Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

A NOVEL APPROACH TO STEGANOGRAPHY USING PIXEL-BASED ALGORITHM IN IMAGE HIDING IN VIDEOS

K. Jeevana Jyothi, K. L. Pravallika Assistant Professor, Department of ECE, Ramachandra College of Engineering
B. Lalitha Devi, U. Lakshmi Prasanna, J. Lakshmi Prasanna, SK.Kalam Abdulla UG Students, Department of ECE, Ramachandra College of Engineering, Eluru, A.P
E-Mail id: boddulalitha123@gmail.com

ABSTRACT

In Recent years there is a rapid growth in wireless technologies, large size of information has been exchanging over many communication channels. However, few applications like military, medical, multimedia, web and civil etc. need to provide the security to the information sending over. Hence, secure transmission is a highly challenging task. Here in this, we introduce a new secure text image transmission scheme by using pixel mapping through video steganography, which is based on the very simple easy method called as pixel mapping. In the proposed paper the video is distributed into the photo frames using a mat lab code and all the frames are sequentially stored afterwards the secret message will be kept into the video sequence. After the completion of keeping text into images the images is placed in a sequential manner and then all the frames are cascaded for generation of the original video file with encryption.

1. INTRODUCTION

Recent years there is a rapid growth in digital information sharing such as digital images or digital videos. Digital information sharing will be done in various applications, each of them need to transmit the information securely without knowing to the unauthorized person or party. Most of the media services and wireless network technologies were providing omnipresent conveniences for sharing, collecting or distributing images or videos over cellular mobile networks, social networks such as wechat, whatsapp, face book etc., wireless public channels and multimedia networks for many organizations and individuals. For the applications like storage and transmission securing an image is a challenging task. For example, many strategic places like commercial centers, financial centers and public transportations will be monitored by digital video surveillance systems for the purpose of homeland security. Every day there is a large amount of images and videos with secure information, which does not known by unauthorized persons have been generated, transmitted or restored. Many applications such as medical, military, construction industries, fashion design industries and automobile industries require scanned information, blue prints and designs

to be protected against espionage. In addition to this, patients records in medical images such as Magnetic Resonance (MR) or Computed Tomography (CT) and medical signal reports such as electro cardiogram (ECG) or electro encephalogram (EEG) will be shared among the most of the doctors from different branches of health service organizations (HSO) over wireless networks for diagnosis purpose. All these medical images, signals and digital videos may contain some private information, which is more confidential. Hence, it is an important task to provide security for this sort of images and videos. Developing and employing schemes to enhance the lifetime of digital images or videos is an important, imperative and challenging task, which protects the content of original data for many years [1]. To protect an image or video encryption is an effective approach [1], which transforms the image or video into different format.The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message[1]. Technically in simple words "steganography means hiding one piece of data within another". Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements. The cover media(C) that will hold the hidden data The secret message (M), may be plain text, cipher text or any type of dataThestego function (Fe) and its inverse (Fe-1)An optional stego-key (K) or password may be used to hide and unhide the message [3]. Steganography is the art or study of hiding information by inserting secret messages in other messages. Medium where information is inserted can be anything. This medium is called the cover object. Steganography that is applied to hide information on the cover of digital objects is called Digital Steganography [3]. Cover objects that are used in digital steganography can vary, for example in the image archive. Steganography algorithms in the image archive have been widely developed. Meanwhile, steganography algorithms in audio archive are relatively few. In recent years there are so many algorithm have been developed to provide more security, enhanced quality with easy implementation and faster calculations. Among them all of the techniques have their own drawbacks like computational complexity, time consumption and reconstruction of secret information etc., Here, in this proposal we implemented pixel mapping based video steganography, which is a very simple and easy calculations and also provide more security.

