Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol. 1 No. 1, 2012, pp.8-11

DOI: https://doi.org/10.51983/ajeat-2012.1.1.2507

Loseless Data Embedding Scheme for Medical Image Transmission in E-Diagnosis

A. Ann Ramola Jeyanthi, B. Babu and T.S.Vishnu Priya
Department of Master of Computer Applications
The American College,Tamil Nadu - 625 002, India
E-mail: annramola@hotmail.com
(Received on 18 December 2011 and accepted on 10 March 2012)

Abstract - **One of the major concerns throughout the world today is to make high quality health care available to all. Traditionally, part of the difficulty in achieving equitable access to health care has been that the provider and the recipient must be physically present in the same place. Recent advances in Information and Communication Technologies have increased the number of ways health care can be delivered to reduce these difficulties. Mobile phones are the most commonly used devices in today's scenario. The expanding use of mobile phone, telecommunication companies added feature such as MMS (Multimedia Messaging Service) in order to attract more customers. The Multimedia Messaging Service (MMS) has became very popular for sending messages containing multimedia objects such as images, audio, or video clips among mobile users. Alongside, the need for the secure communication became more imperative. Steganography is the most reliable technique for hidden communication. Hiding information, especially in images has been an alternative solution for secret communication [2].**

Keywords : **Video Steganography, Medical Images, Information Hiding, Multimedia Messaging Service (MMS), HaarWavelet**

I. Introduction

The Steganography is of Greek source and means "enclosed or hidden writing"[1]. Data hiding should be used concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden. Steganography is implemented in different fields such as military and Industrial applications. By using lossless steganography techniques messages can be sent and received securely. Traditionally, steganography was based on hiding secret information in image files. Lately, there has been growing interest in implementing steganographic techniques to video files as well as audio files. The advantage of using video files in hiding information is to be added security against hacker attacks due to the relative complexity of video compared to image files and audio files. Image-based and video-based steganography techniques are mainly classified into spatial domain and frequency domain based methods[9].

cover_medium + hidden_data + stego_key = stego_medium

The main aim of steganography is to hide information in the other wrap media so that other persons will not observe the existence of the information. This is a major distinction between this method and the other methods of secret exchange of information because, for example, in cryptography, the individuals perceive the information by considering the implied information but they will not be able to realize the information [1]. However, in steganography, the existence of the information in the sources will not be noticed at all. Most steganography jobs have been carried out on images, video clips, texts, music and sounds. For video stream usually being accessible in compressed form, steganography algorithms that are not applicable in compressed bit-stream would require complete or at least partial decompression [2]. This is an unnecessary saddle best avoided. If the requirement of strict compressed domain steganography is to be met, the steganography needs to be embedded in the compressed domain. Nowadays, there are large amount of video watermarking algorithms been proposed. Some of them are applied for compressed video.

To be useful, a steganographic technique should not be easily detectable. If the existence of secret message can be detected with a probability higher than random guessing, the corresponding steganographic technique is considered to be invalid [3]. Similar to cryptography and steganography may suffer from the attack method (steganalysis). Much of the research work in the field of steganalysis has been carried out on images. One approach is based solely on the first order statistics and is applicable only to idempotent embedding.

Steganography Terms

Carrier File : A file which has hidden information inside of it.

Steganalysis : The process of detecting hidden information inside a file.

Stego-Medium : The medium in which the information is hidden.

Redundant Bits – Pieces of information inside a file which can be overwritten or altered without damaging the file.

II. Haar Wavelet Transform

Wavelets are mathematical functions that were developed by scientists working in several different fields for the purpose of sorting data by frequency. Translated data can then be sorted at a resolution which matches its scale [8]. Studying data at different levels allows for the development of a more complete picture. Both small features and large features are discernable because they are studied separately. Unlike the discrete cosine transform, the wavelet transform is not Fourier-based and therefore wavelets do a better job of handling discontinuities in data [7].

The Haar wavelet operates on data by calculating the sums and differences of adjacent elements. The Haar wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. The Haar transform is computed using:

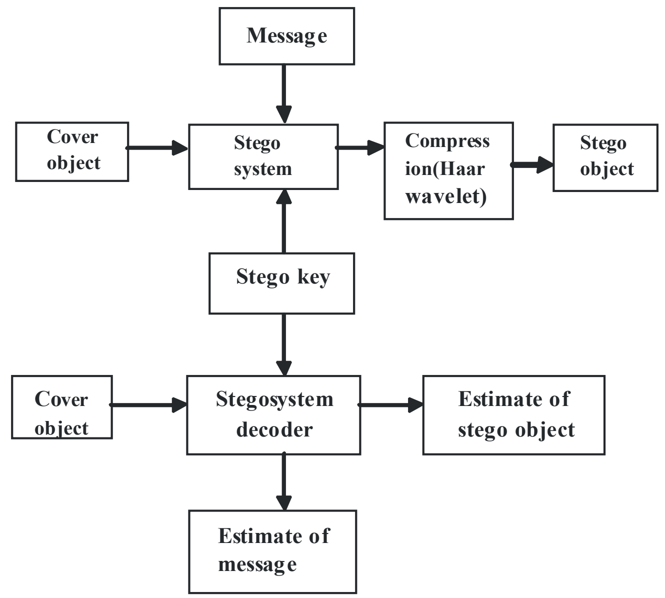
$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

One nice feature of the Haar wavelet transform is that the transform is equal to its inverse. As each transform is computed the energy in the data in relocated to the top left hand corner.

III. Methodology

As discussed earlier Digital video comprises a series of orthogonal bitmap digital images displayed in rapid succession at a constant rate. These images are called frames. The frames in a video are nothing but normal images with some extra information such as the index and other Meta data related to the video [10]. Each frame can be extracted individually from the video and can be converted into an image. This can then be treated as the cover object and the data can be embedded in it using one of the usual techniques used for data hiding in images. The stego-image then obtained can then be converted back into frames and arranged in sequence to obtain the stego-video. This video contains the embedded data which can be obtained by extracting each frame and extracting the data from it.

Our technique spreads the data evenly over the entire video instead of concentrating it in into one single frame, thereby making the detection of the data even more impossible. For example if there are 4 bits of data to be embedded into a video with more than four frames then each bit will be embedded in one of the four frames in the video. This approach gives a huge advantage in the aspect of increasing the imperceptibility of the data embedded into the video. Our methodology is quite simple and unsophisticated and hence very fast when compared to other existing techniques.



IV. The Coding Algorithm

In the usual steganography algorithms, information is hidden in the sequential pixels. Therefore anyone with the knowledge of the coding algorithm can extract the hidden information from the image. In this paper a new approach has been studied for selecting pixels according to a password. This password would enable us to select the pixels in a random manner.

In the usual steganography algorithms, if the size of the information is small in comparison with the size of image, the attacker can find the pattern of altered pixels and extract the hidden information. But in this method, information is in random order pixels in each block, and extracting the hidden information is difficult.

On the other hand if the size of the information is large, the algorithm reaches the end of image. For solving this problem, it has to return to the beginning of the image and hide information in an empty pixel (an empty pixel is defined as a pixel of original image that has no hidden data). This process needs a large amount of memory to remember all empty pixels, but in the mobile phones we have a limited amount of memory. After all, finding an empty pixel needs a lot of time in coding or decoding phases.

The new method for hiding information is described here:

In this method the image is segmented into n blocks of m pixels. Then according to the password, a block is selected and the information is hidden in an empty pixel of this block.

The algorithm for selecting a block and an empty pixel in that block is as follows: if the selected block starts with the pixel number k and has m pixels then the number of the last pixel is k+m-1.

This algorithm uses an array of size m+1 for remembering empty pixels of current block. This array contains the number of pixels having no data. The last cell of the array is the total empty pixels in the current block. According to the password, an empty pixel is selected and the last empty pixel number is copied to this array cell. After this operation the total number of empty pixels on the block decreases by one.

This method is also used for selecting a block to hide the information in itself. The figure-1 shows the array before and after selecting a pixel.

k	k+1	k+2		k+I-1		k+m-2	k+m-1	M
1	2	3	...	i	...			

(a) The array before selecting an empty pixel.

k	k+1	k+2		k+m-1		k+m-2	nul.1	m-1
1	2	3	...	i	...			

(b) The array after selecting an empty pixel.

The advantage of this method is that there is no need to search for an empty pixel in the block, because we have the empty pixel numbers of the current block in an array. On the other hand by dividing the image into small blocks, it only needs a small amount of memory. We indicate that the size of memory is a critical factor among mobile phones applications.

If the image is very large, it can be stored on the hard drive and only one of its blocks is transferred to the memory and after hiding the information on that block, it is stored back on the hard drive.

This method swaps the last cell of the array with the ith cell of the array. The advantage of this work is that the pixels are filled in a random order and cannot decode without knowing the password.

This method for hiding information in images can be used for secure communication, copyright protection, preventing undesirable changes in digital documents, protecting from unauthorized copying and other applications.

V. Proposed Algorithm For Embedding Scheme

Let the Cover video consist of N number of frames. Each of these frames are extracted from the video for the purpose of embedding the data in them.

