ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

A Prototype for Secure Information using Video Steganography

S. Deepa[1], R. Umarani[2]

Asst Professor, Dept of Computer Science, Arignar Anna Government Arts College for Women, Vellore, India [1]

Associate Professor, Dept of Computer Science, Sri Sarada College for Women, Salem, India [2]

Abstract: Steganography is a science that considers the method to hide information in the cover media. The direct purpose is the communication with the secret information. The methods can be classified based on the cover media and secret message type. The cover media can be audio, video, image or even text message. Similarly, the secret message can be images, audio, video and text messages. The challenge here is to cover the secret information properly without degrading the cover media, without noticing and with security. The proposed steganography algorithm based on color histograms for data embedding into Video clips directly, where each pixel in each video frame is divided in two parts, the number of bits which will be embedded in the right part are counted in the left part of the pixel. This algorithm is characterized by the ability of hiding larger size of data and the ability of extracting the written text without errors, besides it gives a high level of authentication to guarantee integrity of the video/images before being extracted. Furthermore, the data were embedded inside the video/images randomly which gave the video/images a higher security and resistance against extraction by attackers.

Keywords: Video Steganography, Signal-to-Noise Ratio (SNR), Histogram, Threshold.

I. INTRODUCTION

Data hiding techniques can be used to embed a secret message into a compressed video bit stream for copy-right protection, access control and transaction tracking. Some data hiding techniques assess the quality of compressed video in the absence of the original reference. The quality is estimated based on computing the degradations of the extracted hidden message. Data hiding is also used for error detection and concealment in applications of video transmission. With the development of the computer and the increase of its use in different areas of life and work, the issue of security of information had gained special importance. One of the concerns of information security is the concept of hidden exchange of information. For this purpose, various algorithms including steganography, cryptography, and so on, have been used. Some of these algorithms depend on hiding data directly in a special domain, where a part of the image is replaced by the secret message. These Algorithms are characterized by the ability of high storage of data (payload) but they can't resist hacking. There are other algorithms that depend on changing the image shape into another using discrete cosine functions (Transform Domain), then embedding the secret message inside the new shape of the image. These algorithms are characterized by resisting hacking, but it can't hide much data.

II. VIDEO BASICS

A video consists of a set of frames (images) that are played back at certain frame rates based on the video standards. Quality of the video depends on a set of parameters such as the number of pixels in a frame, the fps (frames per second), and frame size .The fps parameter is almost standard (between 24 and 30 fps) in many common video formats, however, the other two parameters present several altered from one video standard to another. Each image, which is called a frame, consists of pixels having three or four color compounds such as RGB (Red Green Blue) or CMYK (Cyan Magenta Yellow Black). The rest of the intermediary colors are composed from a mixture of these primary colors. Since the human eye is principally sensitive to green color tones, in some video standards the number of bits of each color compound may differ. For example, the red and blue colors are encoded in 5 bits while the green color consists of 6 bits for 16-bit color standard. In 24-bit RGB color, each red, green, and blue component is 8 bits long and has 256 variants in color density. In the CMYK standard on the other hand, 32-bit is needed and this standard is ordinarily used in modern computer displays. AVI (Audio Video Interleave), which was advanced by Microsoft and IBM as part of RIFF (Resource Interchange File Format) in 1992, is a most common sequence video format. It acts as containers for various sequences of different data types such as audio and video sequences in which the images are stored in BMP (Bit Map) format. Therefore, capacity and resolution computations on bitmap images can be applied to the AVI video sequences without any major change.

III. VIDEO STEGANOGRAPHY

A digital video consists of a set of frames (digital images) that are played back at certain frame rates based on the video standards. The image is a collection of pixels where each pixel is a combination of three colors RGB (Red, Green and Blue). The color of pixel dependent on the numeric value related with each color. Pixels in the image are displayed row by row horizontally. When data is hidden in the videos stego-video get less troubled as compared to other multimedia files. After hiding data in an

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

image, size of the image increases. So compression techniques are necessary. When data is hidden in large size image, the transmission of video over the Internet takes more time and needs higher bandwidth. The size of the video can be reduced by compression technique. Compression techniques are grouped into two types, lossy and lossless.

