ISSN:0975-9646

Video Steganography by Intermediate Significant Bitplanes

Praneetha S.R
Department of Computer Science
Lourd Matha College of Science & Technology
Kerala University

***Abstract* - The availability of relatively inexpensive digital products coupled with the promise of higher bandwidth and quality of service (QoS) for both wired and wireless communication networks have made it possible to create, replicate, transmit, and distribute digital data without any loss in quality. In such a scenario steganography has received huge attention from the research community round the globe, as it has been found useful for information security and under cover communication. Steganography refers to covert communication for transfer of confidential information over a communication channel. Video Steganography is a technique to hide any kind of files into a carrying Video file. This paper presents a high capacity video steganographic technique. Here the video file is divided into its consequent frames. The secret data is embedded in Intermediate Significant Bit planes of the image. The data to be embedded is broken down in blocks of relatively decreasing lengths and each block is embedded in the cover media under control of a highly secure key. This work shows attractive results with respect to imperceptibility and capacity when compared with a few reported techniques in addition to providing adequate data security.**

Keywords- Embedding; Intermediate Significant Bit; Covert communication; Steganography, Video Steganography

I. INTRODUCTION

Text, image, audio, and video can be represented as digital data. The explosion of Internet applications leads people into the digital world, and communication via digital data becomes recurrent. However, new issues also arise and have been explored, such as data security in digital communications, copyright protection of digitized properties, invisible communication via digital media, etc. Steganography is the art of hiding information in ways that prevent the detection of hiding message[1] whereas cryptographic techniques try to conceal the contents of a message. In steganography, the object of communication is the hidden message and the cover data are only the means of sending it. Secret information as well as cover data can be any multimedia data like text, image, audio, video etc The objective of this work is to develop a Video Steganographic Scheme that can provide provable security with high computing speed, that embed secret messages into images without producing noticeable changes. Here we are embedding data in video frames. A video can be viewed as a sequence of still images[2]. Data embedding in videos seems very similar to images. However, there are many differences between data hiding in images and videos, where the first important difference is the size of the host media. Since videos contain more sample number of pixels or the number of transform domain coefficients, a video has higher capacity than a still image and more data can be embedded in the video. Also, there are some characteristics in videos which cannot be found in images as perceptual redundancy in videos is due to their temporal features. Here data hiding operations are executed entirely in the compressed domain. On the other hand, when really higher amount of data must be embedded in the case of video sequences, there is a more demanding constraint on real-time effectiveness of the system. The method utilizes the characteristic of the human vision's sensitivity to color value variations. The aim is to offer safe exchange of color stego video across the internet that is resistant to all the steganalysis methods like statistical and visual analysis. Image based and video based steganographic techniques are mainly classified into spatial domain and frequency domain based methods. The former embedding techniques are LSB, matrix embedding etc. Two important parameters for evaluating the performance of a steganographic system are capacity and imperceptibility. Capacity refers to the amount of data that can be hidden in the cover medium so that no perceptible distortion is introduced. Imperceptibility or transparency represents the invisibility of the hidden data in the cover media without degrading the perceptual quality by data embedding. Security is the other parameter in the steganographic systems, which refers to unauthorized person's inability to detect hidden data. In this Steganographic scheme the data is embedded in the first three ISB planes under the control of a private key. In order to thwart the adversary data is not embedded sequentially. The key, which is generated using Pseudo Random Number Generator (PRNG), ensures a highly randomized data embedding in the three given bit planes. The embedding process is carried out in data embedder, that outputs an image containing secret data and is generally termed as stego-image. The security of data embedded is a function of Key Length. The used pseudo random number generator (PRNG) is capable of addressing all the locations in first three Intermediate Significant Bit planes where data is to be embedded. As such the PRNG uses 18 bit seed word to generate the key for embedding data.

II. APPLICATIONS

Copyright Protection**:** To protect copyrights and assert ownership of a Multimedia content. Generally a signature called watermark is inser inserted in the medium that is to be protected against copyright infringments.

