Pritish Bhautmage, Prof. Amutha Jeyakumar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 1, January -February 2013, pp.1641-1644

Advanced Video Steganography Algorithm

Pritish Bhautmage*, Prof. Amutha Jeyakumar, Ashish Dahatonde*****

*(Department of Elecrical Engineering, VJTI, Mumbai.)
** (Department of Electrical Engineering, VJTI, Mumbai.)
*** (Department of Electrical Engineering, VJTI, Mumbai.)

ABSTRACT

Data embedding is the process of embedding information in a data source without changing its perceptual quality. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under the conditions where a host signal is subject to distortions such as lossy compression and the degree to which the data must be immune to interception, modification or removal by a third party. A new technique is proposed in this paper for data embedding and extraction for high resolution AVI videos. In this method instead of changing the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. The secret message is encrypted by using a simple bit exchange method before the actual embedding process starts. An index can also be created for the secret information and the index is placed in a frame of the video itself. With the help of this index, we can easily extract the secret message, which can reduce the extraction time. The different techniques and advantages of video steganography is discussed in this paper.

Keywords – Encryption, Index Creation, LSB Technique, Stego Key.

I. INTRODUCTION

In conventional cryptography, even if the information contents are protected by encryption, the existence of encrypted communications is known. In view of this, digital steganography provides an alternative approach in which it conceals even the evidence of encrypted messaging. Generally, steganography is defined as the art and science of communicating in a covered fashion[1][2]. It utilizes the typical digital media such as text, image, audio, video, and multimedia as a carrier (called *a host signal*) for hiding private information in such a way that the third parties (unauthorized person) cannot detect or even notice the presence of the communication. In this way, steganography allows for authentication, copyright protection, and embedding of messages in the image or in transmission of the image. A typical digital steganographic encoder is shown in Figure (1). The message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. This is also referred to as the message wrapper. It is not required that the cover and the message have homogeneous structure. In addition, the encoder usually employs a stego-key which ensures that only recipients who know the corresponding decoding key will be able to extract the message from a stego-message.

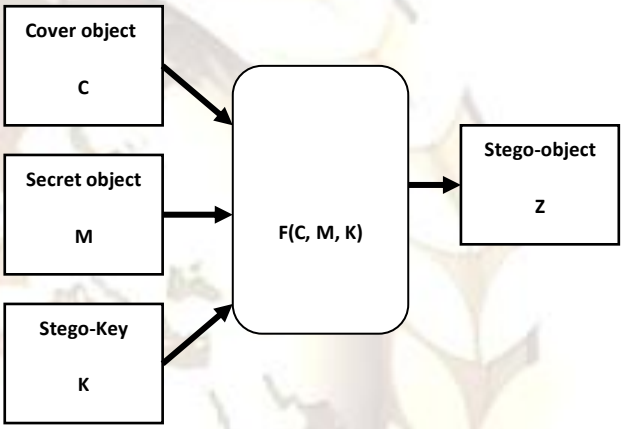

Fig 1. Digital Steganographic Encoder

The original cover file may or may not be required; in most applications it is desirable that the cover file not be needed to extract the message.

It requires the cryptographic decoding key to decipher the encrypted message[3]. The requirements of any data embedding system can be categorized into security, capacity and robustness. All these factors are inversely proportional to each other creating so called data embedding dilemma. We focus at maximizing the first two factors of data embedding i.e., security and capacity. We have attempted on videos rather than on audio and image. The objective of the paper is to develop an algorithm for data embedding in AVI videos.

The proposed scheme is a data embedding method that uses high resolution digital video as a cover signal. The proposed scheme provides the ability to hide a significant quality of information making it different from typical data embedding mechanisms because we consider application that require significantly larger payloads like video-in-video and image-in-video[4]. The purpose of embedding such information depends on the application and the needs of the owner/user of the digital media.

Data embedding requirements include the following:
1) Imperceptibility: The video with data and original data source should be perceptually identical.
2) Robustness: The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.
3) Capacity: Maximize data embedding payload.
4) Security: Security is in the key for embedding or encryption of data.

The paper is organized as follows. Related work of the proposed technique is explained in section II. The methodology of the proposed technique is described in section III. Section IV concludes the paper.

