: The extraction of the hidden data from the medium should be accurate and reliable.

The following figure 1 illustrates subdivided system for basic security system

There are mainly three basic data embedding techniques for images:

Least Significant Bit (LSB)

The primitive, easily implemented embedding method is LSB.Yhe information are embedded in the LSB of pixels colours. On an average, only half of the bits in the image will need to be modified to embed a secret message using the maximal cover size. While using a 24-bit image gives a relatively large amount of space to hide messages, it is also possible to use an 8-bit image as a cover source. The changes of LSB may not be noticeable because of the imperfect sensitivity of the human eyes. 8-bit images require more careful approach due to smaller space and different properties. Where 24-bit images use three bytes to represent a pixel, an 8-bit image uses only one. Changing the LSB of that byte will result in a visible change of colour, as another colour in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in gray scale, as the human eye will not detect the difference between different gray values as easy as with different colours.

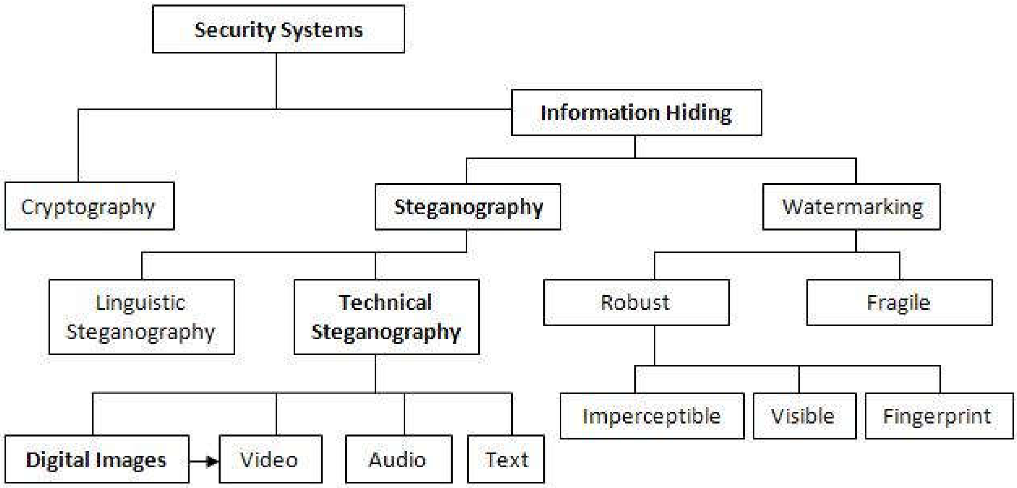

Fig. 1. The different methods of security system

Masking and filtering

This is a different embedding approach of messages. This is done by modifying the luminance part of image (24 bit/gray image). While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the difference. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing.

Transform based

This is highly robust and complex method. Data is embedded in the transform coefficients (DCT, DWT). DCT is used in JPEG compression algorithm to transform successive 8_8 pixel blocks of the image, into 64 DCT coefficients each. After calculating the coefficients, the quantizing operation is performed. Although a modification of a single DCT will affect all 64 image pixels, the LSB of the quantized DCT coefficient can be used to embed information. When only small data are embedded in the video/image, it is not noticeable. But when Large amount of data are embedded in the video, the DWT(sub bands:LL,LH,HL,HH) is used for detection. Data is embedded in LL sub-band to avoid compression losses.

There are some other classification is also available:

Injection

The embedded data is placed inside the original cover file. The end-processing/presentation application prevents from revealing the presence of the embedded data within the cover file by increasing the host file size.

Substitution (bit-twiddling/bit-tweaking)

The replacement is done in the insignificant part (rarely/never used program module/ segment of executable code) of the cover file, resulting file degradation (e.g. audible noise in sound file).

Propagation

It utilizes a generation engine without cover/host file which when fed the payload produces an output file. The content of the output file is called “mimic”.

Neural Network in Steganography

In Biological system, the neural network refers to a network or circuit of Biological neuron. In modern computer usage, this term refers to artificial neural network, composed of artificial neural nodes which may either be used to gain an understanding of biological neural networks, or for solving artificial intelligence problems without necessarily creating a model of a real biological system. Based on the training, the neural net determines computational rules that can then be applied to the features of an image of unknown character. One particular merit of an artificial neural network is that it is adaptive—as additional data is provided to the system it refines its prediction function. Artificial Neural Networks have been applied successfully to speech recognition, image analysis and adaptive control, in order to construct software agents or autonomous robots. It is also applicable in the counter terrorism and law-enforcement communities in measures that can be used to detect the existence of hidden data. Comparative Analysis This paper presented a background of Steganography and a comparative study of some Steganographic techniques. There are two important parameters of evaluating all Steganography technique, first is imperceptibility and the second is capacity.

Imperceptibility means the embedded data must be imperceptible to the observer and computer analysis. Capacity means maximum payload is required, i.e. maximum amount of data that can be embedded into the cover image without losing the fidelity of the original image. The results of surveying the papers in different techniques of video steganography showed that all the methods possess the ability to hide data without noticing changes in their properties. It was found that in (4), they have used the 3-3-2 approach along with LSB and the result was found to be good and about 33.3% from the size of image can be used for data hiding. In other words, in the space of 5 images, 500 pages of data could be stored without resizing. Similarly, 1 second in certain video types contains approximately 27 frames, which in turn creates a lot of room for hiding data. In (5), Results of using this technique showed no visual distortion in the host file and even the quality of the new video generated can be accepted for practical use. In (6), it has been known that in the LSB algorithm due to high replacement rate, MSE value is high. So it lacks from security.

