A SURVEY ON HIDING AND EXTRACTING DATA IN VIDEO FILE USING HIGH FEDILITY COMPRESSION

Ms. Monika S. Shirbhate*

Prof.S.S. Kulkarni**

Abstract

The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security, Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. In the current internet community, secure data transfer is limited due to its attack made on data communication. So more robust methods are chosen so that they ensure secured data transfer. One of the solutions which came to the rescue is the audio Steganography. But existing audio steganographic systems have poor interface, very low level implementation, difficult to understand and valid only for certain audio formats with restricted message size. Enhanced Audio Steganography (EAS) is one proposed system which is based on audio Steganography and cryptography, ensures secure data transfer between the source and destination..

Keywords: Data hiding Algorithm, Data Extracting Algorithm, Ratio Analysis, Security Analysis, 4th bit LSB method

* Scholar, P. R. M. I. T. & R. , Badnera

** Associate Professor, Department of Information Technology P. R. M. I. T. & R. , Badnera

I. INTRODUCTION

The power of steganography is in hiding the secret message by obscurity, hiding its existence in a non-secret file. In that sense, steganography is different from cryptography, which involves making the content of the secret message unreadable while not preventing non-intended observers from learning about its existence1.Because the success of the technique depends entirely on the ability to hide the message such that an observer would not suspect it is there at all, the greatest effort must go into ensuring that the message is invisible unless one knows what to look for.

The way in which this is done will differ for the specific media that are used to hide the information. In each case, the value of a steganographic approach can be measured by how much information can be concealed in a carrier before it becomes detectable, each technique can thus be thought of in terms of its capacity for information hiding. There are numerous methods used to hide information inside of Picture, Audio and Video files. The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial.

Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing. The purpose of steganography is covert communication to hide a message from a third party. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them. Generally, in steganography, the

actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it. There are many to embed information into a popular media using steganography. A good example of this is the relationship between a recorded song, and its lyrics. The audio file containing the recording is much larger than the song lyrics stored as a plain ASCII files. Therefore it is probably safe to assume that the smaller file could be steganographically embedded into the larger one without impacting the quality.

Important domains, besides classic computing, where steganography can be applied are domains using mobile and embedded devices especially mobile phones. In this project we state the fact that steganography can be successfully implemented and used into a next generation of computing technology with image and video processing abilities. The LSB method used for this project which satisfies the requirement of steganogaphy protocols. This research will include implementation of steganographic algorithm for encoding data inside video files, as well as technique to dynamically extract that data as original.

II. LITERATURE REVIEW

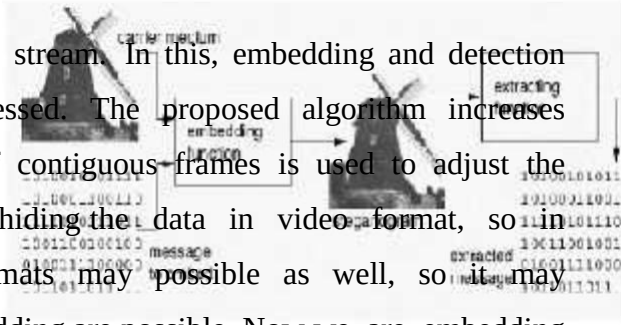
For studying the concepts of video steganography, we have surveyed many latest papers. In this section we have described the relevant papers of different authors. We thank these authors for providing the knowledge of video steganography. These papers were very important to us for studying the basic concept Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas [2], the main requirements of any data hiding system are security, capacity and robustness It is very difficult to archive all these factors together because these are inversely proportional to each other. Authors have focuses on maximizing security and capacity factor of data hiding. The data hiding method uses high resolution digital video as a cover signal. It provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms. They have used the large payloads like video in video and picture in video as a cover image. Ahmed Ch. Shakir [1], the confidential communications over public

networks can be done using digital media like text, images, audio and video on the internet. Simply hiding the contents of a message using cryptography was not adequate. Hiding of message should provide an additional layer of security.

