ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 2, February 2015

5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

Flawless Data Hammering in Videos

B. Almitha Anselin Burna[1], G. Arul Dalton[2]

Dept of Computer Science and Engineering, Magna college of Engineering, Magaral, Anna University, chennai, India[1,2]

ABSTRACT: The science of securing a data by encryption is Cryptography whereas the method of hiding secret messages in other messages is Steganography, so that the secret's very existence is concealed. The term 'Steganography' describes the method of hiding cognitive content in another medium to avoid detection by the intruders. This system combines cryptography and steganography to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. The Data is secured by converting it into cipher text by TDES algorithm using a secret key and conceal this text in another video by steganography method. The communicated data is hidden into the multimedia file using video steganography without losing its perceptible quality using Junk space replacement method thereby quality of the video is not compromised.

KEY WORDS: Data hiding, Video steganography, Junk space Replacement

I. INTRODUCTION

Currently, Internet and digital media are getting more and more popular. So, requirement of secure transmission of data also increased. Various good techniques are proposed and already taken into practice. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data Hiding 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. Generally, in Data Hiding, 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 is sent through the network to the recipient, where the actual message is separated from it.

The requirements of any data hiding system can be categorized into security, capacity and robustness. All these factors are inversely proportional to each other creating the so called data hiding dilemma. The focus of this paper aims at maximizing the first two factors of data hiding i.e. security and capacity coupled with alteration detection. The proposed scheme is a data-hiding method that uses high resolution digital video as a cover signal. the proposed recipient need only process the required steps in order to reveal the message; otherwise the existence of the hidden information is virtually undetectable. The proposed scheme provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms because here we consider application that require significantly larger payloads like video-in-video and picture-in-video.

II. PREVIOUS WORKS

As video file consist of several image sequence, so considering the data hiding technique of image will also apply for video data hiding.

2.1. Least-significant bits technique

The most widely used technique to hide data, is the usage of the LSB. Although there are several disadvantages to this approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside a image, a proper cover image is needed. 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. Thus, a 800 × 600 pixel image can contain a total amount of 1.440.000 bits

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 2, February 2015

5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

(180.000 bytes) of secret data. For example, the following grid can be considered as 3 pixels of a 24 bit color image, using 9 bytes of memory:
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
When the character A, which binary value equals 10000001, is inserted, the following grid results:
(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)
In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The resulting changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden.

While using a 24 bit image gives a relatively large amount of space to hide messages, it is also possible to use a 8 bit image as a cover source. Because of the smaller space and different properties, 8 bit images require a more careful approach. 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 color, as another color in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in grayscale, as the human eye will not detect the difference between different gray values as easy as with different colors.

2.2. Masking and filtering

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the 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 anomalies.

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. The information is not hidden at the ”noise” level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used.

III. PROPOSED WORK

The main high resolution AVI fie is nothing but a sequence of high resolution image called frames The secret information to be hided is encrypted and hided in the junk space of the video file without affecting the perceptible quality of the video. Receive an input text file from the user. The content of the text file is to be hiding inside the video. File chooser is used as the interface of the user. Convert the text file content into the chipper text by using encryption algorithm. Receive an input video file for hiding an encrypted text into the junk space of the video. AVI movies are used to give as the input. Navigator interface provides the easier interaction between the user and input file to get the input. Embedding is the inbuilt process which has been done in the back end of the system. It embeds the message in to AVI file. Extract to get the hidden encrypted file from an embedded video. It separates the message from the AVI file without affecting its content. It will check that the user is valid before extracting the message from the AVI File. Decryption is the inverse process of the encryption. It gives the original message in readable format. Decryption process is done using a same algorithm which is used in encryption process. The extracted message is decrypted using same key.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 4, Special Issue 2, February 2015

5th International Conference in Magna on Emerging Engineering Trends 2015 [ICMEET 2015]

On 27th & 28th February, 2015

Organized by

Department of Mechanical Engineering, Magna College of Engineering, Chennai-600055, India.