In case of LSBMR algorithm due to low replacement rate, MSE value is low which makes it secure when compared to LSB algorithm. In their method, intruder may not be able to identify the presence of the secret message inside the frame. Also, the comparison with the original video never gives the original secret message, which ensures additional security. In (7), videos of different sizes and resolutions are tested for their method and they have got successful in keeping the MSE and PSNR value low enough that it cannot be noticed easily in the Steganalysis process. They have provided a comparison between the basic LSB method and their method gave better values of MSE and PSNR than the LSB method. The average PSNR of the proposed LSB embedding technique (per pixel, RGB) to the traditional layering technique in which embedding is done by layers of RGB. They found an improvement of about 1.5 dB in their PSNR value when compared to the traditional LSB technique and also a lesser MSE which means in detectability. In (Balgurgi *et al.,* 2012), the authors calculated PSNR value for different amount of LSB substitution.

For 1 LSB substitution, the PSNR value was found between 45-50 for different with no of frames. For 2 bit LSB substitution, PSNR was found to be in the range of 40-45. And for 3 bit LSB substitution, PSNR value was about 35. By the use of AES encryption, their method was more secured as compared to traditional LSB techniques. In (Anderson, 1996), their results showed that no visual distortion is there in the host video stream and even the quality of the recovered secret video is also acceptable in practical. In (Nathan *et al*., 2011), use of Hamming code makes the technique highly efficient and more secured. The authors used more than 1 key and thus have obtained a high level of security as compared to traditional steganographic methods like LSB substitution where only one XOR encryption is used. In (Malviya *et al*., 2012), unlike other steganographic technique, the authors have implemented a closed loop feedback steganalysis to test their project's immunity towards steganalysis. The complete project was done in compressed domain hence avoiding decompression process. With continuous advancements in technology it is expected that in the near future more efficient and advanced techniques in steganalysis will emerge that will help law enforcement to better detect illicit materials transmitted through the Internet.

Conclusions

There are many techniques for video Steganogarphy. But this paper discusses only Neural Network method (NN) since the improvement of computer are rapidly growing on the basis of AI. In this paper, we briefly review the research of visual cryptography schemes as special cases of secret sharing methods among participants. Their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated.

REFERENCES

Anderson (ed.), R. J. 1996. "Information hiding", 1st international workshop, volume 1174 of Lecture Notes in Computer Science, Isaac Newton Institute(Springer-Verlag, Berlin, Germany).

Balgurgi, Pooja, P. and Sonal K. Jagtap. 2012. "Audio steganography used for secure data transmission." In Proceedings of International Conference on Advances in Computing, pp. 699-706. Springer India.

Bandyopadhyay, S.K., Bhattacharyya, D., Ganguly, D., Mukherjee, S. and Das, P. 2008. "A tutorial review on steganography". In International conference on contemporary computing Aug 7 (Vol. 101).

Bin Liu, Fenlin Liu, Chunfang Yang and Yifeng Sun.: Secure Steganography in Compressed Video Bitstreams,The Third International Conference on Availability,Reliability and Security,2008

Datta, Biswajita, Souptik Tat, and Samir Kumar Bandyopadhyay. "Robust high capacity audio steganography using modulo operator."International Conference onComputer, Communication, Control and Information Technology (C3IT), IEEE, (2015, December 21-24), Himachal Pradesh, India.

Guohua Wu, Xiaodong Zhou, 2008. "A Fast Audio Digital Watermark Method Based on Counter-propagation Neural Networks", International Conference on Computer Science and Software Engineering, pp. 583-586

Hartung, F. and Girod, B. 1998. Watermarking of uncompressed and compressed video, Signal Processing, Special Issue on Copyright Protection and Access Control for Multimedia Services, 66 (3): 283-301.

Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu,: A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia , VOL. 3, NO. 2, JUNE 2008

Lee, Y. K. and Chen, L. H. 2000. High capacity image steganographic model, IEE Proceedings on Vision, Image and Signal Processing, Vol. 147, No.3, pp. 288-294.

Maher El' Arbi *et al*. 2006. "Video Watermarking Based On Neural Networks", ICME, pp. 1577-1580.

Malviya, S., Saxena, M. and Khare, A. 2012. Audio Steganography by Different Methods. International Journal of Emerging Technology and Advanced Engineering (20) (ISSN 2250-2459, Volume 2, Issue 7.

Manikopoulos, C., Yun-Qing, S., Sui, S., Zheng, Z., Zhicheng, N., Dekun, Z. 2002. "Detection of Block DCT-based Steganography in Gray-scale Images", Proceedings of the IEEE Workshop on Multimedia Signal Processing, 9–11, pp. 355– 358.

Nathan, Mark, Nikhil Parab and Talele, K. T. 2011. "Audio Steganography Using Spectrum Manipulation." In Technology Systems and Management, pp. 152-159. Springer Berlin Heidelberg.

Rahim, L.B., Bhattacharjee, S. and Aziz, I.B. 2014. "An Audio Steganography Technique to Maximize Data Hiding Capacity along with Least Modification of Host". In Proceedings of the First International Conference on Advanced Data and Information Engineering (DaEng-2013) 2014 Jan 1 (pp. 277-289). Springer Singapore.

****