*Content Authentication***:** The use of fragile water marks is made for content authentication. Content authentication is used to verify authenticity of a multimedia content and

ensure whether same piece has been received that was transmitted at transmitter or a changed version of original piece.

*Broadcast monitoring***:** This is used to monitor if the contracted number of commercials were broadcasted in a given time slot or not. This ensures if the commercials were given due air time or not.
*Fingerprinting***:** This is used to discourage unauthorized duplication and distribution by embedding a distinct watermark (or a fingerprint) in each copy of the data.
*Metadata binding***:** Metadata refers to side information embedded in an image that can serve many purposes. For example, a business can embed the Web site address for a specific product in a picture that shows an advertisement for that product.
*Covert communication***:** To transmit information secretly from transmitter to receiver.

III. ESSENTIAL REQUIREMENTS

*Payload***:** This refers to amount of information that can be embedded in cover medium.
Security: The security of data hiding techniques is governed by Kerckhoff's assumption states which state that one should assume the method used to encrypt the data is known to an unauthorized party and that the security lies in the choice of a key [4, 5, 6]. Hence a data hiding technique is truly secure if knowing the exact algorithms for embedding and extracting the hidden data does not help an unauthorized party to detect the presence of the secret data or remove it.
*Perceptual Transparency***:** The data hiding algorithm should be such that the information embedded in the cover medium should not deteriorate the perceptual quality of cover data. An embedding procedure is truly imperceptible if humans cannot distinguish the cover medium from the stego-medium [7].
Roubustness: A watermark (secret data) should stay in the cover medium regardless of various signal processing operations carried over host medium, which include all hostile attacks that unauthorized parties may attempt. This requirement is referred to as robustness. It is a key requirement for copyright protection and fingerprinting applications but less important for applications like steganography where capacity and security are of prime importance.

IV. RELATED WORK

There are mainly three basic data embedding techniques for images in practice, namely Least Significant Bit (LSB) Method, Masking and filtering and Transform based[3]. The primitive method is embedding in LSB. Although there are several disadvantages to this approach, the relative easiness to implement it makes it a popular method. In this method we embed information in the LSB of pixels colours. The changes of LSB may not be noticeable because of the imperfect sensitivity of the human eyes. On an average, only half of the bits in an image will need to be modified to embed a secret message using the maximal cover size. While using a 24-bit image gives a relatively large amount of space to hide messages, it is also possible to use an 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 colour, as another colour in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in gray scale, as the human eye will not detect the difference between different gray values as easy as with different colours.
Masking and filtering techniques, usually restricted to 24 bits or gray scale images, take a different approach to embedding 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 difference. 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 in 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. In transform based data embedding, the cover image is transformed into another domain. Then the data is embedded in the transform coefficients. This method is highly robust and complex. The major transformations used are DCT and DWT. DCT is used in JPEG compression algorithm to transform successive 8_8 pixel blocks of the image, into 64 DCT coefficients each. After calculating the coefficients, the quantizing operation is performed. Although a modification of a single DCT will affect all 64 image pixels, the LSB of the quantized DCT coefficient can be used to embed information. When information is hidden in video, the program or person embedding the information will usually use the DCT method. DCT works by slightly changing the coefficients of each of the images in the video, only so much that it is not noticeable by the human eye. Data embedding in videos is similar to that of data embedding in images, apart from information is hidden in each frame of the video. When only a small amount of information is hidden in a video, generally it is not noticeable. However, when more information is hidden, it will be more noticeable. DWT is based on sub-band coding and is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required. A 2-D DWT transforms an image into four sub bands: LL, LH, HL and HH where L and H stands for Low and High. The LL sub band contains the average information and the other three sub-band gives the finer details of the image. Even if the three sub-bands LH, HL, HH are made zero, the LL alone can give the average image (an image of lower quality, with no finer details). We can embed the message image in two LSB planes of LH, HL and HH sub bands. Data is embedded in LL sub-band to avoid compression losses. Human Visual System (HVS) model points out different

insensitivities among different level sub bands. More insensitive to HVS means that more data can be embedded without causing notable visual artifacts. Transform-based method is found to be superior compared to spatial-domain method . It is more imperceptible and robust though more complex. With the advent of high speed Internet and demand for larger payload, video signal will be the perfect cover signal for the years to come.

