ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

Identical Frames Based Video Steganography

Sukhjinder Singh[1], Neeraj Gill[2], Gagandeep Kaur[3]

Student, Dept. E.C.E, GZS PTU Campus, Bathinda, India [1]

Associate Professor, Dept. E.C.E, GZS PTU Campus, Bathinda, India [2]

Assistant Professor, Dept. E.C.E, GZS PTU Campus, Bathinda, India [3]

Abstract: Steganography is a technique employed for hiding the secret data under cover object. It resolves the problem of network security and provides secure communication through public and private channels. The cover can be text, image, audio or video. In this technique, the secret information is concealed in a video cover. Video file contains some identical frames, which are selected to hide the data. When steganography by this process is used, the probability to uncover the secret information by an attacker is very less as compared to the other methods to hide data frame-by-frame in a sequential manner. It also increases the robustness of data in case of frame dropping and frame adding attacks. In this proposed work a modified technique has been used to embed the data. This technique involves the application of wavelet transform on cover file followed by the application of LSB technique in sub bands. Lower frequency sub-band is selected to hide the encrypted data in cover file. The performance metrics such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Mean Absolute Error (MAE), have been considered for experiment verification.

Keywords: Wavelet transform, Identical frames, Encrypted data, LSB

I. INTRODUCTION

Security is a critical issue in communication systems. This issue can be better resolved by using steganography techniques in a communication system. In steganography valuable information is concealed under the cover object and is transmitted to the target with minimum risk of detect ability [1]. This property of steganography raised its need in all areas such as commerce, banking, national security services, and other private communication systems. Cryptography can also be used along with the steganography. Cryptography protects the content of data by scrambling it and without unscrambling no one can read the data [4]. Steganography hide the existence of data and cryptography secures the content of data. Combination of steganography and cryptography provides additional security level in communication systems [2]. Digital multimedia files such as images, audio and video can be used as a cover. These are also widely used on internet world. Mostly images are used as a cover for hiding the data. More detailed is the image, the lesser restriction of how much data it can hold without it becoming noticeable [3]. Audio can also be used as a cover medium but capacity of these two covers is less as compare to the video. Video contain number of sequential images (Frames) some of them are almost identical [5]. In this paper, a video has been used as a cover medium to hide the information. Identical frames of video file have been used to hide the information. To select the identical frames, intensity histogram of all the frames has been compared with their adjacent frames intensity histograms and those frames are selected that has less difference in intensity histogram. Threshold value is used to detect the difference in intensity histogram value of frames. In this technique, data is not embedded in sequential frames which enhance the security of secret data and also index is not required to detect the stego frame. At the receiver side stego frames can be detected by identical frame selection method. If some attacks like frame dropping and frame adding occurs in video steganography, the detection of stego frames from index become difficult. But identical frames selection method avoids that problem. Moreover it reduces time for extraction process of data. Cryptography has been also applied on the secret information before embedding to enhance the security level. Many methods have been proposed for cryptography. Two basic methods are: public key cryptography and symmetric key cryptography [6,7]. In this paper, the symmetric key cryptography is considered before employing the steganography technique. In symmetric key cryptography same key is used by the sender and receiver to encrypt and decrypt message respectively. This key is shared between the sender and receiver securely. This method is less complex and takes less time for execution as compared to other methods [8]. But key should be securely shared between sender and receiver because security of data is directly related to security of key.

The wavelet transform analyzes different segments of time-domain signal at different frequencies. Use of lifting scheme is simple and efficient algorithm for deriving the wavelet transform as compare to traditional methods. Lifting scheme calculates wavelet transform with some sequential lifting steps. These steps are *split*, *predict*, and *update*. Splitting of signal is also known as Lazy Wavelet Transform [15]. Lifting scheme in wavelet transform has been recognized as a faster approach and also reduces the computational complexity. In this technique, Lazy Wavelet transform has been applied on identical frames which provide sub-bands of different frequencies. Data has been embedded only in low frequency bands because low frequency signal is less

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

affected by noise as compare to the high frequency signal [10]. Data is encoded in LSB of each element of RGB (Red, Green, and Blue) component using LSB technique.
The section I represents the basic introduction to cryptography, steganography and the proposed method of video steganography. Section II describes the System Model, section III deals with Results. Paper is concluded in section IV.

II. SYSTEM MODEL

A. Cryptography

In this work, firstly, the cryptographic operation is performed on secret data. AES (Advance Encryption Standard) algorithm is used for encrypting the data [11]. Symmetric key has also been used in AES method to enhance the security of data. This method distorts the data bits in specific pattern so that nobody can access it without decrypting. Encrypted format of data bits has been embedded into video cover using LSB technique. Then cover file has been sent to the receiver and key has been also shared between sender and receiver in secured manner. At the receiving end after extracting the data from cover, decryption operation has been performed using shared key.
In embedding process, bits of secret data have been embedded into the cover file. Thus, converting the encrypted secret data into a series of bits. Each character of encrypted data is read and then split it into series of bits. Embed this bit series into the cover file using LSB technique [12].

