Different Techniques of Data Hiding in Multimedia

Kanak Meena
Research Scholar, Dept. of Computer Science
Indira Gandhi Delhi Technical University for Women, Delhi, India
kanak556@gmail.com

Arushi Butan
Dept. of Computer Science
Indira Gandhi Delhi Technical University for Women, Delhi, India
arushibutan11@gmail.com

Aalo Majumdar
Dept. of Computer Science
Indira Gandhi Delhi Technical University for Women, Delhi, India
aaloshree@gmail.com

Abstract: There has been an explosive growth of the World Wide Web which has become the primal source of communication. As the number of users of Internet facilities is increasing, privacy of their data becomes of paramount importance. Therefore, it is crucial to ensure that big data does not pose security concerns for its users or violate the privacy of individuals. Several techniques have been proposed to protect and preserve the data from unwanted and unauthorized access. Data hiding is one such technique where the data to be communicated is hidden in order to protect it from intruders. This survey paper aims to present a review of different data hiding techniques like steganography, digital watermarking.

***Keywords*:** Data hiding, Steganography, Cover media, Stego-media, Image steganography, Audio and Video Steganography, Digital watermarking, Visible and Invisible watermarking.

I. INTRODUCTION

The techniques of information hiding are being increasingly employed in the field of information security. It is of two types: digital watermarking and steganography. Digital watermarking is the process of protecting the copyrights of electronic products. Steganography is a method of data hiding where data is conveyed in a secret way. [1].

There are various data hiding methods which were used in prehistoric times. Back then, different emperors used to communicate with each other by utilizing data hiding. When they used to send the information to each other, different methods of data hiding were employed. One such method which was often used was writing the message by invisible ink and when the message was subjected to heat, the ink would darken, and become visible. Such types of techniques were used successfully during WW-II. [2] Another method that was used [3] by the soldiers to send the confidential messages was by writing under the wax known as "wax covered tablet". They wrote a message on the wood then they put the layers of wax on wood.

The concept of data hiding has evolved; nowadays we have so many techniques to protect the secret data from unwanted access like steganography (text, audio, video), digital watermarking (visible and invisible watermarking), cryptography. In this paper, we will be elucidating on two such techniques, steganography and digital watermarking.

Steganography is a process of protecting the confidential data by hiding it. It can be embedded in any form of media like text, images, video, and audio. In this technique, unwanted access is prohibited because the attackers are not aware of the data transmission. Therefore it is impossible to distinguish the message from original one as it is invisible to our eyes.

Steps:

1. Select the media which is used to hide the confidential data.
2. The hidden information which is to be discovered.
3. Select the function which will be used to hide and then recover the hidden data.
4. Select the password or key to validate the data.[4]

The media which is used to hide the information is known as cover medium and the combination of cover medium and key is known as a stego medium. [5] Let us assume we use the audio to hide the message, then the audio is known as cover audio and the final product is known as stego audio.

Digital watermarking is used to protect the copyrights of electronic products. It is done by embedding data into the noise tolerant signals like text, audio, images, videos such that they cannot be removed easily. Digital watermarking is very similar to steganography. It is used to identify the source or the creator of the file.

A good watermarking is such that the actual content of the noise tolerant signals is hidden completely in the message. If the signals are disturbed in the final product, it implies that quality watermarking wasn't done. The techniques of watermarking are being used from last 15 years. Earlier, it was used on paper. For example, the image of Mahatma Gandhi is being used on the rupee to authenticate the Indian currency. The technique used is invisible watermarking, that is, it is not visible to naked eye but if seen from the opposite direction of light, the image of Gandhi is visible. Digital media is booming nowadays which has led to the advent of digital watermarking. [7]

This paper presents an in-depth analysis and a review of various data hiding techniques in steganography and digital watermarking.

II. VARIOUS DATA HIDING TECHNIQUES AND RELATED WORK

In this section, a review of various data hiding techniques in steganography and digital watermarking is presented which facilitate secure data transmission over a network without the loss of confidentiality.

STEGANOGRAPHY:-

Data hiding in still images

In these set of techniques, the secret information is hidden in a 24-bit RGB color image [8]. The information is hidden in the LSB's of the 24 bit color space in the form of a linked list. A linked list is a data structure where each node has the address of the next node in the list and they are placed randomly in the memory. The secret messages are embedded in the form of bytes at random places in the color image such that there is a pointer in each message which points to the next message. A stego key used to authenticate the secret information which embedded in the first secret message. This technique makes the attacker work very difficult to detect and retrieve the secret information and confidential data under the images. [4]

Kuo et al [4] provide another technique where blocks are divided such that each block has secret information embedded in it. In this reversible technique, a histogram is generated for every block of the image. Embedding space is generated on the basis of computing the minimum and maximum points of the histogram for hiding the secret data which also increase the capacity of the images at the same time.

