ISSN:2320-0790

An International Journal of Advanced Computer Technology

Covert Communication Using a Dissimilar Cover

H S Jayaramu[1], K B ShivaKumar[2], Srinidhi G A[3], A K Goutam[4]

[1,2,3]Department of TCE, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India.
[4]S D College of Engineering, Muzaffarnagar, Uttar Pradesh, India

Abstract: Communication is all about information exchange. Recently with the advancement in technology and the rapid exponential growth in the means of communication there are various domains emerged in the field of communication. Data hiding is a recently developed technique in the field of information security and has received significant attention from both academia and industry. Steganography is the practice of encoding secret information in a manner such that the very existence of the information is concealed. Steganography means hiding data inside cover objects such as images that will escape detection and can be retrieved with no distortion at the receiver. The messages such as images, videos, audio files, text and other computer files can be hidden inside images or other digital objects. The purpose of Steganography is not to keep others from knowing the hidden information – it is to keep others away from thinking that the information even exists. This paper presents one of the latest advancements accomplished in the field of data security. In this project a secret text message, technically known as the payload is embedded into a video which is called the cover video. For a general view it seems as a simple video file that is transmitted finally but actually it has got the secret text message hidden in it.

Keywords: Video Steganography, Data hiding, text steganography, video steganography.

I. INTRODUCTION

In the present e-communication scenario, data security is one of the major challenges. After the World War II, the need for a secure and robust communication between the communicating entities has increased due to the fear of terrorism, the publishers of digital audio and video are worried about their works that would be corrupted by illegal copying or redistribution and hence it is of prime importance to protect information and enable secure communication.

During fifteenth century, artists hide some imperative information in their paintings so that the image seems normal to an onlooker, but on observing at an angle reveals the information. During World War II, with the advancement in technology, invisible inks were invented to write messages on a sheet of paper and at the receiver side; some chemical processing was used to retrieve messages. Due to the advent of computers and internet, old steganographic techniques have given way to digital steganography, in which multimedia files are used as hiding medium. Steganography is an alternative to cryptography in which the secret data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. Basically, the purpose of cryptography and steganography is to provide secret communication.

Cryptography deals with scrambling of the structure of a message to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it but the third party will can make a guess easily that there is secret information is being communicated. Cryptography can also provide authentication for verifying the identity of someone or something. In contrast, steganography does not alter the structure of the secret message, but hides it inside a cover-video so it cannot be seen. i.e, this technique does not give any chance for the hackers to get a doubt unless the quality of the carrier gets degraded. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not.

In other words, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

The concept of steganalysis is to discover the hidden messages and to determine their attributes. Steganalytic attacks can be used to distinguish between cover and stego objects. The two major steganalytic methods are targeted attacks and blind steganalysis. The blind steganalysis approaches are not tailored to any embedding paradigm whereas the targeted attacks use the knowledge of the embedding algorithm.

As the original video is difficult to obtain, the blind analysis has become widely applicable research focus of

steganalysis. Blind steganalysis considered being a universal technique which can detect a wider class of steganographic techniques and therefore generally it is less accurate compared to targeted steganalysis. But still it is irreplaceable detection technique if the embedding algorithm is unknown. Steganalytic attacks can be broadly classified as visual attacks, statistical attacks and structural attacks.

In visual attacks the naked eye can identify the altered change in the nature of cover video by steganography of cover medium. The changes in the statistical behavior/properties of cover medium are taken for consideration in statistical attacks. In structural attacks, the changes in the format of data field when secret data is embedded are capable of detecting the existence of image.

The paper is organised as below: In section II litrature review relevant to the topic are explained. Section III deals with the proposed model and section IV with the proposed algorithm. Section V concludes the paper.