B. Embedding procedure

The video file is broken down into frames [13]. Frames of video are considered as different images, so image steganography technique can be used to hide the data in video file [8]. In used technique identical frames of video file has been selected to hide secret information. Lazy wavelet transform is applied on selected frames to get sub-bands. The data is then embedded in low frequency sub-bands. The length of the embedded data hides in the preliminary elements of frame, in encrypted form.

The whole process is expressed in the form of flow chart in fig 1. After embedding process video is reconstructed from frames. The detail of steganography steps are as follow.

C. Frame selection

A sequence of identical frame is known as video shot [5]. Identical frames are identified from the video file to hide the secret information using intensity histogram comparison of each frame. For that calculate the intensity of frame. Intensity can be calculated as for RGB frame [5].

$$I = 0.299R + 0.587G + 0.114B \quad (1)$$

Where R, G and B represent the Red, Green and Blue channel value of the pixel. Then find the intensity histogram difference i.e. the difference between intensity histogram of

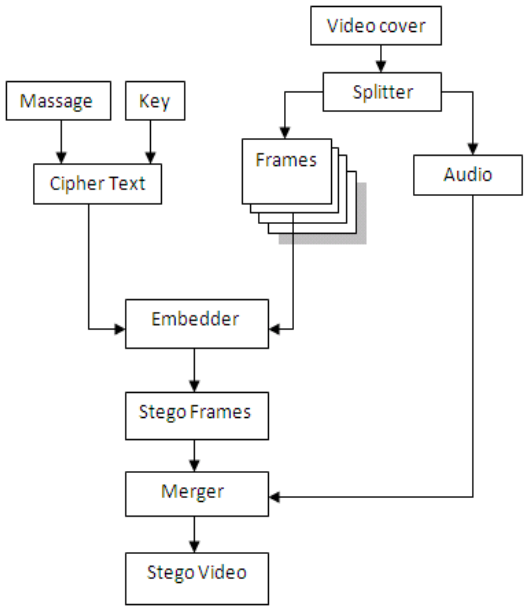

Fig. 1. Flowchart

frame and its adjacent frame. It can be calculated as

$$D_j = \sum_{j=1}^{N} h_j(i) - h_{j+1}(i) \quad (2)$$

Where D_J represents the intensity histogram difference, $h_J(i)$ is value of histogram for j^{th} frame at i level and N denotes total number of level in histogram. Difference in intensity histogram can be detected using a threshold value. Threshold value calculated as [5].

$$T = \mu + \alpha\sigma \quad (3)$$

The frames with intensity histogram difference more than T are selected as identical frames. Here μ is mean value and σ is standard deviation of intensity histogram difference. Value of α varies from 2 to 6.

D. Application of LWT on selected Identical Frames

Each video frame is considered as an image. Now a transformation technique is applied on selected images. In this work, to transform images from spatial domain to frequency domain, wavelet transform has been used. In multimedia files, data get stored in integer form, which avoids the data loss in storing and extraction processes as compare to real form. But many wavelet returns the real values. Use of lazy lifting scheme for wavelet transform overcomes that problem [8]. Lifting scheme does not require complex mathematical calculations. It has an efficient and simple algorithm for wavelet transforms.

2-D lazy wavelet transform process divides the frame into four sub-bands. The four sub-bands, namely the approximate band (LL), vertical band (LH), horizontal band (HL), and the diagonal band (HH).

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

LL	HL
LH	HH

Figure 2: Sub-bands of frame [14]

The approximate band is a low frequency band and holds the most considerable information of the spatial domain image and other bands are high frequency bands and contain information such as edge details [14]. Data is embedded in these sub-bands. Inverse lazy wavelet transform is used to reconstruct the frame from sub-bands.

E. Embedding of data in sub-bands

Generally, the low frequency signal is least affected by noise as compare to high frequency signals [10]. Among four bands of frame, the approximate band has characteristics of low frequency range [14]. So, for the high robustness against noise the approximate band has been selected to hide the data. Data is embedded in the least significant bits of the transform coefficients. Again if this sub-band is over then the same sub-band of next selected frame is used. After embedding all the bits of encrypted message, the video file can be reconstructed from the frames.

To extract secret information from the stego video file reverse steps can be performed to that of hiding information on video file.

III. RESULTS

The simulation is performed on three different video files that act as a cover for encrypted secret data. The information embedded in R, G and B channels of video frames. Properties of test videos described in table I.

TABLE I
PROPERTIES OF TEST VIDEO

Video	Resolution	Length	Frame Rate	No of Frames	Identical Frames
Vipmen	160*120	0.00.09	30f/s	283	8
Traffic	160*120	0.00.08	15f/s	120	9
Rhinos	320*240	0.00.07	15f/s	114	8

A. Video Data

The original images are selected frames from above mentioned video files, used for hiding secret data and after hiding the data resultant image is known as stego image.

Fig. 3. Frame of vipmen video without hiding data and with hiding data

Fig. 4. Frame of traffic video without hiding data and with hiding data

Fig. 5. Frame of rhinos video without hiding data and with hiding data

B. Histograms for Frame

Histogram represents the tonal distribution of digital image. These figures show the histogram of frame before steganography and after steganography with used technique.