To provide the more security the author suggested the new procedures in steganography for hiding ciphered Information inside a digital color bitmap image. He has used quadratic method depending on the locations concluded by the binary image, beside of public key cryptography. He had concluded that the conjunction between cryptography and steganography produce immune information. Andreas Westfield and Gritta Wolf [3], in this work author have described a steganographic system which embeds secret messages into a video stream. Normally the compression methods are used in video conferences for securing acceptable quality. But usually, compression methods are lossy because reconstructed image may not be identical with the original. There are some drawback of compression and data embedding method. Signal noise and irrelevance are common examples of data embedding. But compression methods try to remove signal noise and irrelevance. If signal is compressed more, then there are fewer possibilities of data embedding. The author have solved this problem, they have investigated a typical signal path for data embedding.

In this algorithm security is established by indeterminism within the signal path. Sherly A P and Amritha P [14], in this paper author have proposed a new compressed video Steganographic scheme. In this scheme the data is hidden compressed domain. The data are embedded in the macro blocks of I, P frames and in B frames. The novel embedding technique Triway Pixel Value Differencing (TPVD) is used to increase the capacity of the hidden secret information and for to providing an imperceptible stegoimage for human vision. This algorithm can be applied on compressed videos without degradation in visual quality. Saurabh Singh and Gaurav Agarwal [13], have presented a novel approach of hiding image in a video. In this approach, one LSB of each pixel is replaced by the one bit of secrete message. So It is very difficult to find that image is hidden in the video of 30 frames per second. The analysis is very difficult because each row of image pixels is hidden in multiple frames of the video.

The intruder requires full video to unhide image. Authors have described the LSB algorithm in this paper. The proposed algorithm is very useful in sending sensitive information securely. S. Suma Christal Mary [12], have proposed new Real time Compressed video secure



Steganography (CVSS) algorithm using video bit stream. In this, embedding and detection operations are both executed entirely in the compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity. At present we are hiding the data in video format, so in the future implementation of uncompressed formats may possible as well, so it may support MPEG4 format [16]. Multiple frames embedding are possible. Now we are embedding single frame at a time, but in future multiple frames embedding is also possible.

III Process for the secret Information Hiding

Fig 1 Steganography

The Basic Operation Of Steganography:

This procedure is divided into several operations.

1. Encryption
2. Data chunking
3. Applying steganography
4. Sending this chunked files
5. File recombination
6. Decryption

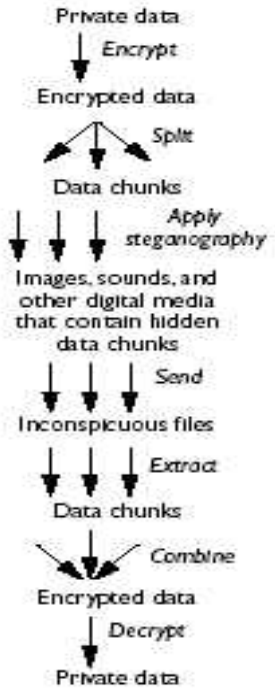
In steganography information can be hidden in carriers such as images, audio files, text files, and video and data transmissions. When message is hidden in the carrier a stego carrier is formed for example a stego-image. Hopefully it will be perceived to be as close as possible to the original carrier or cover image by the human senses.

Images are the most widespread carrier medium. They are used for steganography in the following way. The message may firstly be encrypted. They are used for steganography in the following way. The message may firstly be encrypted. The sender embeds the secret message to be sent into a graphic file. This results in the production of what is called stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey etc. This

stego-image is then

1) Encryption:-

Fig 2 : Procedure of Steganography



transmitted to the recipient.

The recipient extractor extracts the message from the carrier image. The message can only be extracted if there is a shared secret between the sender and the recipient. This could be the algorithm for extraction or a special parameter such as stego key.

To make a steganographic communication even more secure the message can be compressed and encrypted before hidden in the carrier. Cryptography and steganography can be used together. If compressed message will take up far less space in the carrier and will minimize the information to be sent. The random looking message which would result from encryption and compression would also be easier to hide than a message with a high degree of regularity. Therefore encryption and compression are recommended in conjunction with steganography.

The object file which is supposed to be proceed will be encrypted in some binary codes. This binary codes depends on the nature of the object file. This encryption is different for different files. As, example the encryption is made of text file which is absolutely different from any audio file or image files.

2) Data Chunking:-

In this process the encrypted file is chunked in various parts and then this file is to be proceed for the further streganography. The aim of this step is to reduce the stenography time and increase the effectiveness of this procedure.