IV. ALGORITHM

Histograms, arrays of values, indicate the distribution of intensity of colors obtained from each pixels color combination in digital image. The proposed algorithm based on color histograms for data embedding into cover video/images directly, where the cover video is firstly segmented into frames and the histogram values of each frame are calculated. In order to determine appropriate pixels in each video frame for data embedding; first, an evaluating value is computed using the color and motion transitions in each frame by our application. A predefined threshold value controlled by a track bar controls the software user interface. The threshold value, which can be as much as the highest pixel number of the video frame, indicates a certain level of disparity between successive video frames. Histogram variations of consecutive video frames are compared to the threshold value (Histogram constant Value HCV) and appropriate pixels in those frames are selected for data embedding procedures. The higher the threshold values are, the more the perceptibility precision is increased at frame transitions in contrast to a decrease in the number of segmented frames. This consequently means a capacity drop for the embedded data. If the threshold value is configured as low, parameter values mentioned above will be inversed. So each pixel in each video frame is divided in two parts, the number of bits which will be embedded in the right part are counted in the left part of the pixel.

Video's Segmentation and pixels in frames

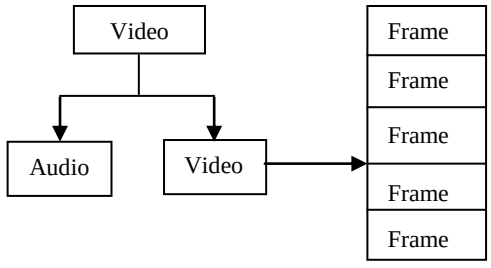

Fig.1. Video divided into frames

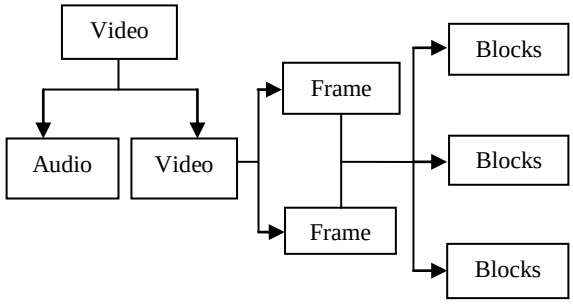

Fig.2. Frame divided into block

The detail of the embedding and extracting algorithms are shown below. The data hiding process is initiated by segmentation of cover-video file into the frames Fig. 1. The average histogram values of frames are calculated and appropriate frames are determined in respect to the HCV parameter.

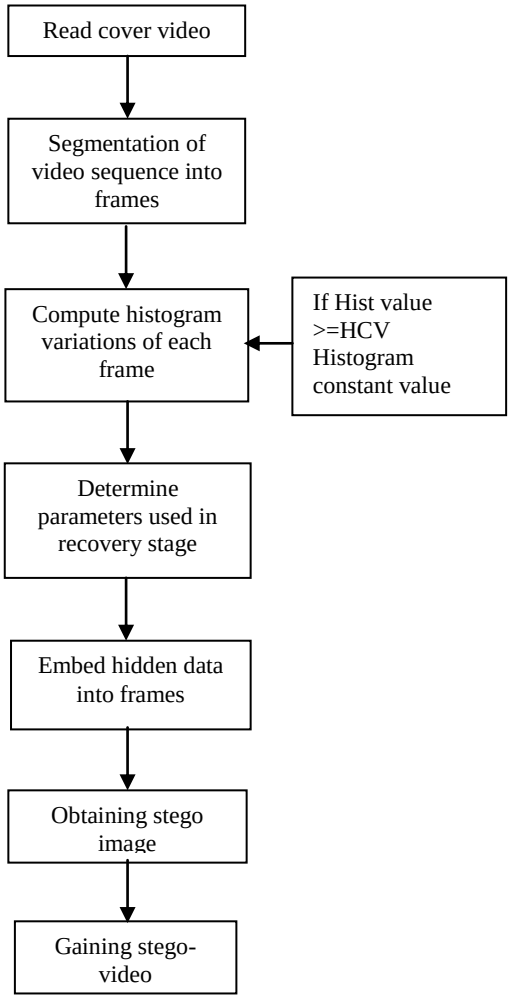

Fig.3. Flowchart of embedding algorithm

1. Initially each selected frame is divided into blocks (n x n) as shown in Fig.2 and then appropriate pixels are determined by comparing consecutive blocks in the frame.