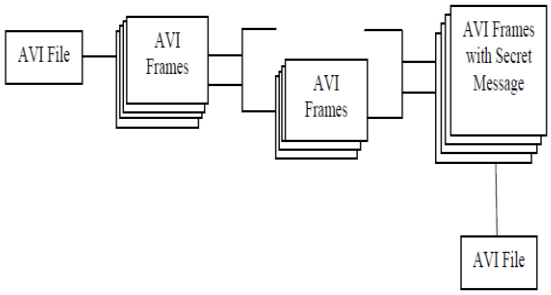

Figure:AVI video Streaming and Data Hiding

Advantage

The proposed method is found to have lower distortion to the quality of the video even though data size increase.
Retrieval of hidden data tend to be accurate
Pixel breakage is avoided
Loss of Image quality is at minimum

IV. CONCLUSION

Data hiding is becoming one of the most rapidly advancing techniques in the field of research especially with increase in technological advancements in internet and multimedia technology. With the technology advancing on one side, so has the rate of threat to hack, tamper or steal the data that is being transmitted over these medial also increased in leaps and bounds. To cater the above needs this paper has been proposed Flawless Data Hiding in Videos and I implemented the encryption of data to be hided and preprocessing the video in which the data to be hided. The encrypted text will be embedded into the pre-processed video, extraction of embedded data from the video and decoding the extracted data will be implemented. The above mentioned implementations will make this project as very useful tool for secure & robust transmission of secret data by hiding the information inside video without affecting the perceptible quality of the video.

REFERENCES

[1] G. J. Sullivan , J. Ohm , W.-J. Han and T. Wiegand "Overview of the High Efficiency VideoCoding (HEVC) standard", *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, pp.1649 -1668 2012
[2] I. Cox , M. Miller , J. Bloom , J. Fridrich and T. Kalker " *Digital Watermarking and Steganography"*, 2008 :Morgan KaufmannPublishers Inc.
[3] A. Khan , S. A. Malik , A. Ali , R. Chamlawi , M. Hussain , M. T. Mahmood and I. Usman "Intelligent reversible watermarking and authentication: Hiding depth map informationfor 3D cameras", *Inform.Sci.*, vol. 216, pp.155 -175 2012
[4] S. Bhattacharya , T. Chattopadhyay and A. Pal "A survey on different video watermarking techniques and comparativeanalysis with reference to H.264/AVC", *Proc. IEEE 10th Int. Symp. Consum.Electron*, pp.1 -6 2006
[5] A. Alattar , E. Lin and M. Celik "Digital watermarking of low bit-rate advanced simple profile MPEG-4 compressedvideo", *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, pp.787 -800 2003.
[6] M. Stamm , W. Lin and K. Liu "Temporal forensics and anti-forensics for motion compensated video", *IEEE Trans. Inform. Forensics Security*, vol. 7, no. 4, pp.1315 -1329 2012
[7] O. Cetin and A. T. Ozcerit "A new steganography algorithm based on color histograms for dataembedding into raw video streams", *Comput. Security*, vol. 28, no. 7, pp.670 -682 2009
[8] A. Cheddad , J. Condell , K. Curran and Kevitt "Digitalimage steganography: Survey and analysis of current methods", *SignalProcess.*, vol. 90, no. 3, pp.727 -752 2010
[9] K.-L. Chung , Y.-H. Huang , P.-C. Chang and H.-Y. Liao "Reversibledata hiding-based approach for intra-frame error concealment in H.264/AVC", *IEEE Trans.Circuits Syst. Video Technol.*, vol. 20, pp.1643 -1647 2010
[10] T. Stutz and A. Uhl "A survey of H.264 AVC/SVC encryption", *IEEETrans. Circuits Syst. Video Technol.*, vol. 22, pp.325 -339 2012