II LITRATURE REVIEW:

Katzenbeisser and Petitcolas[1] proposed information hiding techniques for steganography and digital Watermarking in which the spatial frequency (computed from the amplitude of Fourier transform) and the orientation (computed from the phase of Fourier transform) components are transmitted in to eye to cortex through different channels. The masking effect occurs when channel component is invisible due to higher energy component in neighboring channel. It is commonly admitted that Watermark must survive all image manipulations that do not damage an image beyond usability.

Tobla et.al.,[2] presented colored image-stegnography using integer wavelet transforms where the daubechies lifting wave transform applied on cover image to generate four sub-bands and LWT is applied on two diagonal sub-bands to generate blocks and remaining two sub- bands and retained in spatial domain itself. Hemalatha et.al.,[3] proposed a steganography technique to hide multiple secret images and keys in cover image using Integer Wavelet Transform (IWT). Shejul.A.Kulkarni et al.,[4] proposed a secure Skin Tone Based Steganography technique where secret data embedding is performed using frequency domain approach. Secret data is hidden in one of the high frequency subband of DWT by tracing skin pixel in that sub-band. Mausd .,et al.,[5] proposed LSB based Images stegnography which enhances the existing LSD substitution technique to improve security level of hidden information. The security conception hides secret information with in LSB of image where a secret key encrypts the hidden information to protect from unauthorized users the hidden information is stored in to specific position of LSB of image depending on secret key the PSNR value gives optimized result because this method changes very small number of bits of image. Xie Qing et al., [6] proposed information hiding algorithm of adaptive multiple plane bit based on spatial domain in color image, which has low computing complexity and high capacity of information hiding. The main idea is to judge each pixel and then embed hidden information in the designated point behind the highest non-zero bit until another designated point is found according to human visual characteristics. Sachdeva S et.al.,[7] proposed color image steganography based on modified quantization table. This Steganography method is compared with a method JPEG-JSteg. Two performance parameters namely capacity and stego size are compared. Rong-Jian Chen et.al.,[8] explained that the embedding algorithm adaptively evaluates the most similar value to replace the original one by embedding logo data into cover data then adaptively adjust the LSB's of cover data and later adaptively adjust MSB's of cover data.

Shankar Roy et.al.,[9] proposed a secure keyless image steganography approach for lossless RGB images using the compression technique to increase security level and storage capacity. Storage capacity is improved by utilizing all the color channels for storing information and providing the text message compression. Mandal J K et.al.,[10] proposed steganographic technique based on minimum deviation of fidelity where two bits/bytes are replaced by choosing the position randomly between LSB up to MSB. Mandal, J. K et.al.,[11] proposed a DWT based frequency domain steganographic technique termed as WTSIC where the cover PPM image is transformed DWT resulting for sub-image components. Secret image/ message bit stream in varying positions are embedded in all 3 components. The experimental results against statistical and visual attack are computed and compared with the existing steganographic algorithms. Sarreshtedari S et.al.,[12] proposed high capacity image steganography in wavelet domain the wavelet transform co-efficient of the original image to embed the secret data. This is achieved through retaining integrity of the wavelet coefficients at high capacity embedding.

Rubab S et.al., [13] proposed an algorithm to hide the text in any colored image of any size using wavelet transform. It improves image quality & imperceptibility. This method sustains security attacks. S.Hemalatha,.et.al.,[14] proposed a image steganography technique to hide multiple secret images & keys in color image using DWT. Extracted secret images are similar to the original secret images. The results are compared with the results of other technique where single image is hidden. Ghoshal N et.al.,[15] proposed that

the image authentication is done by hiding secret image in frequency components of carrier image. Robustness is achieved by hiding an authenticating or secrets image in frequency component. IDFT is performed after embedding to transform embedded image in frequency domain to spatial domain. The technique is also applicable for secret data transmission through carrier color image by hiding secret data.