Naseem et al [9] have proposed the Optimized Bit Plane Splicing technique. This technique is a modification of the traditional bit plane splicing technique where the data is hidden based on the intensity of the pixels. The intensity of each pixel is calculated and arranged into different categories based on their range. Then based on the intensity of a pixel, the required number of bits are selected in a particular plane in which data is hidden. The bits are hidden in a random fashion and the planes are transmitted sporadically therefore improving the efficiency of the algorithm.

Fu et al. have proposed an interesting technique for information hiding in halftone images [4][10] Using the method, large amounts of data can be hidden in halftone images without the use of original multi-tone images. This can be achieved with the help of forced pair-toggling. The resulting images, called stego-images are identical to the original image and virtually indistinguishable from it.

Dey et al.[4] have proposed a modification of the Fibonacci decomposition method since only the LSB planes are being used to hide the data in the original technique. In this technique, the number of planes is increased so that higher planes can also be used to hide the data. This is achieved by utilizing the concept of prime numbers. The original bit planes are converted another binary number system using prime numbers as a the weighted function so that the number of bits to represent each pixel increases which in turn can be used hide data in higher bit planes. The authors have also performed a comparison of the Fibonacci decomposition method with the traditional LSB data hiding technique showing that the former outperforms the latter method and on comparing Fibonacci Decomposition method with the proposed method, it is observed that this method outclasses the former method. Also, the proposed method generates the stego-image which is virtually indistinguishable from the original image

Data hiding technique in audio

Embedding the secret data in audio files is known as the audio Steganography. It is a very difficult and one of the most challenging techniques to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. Several formats that are used in this technique are Sample Quantization (.WAV and .AIFF.), Temporal Sampling Rate((uses selectable frequencies (8 kHz, 9.6 kHz, 10 kHz, 12 kHz,16 kHz, 22.05 kHz and 44.1 kHz.)) and Perceptual Sampling (ISO MPEG(MP3).). [2]

Methods of audio steganography

a. LSB Coding

Analog audio signals are converted to digital binary sequence by sampling the data with the help of quantization. In order to hide the secret messages using this technique, binary equivalent of the secret message is embedded in the LSB of the binary sequence in the digitized audio file. [12]

b. Phase coding

Phasing coding is one the most effective techniques. In this method, the secret message is embedded in the phase where the reference phase of the hidden data is replaces the phase of the original audio signal. [2]

c. Echo data hiding

Echo data hiding is an interesting method with hides the secret messages in the form of an echo in the original audio signal. The data is hidden in the parameters of an echo like initial amplitude and decay rate. The signals seem to blend as the offset between them decreases and after a certain point, they are indistinguishable to the human ear. The human ear perceives it as added resonance. This point depends on the quality of the original recording, the type of sound being echoed, and the listener. [13]

Two methods were proposed by Kekre et al. for transferring secret data over a network by embedding it in audio signals, thus generating a stego-audio signal [14]. In the first method, the secret data is hidden in the LSB of audio by replacing the digitized sample of the audio. The parity of the sample is first checked and then the secret data is embedded into the LSB. Therefore, it becomes difficult for the intruders to evaluate where any is data is being transmitted. In the second approach, we use the XOR function on the LSBs. The LSBs are XORed and depending on the output of the XOR function and the secret data to be embedded, the LSB of the sample data is to be changed or left unchanged.

Kondo[14][4] proposed another data hiding algorithm to implant secret data in audio signals. The concept of polarity of reverberations is used in the algorithm using which high frequency signals are altered. In this method, data is hidden in the middle channel which is used to replace the high frequency channels. The polarity of reverberations on each channel is performed to adjust the coherence between the channels. The hidden data is detected by using the correlation between the sum and difference of the stereo signal.

Data hiding technique in video

Embedding the secret data in the video files is known as video steganography. It is the most advanced form of steganography which makes it very difficult for the attacker to retrieve and detect the confidential data as it is a collection of the images and audio. Video steganography is a combination of the audio and images steganography. It contains large amounts of data and moving streams of images and sound which makes it easier to hide the data inside the videos. [15]

A data hiding technique in videos was proposed by Li et al [16] [4] which is based on video sequences. An embed point, where the secret data is to embedded is selected using an adaptive embedding algorithm. 4x4 DCT residual blocks are adopted and a predefined threshold is determined. The blocks are then traversed in an inverse zigzag manner to search for the first non-zero coefficient. The predefined threshold is compared to the value of this coefficient determined and if it is lesser than the value of the coefficient, then data is embedded at that pixel.