2. For each block calculate difference value D_i for each two consecutive pixels (P_i , P_{i+1}) from equation (1)

$$D_i = (P_i - P_{i+1}) \longrightarrow (1)$$

3. For each block calculate

$$\text{Median} = \frac{\text{SUM}(D_i)}{(n \times n)/2}$$

then calculate M paramater from equation (2)

$$M = \text{FIX}(\sqrt{\text{Median}}) \longrightarrow (2)$$

4. Each pixel in each video frame is divided into two parts MSB and LSB and count NUM = numbers of 1's in MSB

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

part.

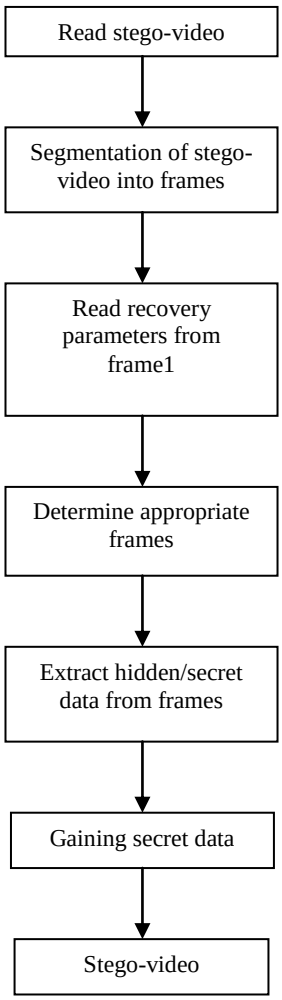

Fig.4. Flowchart of extracting algorithm

Embedding Algorithm

The flowchart is shown in Fig.3.

Input: Secret Data, original selected frames of cover video

Use equations 1 and 2 to Compare D_i for each consecutive pixel with value of M

If $D_{i>M}$ then Embed data in pixels (P_i, P_{i+1})

If $Di < M$ then no data embed in pixels (P_i, P_{i+1})

If NUM = 0 or 4 Embed 1 secret Bit in LSB part.

If NUM = 2 Embed 2 secret Bit in LSB part

If NUM = 1 or 3 Embed 3 secret Bit in LSB part.

Extracting Algorithm

The flowchart is shown in Fig.4.

Input: Stego-video, Stego image for selected frames of Stego-video

Use equations 1 and 2 to Compare D_i for each consecutive pixel with value of M

If $D_{i>M}$ then Extract data from pixels (P_i, P_{i+1})

If $Di < M$ then no data in pixels (P_i, P_{i+1})

If NUM = 0 or 4 Extract 1 secret Bit from LSB part.

If NUM = 2 Extract 2 secret Bit from LSB part

If NUM = 1 or 3 Extract 3 secret Bit from LSB part.

The proposed algorithm is able to hide messages within part of the frames or the whole frames based on HCV value and the random selection of frames and pixels increases the level of security to hide and extract the secret messages.

V. CONCLUSION

In this paper the goal of the proposed steganography algorithm is based on histograms to decrease the faded pixels in each frame, in order to increase the embedding capacity. The experimental results showed that the proposed algorithm improves the embedding capacity, maintains the quality of the stego-video, more efficient, simple, appropriate and accurate than other algorithms, as well as it makes the secret message more secure.

REFERENCES

1. T. Shanableh," Data hiding in mpeg video files using multivariate regression and flexible macro block ordering ", IEEE Transactions on Information Forensics and Security , Vol. 7, pp.455-464 , 2012.
2. Yang C.H., and Tsai M.H.: `Improving Histogram-based Reversible Data Hiding by Interleaving Predictions', IET Image Processing, 2010, 4, pp. 223-234.
3. M. H. S. Shahreza and M. S. Shahreza, "Arabic/Persian Text Steganography Utilizing Similar Letters With Different Codes", the Arabian Journal for Science and Engineering, Volume 35, Number 1b pp. 213 - 222, April 2010.
4. Sharma V.K. Shrivastava V.,"A steganography algorithm for hiding image in image by improved LBS substitution by minimize detection", Journal of Theoretical and Applied Information Technology, Vol. 36, No. 1,pp. 1-8, 2012.
5. Singh N., Bhati B.S., Raw R.S., "Digital image Steganalysis for computer forensic investigation", Computer Science and Information Technology (CSIT), pp. 161-168, 2012.
6. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al - Qershi, "Image Steganography Techniques: an Overview", International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3): 2012.