2. AUDIO CRYPTOGRAPHY

Audio cryptography is the technique of hiding information inside an audio signal. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio cryptography software can embed messages in WAV, AU, and even MP3 sound files. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. As

data is embedded in the signal, it gets modified. This modification should be made imperceptible to the human ear. Image can also be taken as a medium but audio cryptography is more challenging because of the characteristics of Human Auditory System (HAS) like large power, dynamic range of hearing and large range of audible frequency.

Least Significant Bit (LSB) Coding

One of the earliest techniques studied in the information hiding of digital audio (as well as other media types) is Least Significant Bit modification coding technique. In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. LSB hiding is a simple and fast method for embedding information in an audio signal. It consists of embedding each bit from the message in the least significant bit of the cover audio in a specific way. LSB hiding schemes provide a very high channel capacity for transmitting many kinds of data and is easy to implement and to combine with other hiding techniques. The length of the secret message to be encoded should be smaller than the total numbers of samples in a sound file. The LSB technique takes advantage of the HAS which cannot hear the slight variation of audio frequencies at the high frequency side of the audible spectrum. The LSB technique allows high embedding rate without degrading the quality of the audio file.

Furthermore, it is relatively effective and easy to implement.

Disadvantage:.

- Since the length of secret message to be encrypted is limited in size large text cannot be embedded into Audio
- Decrypting binary secret message has much more complexity Compared to Image Stenography.

3. **PROPOSED METHOD**

A) STEGANOGRAPHY

Steganography is the art of hiding information by embedding message within each other. It works by replacing the very useless bits by the information content to be transmitted. It works by hiding information inside a cover. The cover may be an image file or a video file as per the user requirement. Even though the cover looks very simple and unchanged but it has information contained in it. Figure 4 describes the simplified process of steganography. First of all the video file is converted into a series of frames of equal size. The information content which is to be transmitted by mapping onto the video file is distributed into small portion depending on the size of the frames in the video file. From each frame a smaller region is modified depending upon the private key. Due to this the selected groups looks very random to the third party who does not have the private key with them. The selected pixels are then converted into the frequency domain with the help of the discrete cosine transform. Usually a predefined portion of the pixels like we say the last two or three bits are then replaced by the spilled message portion and then the pixel portion is again converted

back into the spatial domain. The conversion from the frequency domain to the spatial domain is done with the help of inverse DWT. Then that group of pixels is placed back into the particular frame. This process is followed until the end of the whole information content. The frames are then arranged into a sequential manner and the video is constructed from it. Now this video contains the information which gets transmitted along with the transmission of the video file. Proposed method include both embedding and extraction processes. Embedding is a process in which the message information will be inserted into the cover video by using the pixel mapping algorithm. And the retrieving of message information by applying inverse process of embedding is called as extraction process. Figure 5describes the sequence of steps to be executed for generating the embedded video file for secured text data transmission. The algorithm is briefly described in terms of block diagram for the better understanding of the whole process. The complete algorithm is coded in a Matlab code showing the detailed process involved in the video steganography and the text insertion in the video file for secured transmission. As shown in the algorithm in figure 5 the complete video is segmented into number of images using a small Matlab code module and after the processing of the video by the Matlab code module the video gets divided into different frames of same size. Then select the image to embed the message file into it. Then apply pixel mapping algorithm to embed the message bits.