J. J. Chae et al [17] proposed another technique of data hiding in video. In this method, there are two main categories. The first one involves an uncompressed raw video stream and secret data is embedded in that. Giuseppe Cacao et al [17] proposed the second category which embeds secret data directly into a compressed video stream.

A algorithm for video compression was proposed by Sherly A P et al.[18] known as tri-way pixel-value differencing with pseudorandom dithering (TPVDD) [3][4] This algorithm is used for embedding secret data. It increases the capacity of the hidden secret information and provides enhanced security.

DIGITAL WATERMARKING

Digital watermarking is used to preserve the copyrights of electronic and digital products. It is done by embedding information into the noise tolerant signals like text, audio, images, videos such that they cannot be removed easily. This technique is essential to prevent plagiarism and address the rapid proliferation of digital content [2]. There are two types of digital watermarking. **Visible watermarking** is a digital watermarking technique which is most commonly used for the purpose of copyright protection. For example, there is a situation where a set of images is uploaded on the Internet and the creator wants to ensure that the images are not reproduced by others, so they watermark his work. It also indicates the ownership. **Invisible watermarking** is a technique which is not visible to anyone. It can only be extracted with the use of a watermark extraction algorithm. Invisible watermarked image is indistinguishable from the original image [5][6].

Digital Watermarking can be done in any multimedia like audio, video, text, images, Hardware/Software.

Kunal D Megha et al. [19] proposed an algorithm for digital watermarking using DCT-DWT Algorithm. In this algorithm, they take an image which is extracted from the cover image and then assess the quality of extracted image and its robustness.

Another digital image watermarking algorithm was proposed by Huiping Guo et al.[20] based on a generalized secret sharing scheme. This scheme is built on threshold cryptography which was proposed by the *Shamir.*

Saraju P. Mohanty et al.[3]proposed the technique for Invisible Watermarking on digital content using Image Adaptive Watermarks.

Mohanty et al[3] Srdjan Stankovi´et al. [21] suggested that watermarking must be performed on the cover image using several functions like discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT), and fractal transform.

Qi et al. have proposed adaptive digital image watermarking method in the domains of spatial and DCT domain processing. [21] Mahmoud Elnajjar et al.[7] proposed the algorithm for optimization in which they divide the algorithm in two categories: Watermark Embedding and Extracting the Embedded Watermark.

III. COMPARISION OF DISCUSSED TECHNIQUES

This section contains a comparative analysis of different data hiding techniques discussed in the paper:-

In steganography, several techniques are used to hide data in still images and generate stego-images with embedded secret messages. In the first technique, data is be embedded in 24-bit RGB color images using data structures like linked lists where the secret messages are stored in a list of pointers. This method is advantageous because data is hidden randomly and not sequentially which makes it difficult for the attacker to locate it. Moreover, the attacker cannot access the next piece of data in the image without the authentication key. The next technique employs the use of histograms of blocks of images. The maximum and minimum points of the histogram are computed and the secret messages are embedded between these points. This technique is an improvement over the previous technique because it provides a higher range to hide data. In next method of halftone, the author suggests the algorithm for large amount of data which was not possible in earlier algorithm. In the Fibonacci decomposition method, the concept of Prime numbers is utilized to hide the secret data in the images. The number of the bit planes are increased which allows the cover image to embed more strongly and stego-image which is generated is identical to the original image.

Another way to hide data is to embed it in audio signals. This uses the concept of polarity of reverberations which is applied to the high frequency signals. A middle channel replaces the high frequency channels such that the hidden data is embedded in the channel. The XOR functions are also used to make the secret message strongly embedded in audio.

A technique that is used to transfer data securely over a communication channel is the Jigsaw-based approach. In this scheme the secret data to be embedded is broken down into block of variable sizes and a key, known as the message authentication code (MAC) is used to validate each and every block of data. Moreover, every message contains a prefix as well as a suffix of binary 1. Fragmenting of the data helps in misleading the attacker as the attacker cannot retrieve any information from it and the attacker requires the authentication key to access any of the data.

Next method suggested is for a compressed video. This is the most secure method to hide the data. Another algorithm was suggested for compressed video but it was very secure and safe to transfer the date over network because it also increases the capacity of the hidden data.