III PROPOSED MODEL

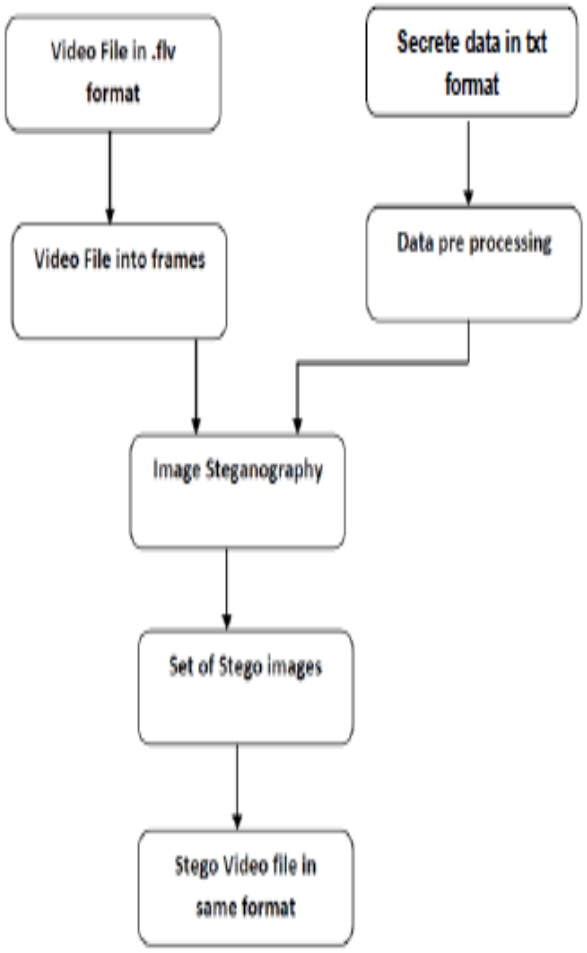

Fig 1: Proposed data hiding Scheme

- Stego video: The final video file which is obtained after the completion of embedding and post processing of stego images is called stego video. This video file should remain apparently same as the video file considered in the beginning.
- Cover Video: Secrete information carrier is cover video which may be any size and format, for example mp4, mpeg, flash video, HD video, real video etc. A cover video can be divided into number of frames and each frame is consists of number of pixels.
- Payload: Our secret information is known as payload which will be in the form of text. Payload can get from user by using a graphical user interface which can be developed by using MATLAB. Same user interface can be used to take the data to be transmitted to the receiver from the sender so that there will be flexibility for the user to reuse.
- Embedding: Read the character length of secret information convert into equivalent of ASCII or binary representation. Replace LSB of first frame of cover video into character length of secrete information, remaining frames of one to four bit LSB replaces with secrete information bit. Now convert frames back in uncompressed avi format.
- Decoding Read an avi video and convert into number of frames and get message length from first pixel. Read remaining frame of first pixel of decimal value and convert to character.

The concept followed here is to consider a video file which is converted into a set of images by using a special MATLAB code and then follow a steganography algorithm to embed the data in text(.txt) format to obtain a set of stego images. This set is converted back into a video file which is called the stego video in the same format and other features as that of the cover video file.

IV: ALGORITHM

A. Embedding:

- First take any video format
- Read frames from video
- Read a message from user
- Convert the message to the set of character and get the decimal ASCII code of Character.
- Save the message length in first frame
- Replace first pixel of all subsequent frames with decimal ASCII code
- Write the frames back in uncompressed .avi format

B. Decoding:

- Read avi video
- Read First frame get message length from first pixel
- Read remaining all frame get decimal value convert to character

V. CONCLUSIONS

Security plays a vital role in all aspects of life and technology. As the technology grows, it bounds in the positive direction, so do the reverse engineering of it. Data security has been of chief concern these days and plays a

major role in terms of its complexity. One such means of providing data security is using steganography.

This paper Covert Communication Using a Dissimilar Cover is one of the latest advancements accomplished in the field of data security. In this model, a secret message, technically known as the payload is embedded into an video frames which is called the cover video. Our payload which is text will be embedded into a cover video and resulting a stego video file. For a general view it seems as a simple video file that is transmitted finally but actually it has got the secret message and text message hidden in it. Our technique is unique and distinct from other existing techniques.