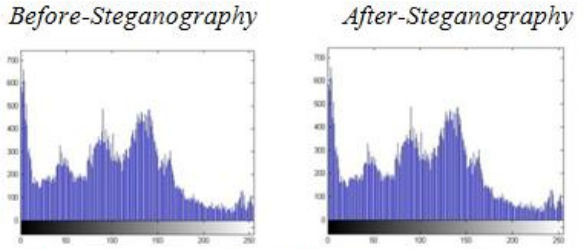

Fig. 6. Histogram of fig 3 without hiding data and with hiding data

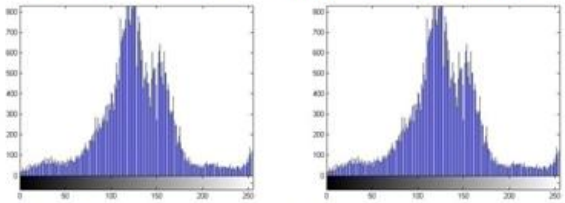

Fig. 7. Histogram of fig 4 without hiding data and with hiding data

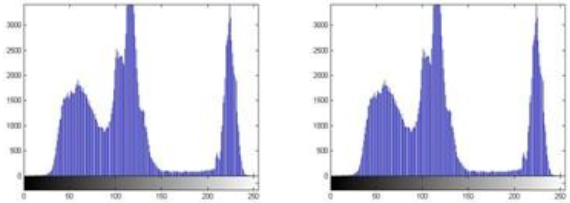

Fig. 8. Histogram of fig 5 without hiding data and with hiding data

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

C. Result Analysis

For result analysis MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio) and MAE (Mean Absolute Error) are measured for original image and stego image. Table 1 show the MSE, PSNR and MAE values of mentioned test images.

TABLE II
MSE, PSNR AND MAE VALUES

Video	MSE	PSNR	MAE
Vipmen	0.0189	65.3688	0.0208
Traffic	0.0187	65.3971	0.0784
Rhinos	0.0048	71.443	0.819

High value of PSNR indicates less distortion caused by data embedding. In this technique data is embedded only in identical frames of each video file. Table II represents different average values of identical frames.

To test robustness of data in case of frame dropping and frame adding some frames are dropped and added randomly in stego video and embedded data has been successfully recovered in those cases. If any stego frame is dropped then remaining frames data can be recovered.

IV. CONCLUSION

Identical frame selection technique in video steganography provides more security to the secret data as well as it increases the quality of stego video. Index is not required to detect stego frames at receiver side, so in case of frame dropping and frame adding attacks stego frames can be easily detected. Selecting low frequency sub-band for embedding information increases robustness of secret data against the noise attack.

REFERENCE

[1] A. Kumar, and K. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[2] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image Steganography Techniques: An Overview" International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012 168

[3] D.Artz, "Digital Steganography: Hiding Data within Data," IEEE Internet Computing Journal, June 2001.

[4] Anju, Babita, Reena, and A. Aggarwal, "An Approach to Improve the Data Security using Encryption and Decryption Technique" IJICT. ISSN 0974-2239 Volume 3, Number 3 (2013), pp. 125-130

[5] T. Tabassum, and S. M. M. Islam, "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT"

[6] Symmetric key cryptography. From Wikipedia http://en.wikipedia.org /wiki/Symmetric_key_cryptography

[7] Public key cryptography. From Wikipedia http://en.wikipedia.org /wiki/Public-key_cryptography

[8] K. Patel, K. K Rora, K. Singh, and S. Verma, "Lazy Wavelet Transform Based Steganography in Video" 978-0-7695-4958-3/13 © 2013 IEEE

[9] R. Polikar, "The Wavelet Tutorial Second Edition"

[10] D. F. H. Al-layla, "*Clearing the detail coefficient of 2-D DWT Architecture based on Lifting scheme of 5/3 and 9/7 Filters*" ISSN:1812125X/2011©IRAQI

[11] J. J. Buchholz , "*Matlab Implementation of the Advanced Encryption Standard*" http://buchholz.hs-bremen.de

[12] A. Swathi, and Dr. S. A. K Jilani, "*Video Steganography by LSB Substitution Using Different Polynomial Equations"* International Journal of Computational Engineering Research Vol. 2 Issue. 5 Issn 2250-3005 September| 2012 Page 1620

[13] E. Agarwal, S. Gupta, and M. A. Chandra, *"Data Hiding Using Lazy Wavelet Transform Strategy" ® (IJCA) (0975 – 8887)*

[14] A. Verma, R. Nolkha, A. Singh, and G. Jaiswal, "*Implementation of Image Steganography Using 2-Level DWT Technique*" IJCSBI, ISSN: 1694-2108 Vol. 1, No. 1. MAY 2013 1

[15] S.T. Abdulwahab, and E. K. Jabbar, "*Proposed Hybrid Algorithm for Generate Database Index Key Based on Image Contents*" IHJPAS VOL.23 (3) 2010