II. 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[5].

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[4].

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[6].

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.

III. PROPOSED METHOD

There are two distinct method to embed a secret message file in the cover file. The block diagram of video steganography (Encoding) is shown in fig2.

(1) We encrypt the secret message file using simple bit shifting and XOR operation in the secret message file.
(2) The encrypted secret message we embed in the cover file in alternate byte. We substitute bits in LSB and LSB+3 bits in the cover file.

1. Bit Exchange method

Simple bit exchange method is introduced for encrypting any file. The following are the steps for encryption method.

- Step-1: Read one by one byte from the secret message file and convert each byte to 8-bits Then we apply 1 bit right shift operation on the entire file so that each byte will be modified accordingly.
- Step-2: We read 8 bits at a time and divide into two blocks 4 bits each and then perform the XOR operations with 4-bits on the left side with 4 bits on the right side and substitute the new bits in right 4-bit positions. The same thing repeated for all bytes in the file.
- Step-3: Repeat step-1 by performing 2 bits right shift for all bytes in the secret message file. Then repeat step-2 again.

In this paper, maximum 5 bits are shifted to right. But the user can take more bits for right shift operation to make the secret file more random. In the decryption process we follow the reverse process.

2. Steganography Algorithm:

In this paper we have use the substitution of LSB and LSB+3 bits of the cover file in alternate bytes. The last 300 bytes of the cover file we use for embedding password, size of the secret message file. After that we start to embed the secret message file. We read one byte from encrypted secret message file and convert it into 8 bits and then we take 2 bits of the encrypted secret message and substitute the LSB and LSB+3 bits of the cover file and then leave one byte of the cover file intact. Then again substitute 2 bits. The same process we repeat for all 8 bits of the secret message.

Here the change is prominent as we embed in text characters but if we do the same in some image then the changes made here will not be very significant as our eye will not be able to differentiate between two colors. To embed secret message we have to first skip 300 bytes from the last byte of the cover file. After that we start to embed bits of the encrypted secret message into the cover file. The size of the secret message file must be less than 10% of the cover file. For .EXE or .DOC file the size of the secret message file must be 1-5% of the cover file.

3. Index Creation

We can also create index for the secret information and the index is placed in a frame of the video itself. With the help of this index, the frames containing the secret information are located. Hence, during the extraction process, instead of analyzing the entire video, the frames containing the secret data are analyzed with the help of index at the receiving end. When steganographed by this method, the probability of finding the hidden information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential

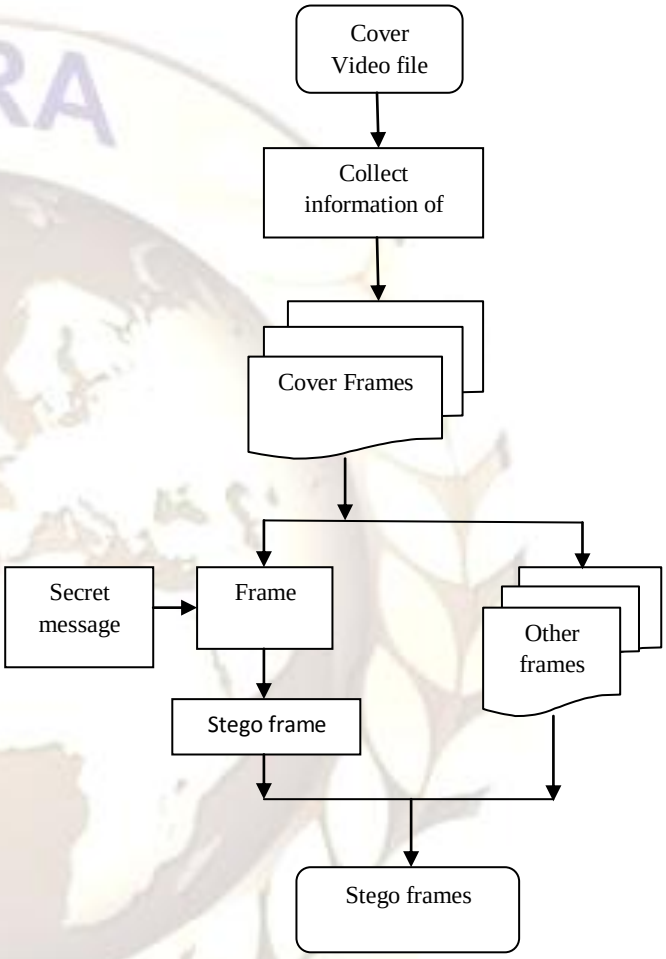

Fig 2. Block diagram of LSB Video Steganography technique (Encoding). manner. It also reduces the computational time taken for the extraction process.