3) Steganography:-

In this process the steganography is done on the chunked encrypted files. In this process the binary codes of the encrypted files are to be changed by any of the method as mentioned below. Specific method changes the specific binary numbers.

decrypted so that the receiver can get the original file which is sent from the sender. And now by entering the secret information the receiver is supposed to get the original file which is sent by thesender. This procedure ends the whole procedure.

4) Sending the chunked files:-

In this process this chunked files are supposed to be sent to the receiver and this files will be in the hidden form. This all files are received by the receiver and then are proceed to get the original data.

5) File recombination:-

In this process the chunked files are supposed to be recombined to get the whole file and this procedure are done on the receiver end, so the receiver must have the stego-key or any secret information from the sender so that the receiver can get the original file.

6) Data Decryption:-

In this process the previously recombined file is to be decrypted so that the receiver can get the original file which is sent from the sender. And now by entering the secret information the receiver is supposed to get the original file which is sent by thesender. This procedure ends the whole procedure.

IV. ADVANTAGES

Less computational time:

Since the proposed system uses indexing concept, the process of retrieving the secret data from the steganographed video becomes very simple and requires very less time.

Highly secure:

Since random data are also placed in unused frames in the video, the attacker is left clueless to know the real secret data hidden in the video. Hence highly confidential data like military secrets and bank account details can be easily steganographed in ordinary video and can be transmitted over internet even in unsecured connection.

V. CONCLUSION

We presented a reduced distortion bit-modification algorithm for LSB video steganography. The key idea of the algorithm is data bit embedding that causes minimal embedding distortion of the host audio. Listening tests showed that described algorithm succeeds in increasing the depth of the embedding layer from 4^{th} to 6^{th} LSB layer without affecting the perceptual transparency of the watermarked audio signal. The improvement in robustness in presence of additive noise is obvious, as the proposed algorithm obtains significantly lower bit error rates than the standard algorithm. The steganalysis of the proposed algorithm is more challenging as well, because there is a significant number of bits flipped in a number in bit layers and the adversary cannot identify exactly which bit layer is used for the data hiding

VI .REFERENCES

[1] Ahmed Ch. Shakir," Steno Encrypted Message in Any Language for Network Communication Using Quadratic Method", Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.

[2] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J.Robles, and Maricel O.Balitanas," Data Hiding in Video", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009

[3] Andreas Westfeld and Gritta Wolf," Steganography in a Video Conferencing System", Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998.

[4] Cheng Cheok Yan, "Introduction on Text Compression Using Lempel, Zip, Welch (LZW) method".

[5] D.P.Gaikwad and Dr. S.J.Wagh, "Image Restoration Based LSB Steganography for Color Image", AISA-PACIFIC Regional Conference in ICTM-2010 on Innovations and Technology Management at Mumbai.

[6] Richard E. Woods & Rafael C. Gonzalez "Digital Image Processing", Book.

[7] F 5 algorithm implementation: 2009, Fridrich, J.R.Du, M. Long: Steganalysis in Color Images, Binghamton, 2007.

[8] Neil F. Johnson and Sushil Jajodia,"Exploring Steganography: Seeing the Unseen", George Mason University.

[9] S. Suma Christal Mary, "Improved Protection In Video Steganopgraphy Used Compressed Video Bitstream ," International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397.

[10] Saurabh Singh and Gaurav Agarwal,"Hiding image to video: A new approach of LSB replacement", International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003.

[11] Steganography on new generation of mobile phones with image and video processing abilities, as appeared Computational Cybernetics and Technical Informatics (ICCCCONTI), 2010 International Joint Conference on 27-29 May 2010 in Timisoara, Romania ISBN: 978-1-4244- 7432-5.

[12] Y. J. Dai., L. H. Zhang and Y. X. Yang.: A New Method of MPEG Video Steganographying Technology .International Conference on Communication Technology Proceedings (ICCT), 2003.

[13] D.-C. Wu and W.-H. Tsai: A steganographic method for images by pixel-value differencing, Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.

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

[15]Sherly A P and Amritha P P,"A Compressed Video Steganography using TPVD", International Journal of Database Management Systems(IJDMS) Vol.2, No.3, August 2010 DOI: 10.5121/ijdms.2010.2307 67