V. PROPOSED METHOD

The philosophy behind data embedding in the proposed system is,more significant the bit plane, lesser the amount of data embedded in it. This philosophy ensures better perceptual qualities of the stego object.Data to be embedded in the bit planes has been divided into three variable length data vectors of continuously decreasing lengths. The data vector with total length is divided into three variable length data vectors,viz:L1, L2 and L3 of continuously decreasing magnitude.The data is embedded in the first three ISB planes under the control of a private key. In order to thwart the adversary, data is not embedded sequentially. The key, which is generated using Pseudo Random Number Generator (PRNG), ensures a highly randomized data embedding in the three given bit planes.The embedding process is carried out in data embedder, that outputs an image containing secret data and is generally termed as stego-image.

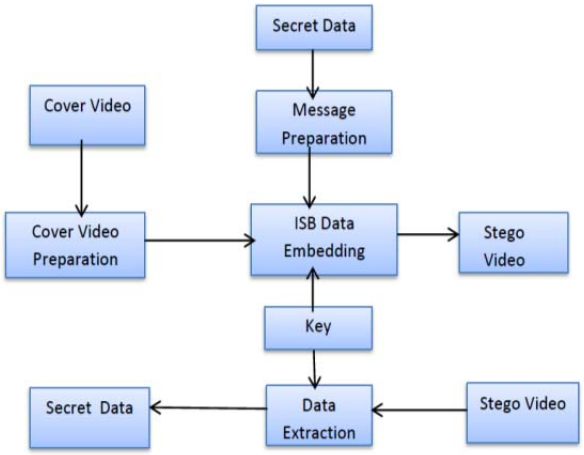

Fig 1: Proposed System Architecture

A. Secret data and Cover Video Preparation

Firstly, Cover Video is prepared for data embedding by breaking it into its constituent frames. Intermediate frame is selected for data embedding. Image is prepared for data embedding by breaking it into its constituent bit planes . The philosophy behind data embedding in the proposed system is, more significant the bit plane, lesser the amount of data embedded in it. This philosophy ensures better perceptual qualities of the stego image. As such data to be embedded in the bit planes has been divided into three variable length data vectors of continuously decreasing lengths. The embedding strategy is the data vector with total length is divided into three variable length data vectors, viz: : L1, L2 and L3 and of continuously decreasing magnitude.

B. Key Generation

A pseudorandom number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. The sequence is not truly random in that it is completely determined by a relatively small set of initial values, called the PRNG's *state*, which includes a truly random seed. Although sequences that are closer to truly random can be generated using hardware random number generators, *pseudorandom* numbers are important in practice for their speed in number generation and their reproducibility.

C. Embedding Strategy

The proposed data hiding system, breaks the data vector to be embedded, in smaller size vectors equal, in number to the number of ISB planes in which data is to be hidden. The lengths of data vectors can be related in several ways. In the implemened technique the data has been broken into three blocks with lengths L1, L2 and L3. This is because data is to be embedded in three ISBs. The relation between the lengths of data blocks is L1= L/2, L2= 3L/8 and L3=L/8; where L is the total length of data vector to be embedded in the cover medium. The data is embedded in the embedder under the control of a private key.

D. Blind Extraction Strategy

The embedding algorithm uses private key to embed the data in the ISBs of cover image. The resultant image yeilded by data embedder is called stego image. At the receiving end the the extraction algorithm uses stego-image along with same key as that used at embedder to extract data from the stego-image. Since cover image is not needed for the retrieval of secret data the proposed system falls in the category of blind detection.