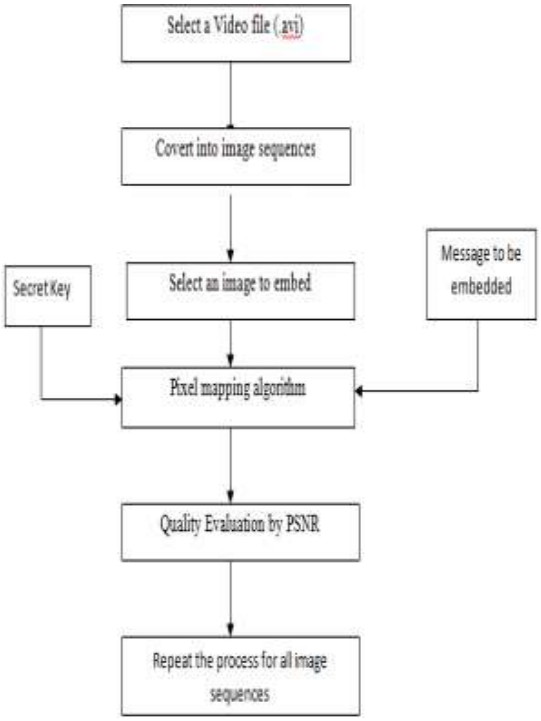

Fig 1. Proposed method flowchart

B)Pixel mapping algorithm

Step1: Select the cover image ‘C’ from the video sequences, which had converted by using MATLAB code

Step2: Convert the image ‘C’ into unsigned integer format (uint8) and divide the cover image into Red (R), Green (G) and Blue (B) components

Step3: Select the number of input bits „n“ to be substituted in „C“

Step4: Now, do the logic AND operation to the number of bits in R component of ‘C’ and substituted ‘n“ bits

Step5: Then do the bit OR operation to the output of above step and the entire shifted message bits with „n’ bits

Step6: Repeat the same for green and blue components also

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, April : 2023

Step7: Do the same process for all the selected frames from the video file and then convert R, G and B components into stego frame then after reconstruct all the frames into stego video, in which the message information has been embedded.

Fig7. Video frame

c) LSB Approach

- Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover video.
- Video is converted into a number of frames, and then convert each frame in to an image.
- After that, the Least Significant Bit (in other words the 8 bit) of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue color components can be used, since they are each represented by a byte.
- In other words one can store 3 bit in each pixel.
- We implemented our project such that it can accept and video of any size.

Fig 2. Secret image

4. SIMULATION RESULTS

Experimental results has been shown in this section, all the experiments have been done in MATLAB 2009a. We had tested the proposed algorithm for videos for different number of bits substitutions. The histogram approach is used to compare the extracted message with the original message.

Fig 3. Stegano video frame

Cipher images	MSE	PSNR
College logo.jpg	0.455	39.46
Jntu logo.jpg	0.435	41.04

Table 1: comparison table

The performance of the proposed scheme is compared by the parameters, (i) mean square error (MSE), (ii) peak signal-to-noise ratio (PSNR). The capacity is measured in bits. A steganography technique should strive for getting higher capacity and lesser distortion. The smaller value of MSE refers to lesser distortion. Unlike MSE the higher PSNR value refers to lesser distortion.

5. CONCLUSION

One of the important features of the proposed work is it plays a vital role in transmitting the information mapped on an either image or a video file very effectively an efficiently. The information underlying the image or a video is not visible to the naked eye when we embed the message information into LSB. Only the person having the private key and the rule list can identify and decode the original information into its original form. This method simplifies the task of securing the vital information from the misuse and protects it from the unwanted user. With the use of the cryptography and steganography combination the information security can be increased.

REFERENCES

[1] http://en.wikipedia.org/wiki/Time-lapse.
[2] Handbook of image and video processing by Alan Conrad Bovik, Elsevier Inc., ISBN 0-12-119192-1.
[3] Digital Video Processing by A. Murat Tekalp, Prentice Hall Signal Processing Series.
[4] R. Schaphorst, Videoconferencing and video telephony, Boston, MA: Artech House Publishers, 1996.
[5] Adnan M. Alattar, Reversible watermark using the difference expansionof a generalized integer transform, IEEE Trans. On Image Processing,vol. 13, no.8, Aug, 2004.
[6] Avcibas, N. Memon, and B. Sankur Steganalysis using image qualitymetrics, IEEE Trans. IP, VOL. 12, PP.221-229, Feb. 2003.
[7] Dipesh G. Kamdar, Dolly Patira and Dr. C. H. Vithalani,Dual layer datahiding using cryptography and steganography in IJSET volume 1,issue 4,ISSN : 2277-1581