4. Stego Key

To make the system more secured we have introduced the password(Stego key) while embedding an encrypted secret message file. If password is correct then the program will read the file size from the cover file and start to work on the cover file.

To extract the secret message we perform exactly the reverse process of the encryption method. The program first matches the password. If it is correct then it will read the size of the secret message file from the embedded cover file. Then it will read 8 bytes and extract 8 bits from 4 alternate

bytes and convert them to a character and write onto an external file. Once all bytes extracted from the cover file then we run the decryption program to get the original secret message file. This steganography algorithm can be applied on different cover files such as image file, audio file, video file, word file, Excel file, Power point file, .exe file. This method could be most appropriate for hiding any file in any standard or non standard cover file such as word, excel, .ppt, .exe, image, audio, video files.

5. 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.

- **Less computational time**

Since use of indexing concept, the process of retrieving the secret data from the steganographed video becomes very simple and requires very less time.

IV. CONCLUSION

In this paper a robust method of imperceptible audio, video, text and image hiding is proposed. This system is to provide a good, efficient method for hiding the data from hackers and sent to the destination in a safe manner. Thus it can be concluded that Bit Exchange Method and indexing in proposed method can be used which will bring various advantages which can be used for a number of purposes other than covered communication or deniable data storage.

REFERENCES

[1] A.Nath, S.Das, A.Chakrabarti, Data Hiding and Retrieval, *Proceedings of IEEEInternational conference on Computer Intelligence and Computer Network held at Bhopal from 26-28* Nov, 2010.

[2] Samir K Bandyopadhyay, Debnath Bhattacharyya1, A Tutorial Review on Steganography, *UFL & JIITU, IC*-2008, pp. 105-114.

[3] A.Nath, S.Ghosh, M.A.Mallik, Symmetric key cryptography using random key generator, *Proceedings of International conference on SAM- 2010 held at Las Vegas(USA) 12-15 July, 2010, Vol-2*, pp. 239-244

[4] Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles, and Maricel O. Balitanas, Data Hiding in Video, *International Journal of Database Theory and Application*, June 2009.

[5] Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath , Advanced steganographic approach for hiding encrypted secret message in LSB, LSB+1, LSB+2 and LSB+3 bits in non-standard cover files, *International Journal of Computer Applications(0975-8887) Vol 14-No7*, Feb 2011

[6] Yongjian Hu, and Heung Kyu Lee, and Jianwei Lee, DE-based reversible data hiding with improved overflow location map, *IEEE Transaction on circuits and systems for video technology, volume 19*, number 2, February, pp. 250-260, 2009.

[7] Joyshree Nath and Asoke Nath, Advanced Steganography Algorithm using encrypted secret message, *International Journal of Advanced ComputerScience and Application (IJACSA)Vol-2 No.3*, pp. 19-24, March (2011).

[8] Agniswar Dutta, Abhirup Kumar Sen, Sankar Das, Shalabh Agarwal, Asoke Nath, New Data Hiding Algorithm in MATLAB using Encrypted secret message,*IEEE ICCSNT-201*,pp.262-267.

[9] R. Balaji, G. Naveen, *Secure Data Transmission Using Video Steganography.*

[10] V.S.,K.Balasuhramaniyam ,N.Murali, M.Rajakumaran, Vigneswari, Data Hiding in Audio Signal, Video Signal, Text and JPEG Images,*IEEE ICAESM -2012*, pp. 741-746.

(11) G. Doerr and J. Dugelay, "Security pitfalls of frame-by-frame approaches to video watermarking", *IEEE Transactions on Signal Processing, vol. 52*, 2004, pp. 2955-2967