VI ADVANTAGES

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.

Capacity:

Text based steganography has limited capacity and Image steganography tried to improve the capacity where 50% of original image size can be used to hide the secret message. But there is limitation on how much information can be hidden into an image. Video Steganography has been found to overcome this problem.

Imperceptibility:

Lowest chances of perceptibility because of quickly displaying of the frames, so it’s become harder to be suspected by human vision system.

Video error correction:

Since the transmission of any data is always subject to corruption due to errors, then the video transmission must deal with these errors without retransmission of corrupted data. This is another application for steganography rather than security purpose.

VII RESULT AND ANALYSIS

In the data hiding paradigm there are two parameters of opposing nature that is to embed maximum information in an image and keeping the image degradation minimum so that it could not be perceived that something has been embedded in the host image. With this kind of motive a number of standard grayscale images (512 x512) as shown in Fig2 and Fig3 were used in the proposed system. Fig2 and Fig3 also presents stego images obtained for each gray scale test image after embedding 294906 bits of data in each of them. The implemented scheme embeds more than 14% of data in the host images compared to 12.5% in case of LSB methods. Besides this the proposed system improves the Peak Signal to Noise Ratio on an average by 1.5db and by 2db at some instances like in case of test Image 'Bridge'. A comparison of the proposed data hiding scheme with that of LSB schema is presented in Table 1. Tables 2 and 3 respectively show a graphical comparison of the proposed scheme with LSB schema.The proposed technique besides providing improvements in both hiding capacity and PSNR provides additional feature of high security, as data is embedded under the control of a secure key in the selected bit planes. The hiding Capacity (HC) and PSNR have been calculated as follows.

Hiding Capacity (HC):

Size of data in a cover image that can be modified without deteriorating integrity of the cover image gives an idea about the hiding capacity. It is also referred to as payload. Capacity is represented by bits per pixel (bpp). It is given by (total number message bits/total number of image bits) multiplied by 100. If m and N respectively denote total message bits and image bits the hiding capacity is given by

$$\text{Hiding Capacity (HC)} = (m/N)*100$$

Peak Signal to Noise Ratio (PSNR):

It is measure of quality of image. It gives an idea about how much deterioration has embedding caused to the image. It is represented as

$$\text{PSNR}=10\log_{10}\frac{255^2}{mse}\ \text{db}$$

Where mse is mean square error and is given by

$$\text{Mse} = \left[\frac{1}{N*M}\right]^2 \sum_{i=1}^{N}\sum_{i=1}^{M}\left(X_{ij}-Y_{ij}\right)$$

Where N and M are image dimensions, and represent original and stego images respectively.

Fig2: Original Image

Fig3: Stego Image

Name of Image	LSB[8] (Hiding Capacity in bits)	Proposed(Hiding Capacity in bits)	LSB[8] (PSNR in db)	Proposed(PSNR in db)
Lena	262143	294906	47.164	48.663
Peppers	262143	294906	47.170	48.648
Baboon	262143	294906	47.171	48.745
Boats	262143	294906	47.074	48.587