Steganography is modifying the original image such that only the sender and the receiver for which the image is intended is able to decode the message sent. It is invisible to the outside world and detecting the secret messages is not easy. [2] The techniques of sending secret messages are better and more efficient than encoded messages. Digital watermarking is employed to verify and protect the identity and authenticity of the owner who has created a digital image. It is a process of embedding information into a digital image or noise tolerant signal which verifies the identity of the owner and protects the copyrights. [22]

IV. CONCLUSION

After the thorough review of all the techniques of data hiding, it is concluded that steganography is modifying the original image such that only the sender and the receiver for which the image is intended is able to decode the message sent. It is typically invisible and the generated stego-image is virtually indistinguishable from the original image. Watermarking is a process of embedding information into a digital image or noise tolerant signal which verifies the identity of the owner and protects the copyrights. Watermarking can be of two types; visible watermarking, which is visible to the naked eye and invisible watermarking which is hidden. Watermarking is usually employed for the copyright protection and source tracing. Watermarking is more robust then the steganography.

REFERENCES

[1] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, Information Hiding—A Survey,Proc. IEEE, 1999.

[2] Sabu M Thampi ,Information Hiding Techniques: A Tutorial Review,ISTE-STTP on Network Security & Cryptography, LBSCE 2004,pp.1-19.

[3] Saraju P. Mohanty and Bharat K. Bhargava, Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks,ACM Journal Name, Vol. V, No. N, February 2008,pp.1-24.

[4] Harshvardhan et al,A Survey on Various Data Hiding Techniques and their Comparative Analysis,pp,1-9.

[5] Arvind Kumar and Km. Pooja, Steganography- A Data Hiding Technique, International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010,pp.19-23.

[6] Jonathan K. Su, Frank Hartung, Bernd Girod,Digital Watermarking of Text, Image, and Video Documents,Preprint submitted to Elsevier Preprint 23 August 1999,pp 1-16.

[7] Mahmoud Elnajjar, A.A Zaidan, B.B Zaidan, Mohamed Elhadi M.Sharif and Hamdan.O.Alanazi, Optimization Digital Image Watermarking Technique for Patent Protection , Journal of computing, volume 2, issue 2, february 2010, issn 2151-9617,pp.142-147.

[8] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, Embedding stego-text in cover images using linked list concepts and LSB technique, Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.

[9] M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding, International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA,pp 36-38.

[10] Ming Sun Fu and O.C. Au, Data hiding watermarking for halftone images, IEEE Transactions on Image Processing, Vol.11, No. 4, Apr. 2002, pp.477-484.

[11] Hsien-Wen TSENGand Chin-Chen CHANG, High Capacity Data Hiding in JPEG-Compressed Images, INFORMATICA, 2004, Vol. 15, No. 1, 127–142 127 □□2004 Institute of Mathematics and Informatics.

[12] Masoud Nosrati,Ronak Karimi and Mehdi Hariri,An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011. 191-195 ISSN: 2222-2510 ©2011 WAP journal.

[13] W. Bender,D. Gruh and N. Morimoto A. Lu,Techniques for data Hiding IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996,pp.313-336.

[14] H. B. Kekre, Archana Athawale, Archana Athawale, Uttara Athawale, Information Hiding in Audio Signals, International Journal of Computer Applications IJCA, Vol. 7, No. 9, Foundation of Computer Science, New York, USA, pp. 14-19.

[15] B.SUNEETHA, CH.HIMA BINDU & S.SARATH CHANDRA,SECURED DATA TRANSMISSION BASED VIDEO STEGANOGRAPHY,International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315-4489, Vol-2, Iss-1, 2013,pp.78-81.

[16] Yu Li, He-xin Chen, Yan Zhao, A new method of data hiding based on H.264 encoded video sequences, IEEE 10th International Conference on Signal Processing(ICSP), 24-28 Oct. 2010, pp. 1833-1836.

[17] P.Paulpandi1and Dr.T.Meyyappan, Hiding Messages Using Motion Vector Technique In Video Steganography, International Journal of Engineering Trends and Technology- Volume3Issue3- 2012,pp.361-365.

[18] Sherly A P and Amritha P, A Compressed Video Steganography using TPVD, International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010,pp 67-80.

[19] Kunal D Megha1, Nimesh P Vaidya, Asst. Prof Ketan Patel .Digital Watermarking: Data Hiding Techniques using DCT-DWT Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013. ISSN (Online) : 2278-1021.

[20] Huiping Guo, Nicolas D. Georganas,A novel approach to digital image watermarking based on a generalized secret sharing scheme, Multimedia Systems (2003) Digital Object Identifier (DOI) 10.1007/s00530-003-0096-1 Multimedia Systems© Springer-Verlag 2003,pp.1-12.

[21] Igor Djurovi´c, Srdjan Stankovi´c† and Ioannis Pitas ,Digital watermarking in the fractional Fourier transformation domain, Journal of Network and Computer Applications (2001) 24, 167–173 doi:10.1006/jnca.2000.0128.

[22] Dr. Vipula Singh, Digital Watermarking: A Tutorial, Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition, 2011,pp.10-21.