REFERENCE:

[1] Katzenbeisser, S. And Petitcolas F.A.P., "Information Hiding Techniques For Steganography and Digital Watermarking," Artech House, Inc., Boston, London (2000).

[2] M. F. Tolba, M. A. Ghonemy, I. A. Taha, A. S. Khalifa, "Using Integer Wavelet Transforms InColored Image-Stegnography", International Journal on Intelligent Cooperative Information Systems, Volume 4, pp. 75-85. (2004).

[3] Hemalatha S., U. Dinesh Acharya., Renuka A. And Priya R Kamath, "A Secure And High Capacity Image Steganography Technique," International Journal,Volume-4, Febrauary (2013).

[4] Shejul.A.Kulkarni, U.L., "A Secure Skin Tone Based Steganography (SSTS) Using Wavelet Transform," International Journal Of Computer Theory And Engineering, Vol.3, No.1, pp. 16-22 (2011).

[5] Masud, Karim S.M., Rahman, M.S., Hossain, M.I., "A New Approach For LSB Based Image Steganography Using Secret Key," International Conference On Computer And Information Technology, IEEE Conference Publications, pp 286 – 291 (2011)

[6] Xie Qing., XieJianquan., XiaoYunhua., "A High Capacity Information Hiding Algorithm In Color Image.", 2nd International Conference On E-Business And Information System Security, IEEE Conference Publications, pp 1-4 (2010).

[7] Sachdeva S and Kumar A, "Color Image Steganography Based on Modified Quantization Table," Second International Conference On Advanced Computing & Communication Technologies, IEEE Conference Publications, pp 309 – 313 (2012).

[8] Chen, R.J., Peng, Y.C., Lin, J.J., Lai, J.L., Horng, S.J. Novel Multi-Bit Bitwise Adaptive Embedding Algorithms With Minimum Error For Data Hiding. Fourth International Conference On Network And System Security (NSS 2010), IEEE Conference Publications, pp. 306 – 311,(2010).

[9] Roy, S., Parekh, R., "A Secure Keyless Image Steganography approach For Lossless RGB Images," International Conference On Communication, Computing & Security, ACM Publications, pp 573-576 (2011).

[10] Mandal, J K, Sengupta M , "Steganographic Technique Based On Minimum Deviation Of Fidelity (STMDF)," Second International Conference On Emerging Applications Of Information Technology, IEEE Conference Publications, pp 298 – 301, (2011).

[11] Mandal, J.K., Sengupta, M. "Authentication/Secret Message Transformation Through Wavelet Transform Based Subband Image Coding(WTSIC).", International Symposium On Electronic System Design, IEEE Conference Publications, pp 225 – 229, (2010)

[12] Sarreshtedari S and Ghaemmaghami S, "High Capacity Image Steganography In Wavelet Domain," IEEE Consumer Communications and Networking Conference (CCNC), IEEE Conference Publications, pp 1-5, (2010).

[13] Rubab S and Younus M, "Improved Image Steganography Technique for Colored Images Using Wavelet Transform," International Journal of Computer Applications, Volume 39, No.14, pp 29-32(2012).

[14] Kapre Bhagyashri S, Joshi M Y, "All Frequency Band DWT-SVD Robust Watermarking Technique for Color Images in YUV Color Space," IEEE International Conference On Computer Science And Automation Engineering (CSAE), IEEE Conference Publications, pp. 295-299, (2012).

[15] Ghoshal N and Mandal J K, "A Steganographic Scheme for Colour Image Authentication (SSCIA)," International Conference On Recent Trends In Information Technology, IEEE Conference Publications, pp.826 -831, (2011).

[16] S Hemalatha, U DineshAcharya, A Renuka and Priya R Kamath "A Secure Image Steganography Technique To Hide Multiple Secret Images," Fourth International Conference On Networks & Communications, LNEE, Springer, pp 613-620 (2012).