Table1: Comparison between proposed technique and that of LSB method

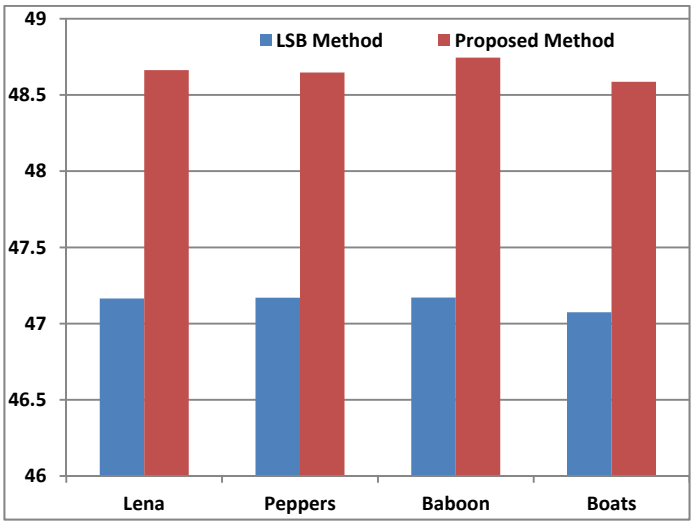

Table 2: Comparison between proposed technique and that of LSB method(PSNR Value)

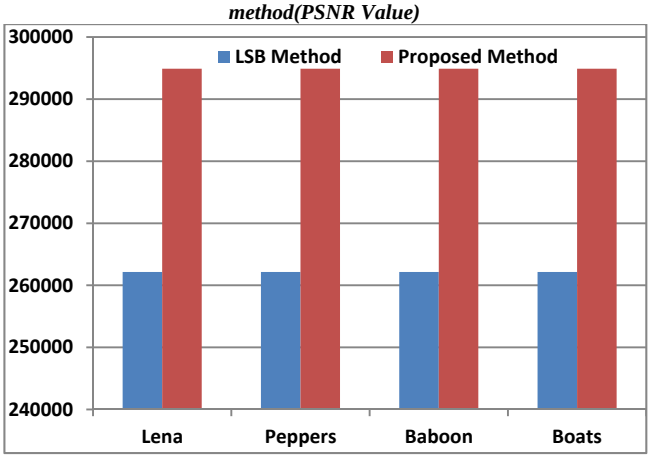

Table 3: Comparison between proposed technique and that of LSB method(High Capacity)

VIII. CONCLUSION

A secure and high capacity data hiding technique with blind detection is presented in this paper. The video is divided into constituent frames and the intermediate frame in which the data is embedded has been broken into its constituent bit planes. The data to be embedded in the cover medium has been divided into three variable length data vectors. The data vectors are subsequently embedded in first three ISB planes using a private key generated by Pseudo Random Number Generator (PNRG). The PRNG not only embeds data pseudo randomly in various bit planes but it also ensures pseudorandom embedding of data at various pixel locations, thus providing an adequate security to the data carried by the cover medium. The technique has been implemented using MATLAB 7. The proposed technique, on an average provides about 8db improvement in PSNR when compared with [8] even when payload is increased on an average by 2.2%. The results clearly show that the proposed technique has a better performance.

REFERENCES

[1] C. Cachin, "An information-theoretic model for steganography,"Information and Computation, Vol. 192, 41-56. 2004

[2] Bin Liu., Fenlin Liu., Chunfang Yang and Yifeng Sun.: Secure Steganography in Compressed Video Bitstreams, The Third International Conference on Availability,Reliability and Security,2008

[3] N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, **(2000)**, pp. 43-78.

[4] G. M Bhat, Shabir A. Parah et.al, "VHDL Modeling and Simulation of Data Scrambler and Descrambler for Secure Data Communication", Indian Journal of Science and Technology,Vol 2, No. 10, pp. 41-43, 2009.

[5] G. M Bhat, Shabir A. Parah et.al, "FPGA Implementation of Novel Complex PN Code Generator based data Scrambler and Descrambler", Maejo Int. J. Sci. Technolgy. 4(01), 125-135,2010.

[6] Shabir A. Parah et.al, "On the realization of a secure, high capacity data embedding technique using joint top-down and down- top embedding approach" Elixir Comp. Sci. & Engg. (49) 10141-10146 , 2012

[7] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data-embedding and watermarking technologies," Proc. IEEE, vol. 86, pp. 1064-1087, June 1998.

[8] M. A. Zeki et. al, "High watermarking capacity based on spatial domain technique" Information technology journal:**,** 10(7),1367-1373, 2011.