1. Read the data to be embedded and convert it into binary form containing B bits.
2. Considering the amount of data to be embedded and the capacity of video calculate the value of k(no. of LSB's to be modified in each pixel), using the following formula.

   K=(MAXDATA/B).Where MAXDATA=N*Height*Width

   (K should not exceed 4 in order to maintain satisfactory video quality).
3. Divide the B into N number of blocks of data. Let these blocks be called BLi.
4. Divide each block into groups of K bits.
5. Consider one frame at a time and embed the K groups of bits in blocks BLi into the Pixels in the corresponding frame. For example block BLi is embedded into the ith frame. For embedding OPAP (Optimal Pixel Adjustment Process) is used.
6. The frames with embedded data are again combined together to obtain the Stego-video.

VI. Proposed Algorithm for Decoding Scheme

1. Read the Stego- video with .avi extension.
2. Let the Stego video consist of N number of frames. Each of these frames are extracted from the video for the purpose of retrieving the data from them.
3. Calculate the value of K using the followingformula.

   K=(MAXDATA/CHARBITS). Where

   CHARBITS = (number of characters that have been embedded in the video)* 8.
4. Calculate the size of block of data to be extracted from each frame of the video using the formula

5. Extract the BLi bits of data from the ith frame using the OPAP technique .

6. The Extracted data which is a stream of bits should be grouped into groups of 8 bits each and converted back into the character format in order to retrieve the data embedded in the video.

Video (Covering medium)

(a) Before encoding

(b) After encoding

Decrypted images

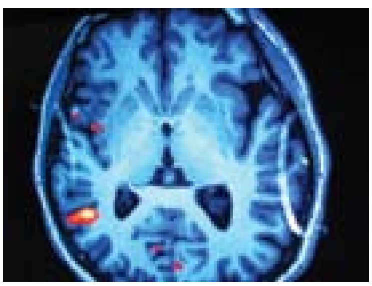


TABLE I EXPERIMENTAL EVALUATION

Carrier File Types	Compression Size	Compression Ratio	Embedding and Compression Time(s)
Video	1.72MB	98.7%	5.12
Video	5.23MB	98.7%	9.26
Video	4.31MB	98.7%	9.15
Audio	2.65MB	99.3%	7.24
Audio	2.88MB	99.3%	7.29
Audio	7.24MB	99.3%	12.00
Audio	3.76MB	99.3%	8.21
Text	1.59KB	99.7%	2

The probability that one can detect a stegano image is relatively low, due to the high volume of images exchanged between mobile phones and computers. The password is not stored in the stegano image; therefore it is difficult to detect the password. The decoding program fast enough to retrieve the images with few kilobytes of memory. This approach is used on mobile phones with no limitation for selecting the password.

VII. CONCLUSION

The proposed approach used to embed any number of files in audio or video. Precious human life could be saved in E-diagnosis. These approaches concentrate on achieving higher compression ratio without sacrificing the quality of the Image. Since processing power required in the mobile handset is limited, a new approach is developed with energy efficient, computing efficient and adaptive image compression and communication techniques. Performance analysis is made in terms of accuracy and computational time, which is a positive scope of this paper. Most of the computational burden is reduced in Haar wavelet transform.

REFERENCES

[1] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb, "A Secure Covert Communication Model Based on Video Steganography", *in Military Communications Conference,* 2008 MILCOM. IEEE on 16 – 19 Nov. 2008.

[2] M.Shirali-Shahreza, "Steganography in MMS", *Proceedings of the 11th IEEE International Multitopic Conference* (INMIC 2007), Lahore, Pakistan, December 28 – 30, 2007.

[3] K. Papapanagiotou, E. Kellinis, G.F. Marias, and P. Georgiadis, "Alternatives for Multimedia Messaging System Steganography", *Proceedings the IEEE International Conference on Computational Intelligence and Security* (CIS 2005), Part II, LNAI 3802, Xian, China, pp. 589 – 596, December 2005.

[4] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography", in *proceedings of the fifth Annual Information Security South Africa Conference (ISSA2005),* Sandton, South Africa, June/July 2005 (Published electronically).

[5] K. Papapanagiotou, E. Kellinis, G.F. Marias, and P. Georgiadis, "Alternatives For multimedia Messaging System Steganography", *Proceedings the IEEE International Conference on Computational Intelligence and Security* (CIS 2005), Part II, LNAI 3802, Xian, China, pp. 589 – 596, December 2005.

[6] Marvel L.M., Boncelet Jr., C.G. and Retter C., "Spread Spectrum Steganography", *IEEE Transactions on image processing,* Vol. 8, No. 8, 1999.

[7] G. Langelaar, I. Setyawan, R.L. Lagendijk, "Watermarking Digital Image and Video Data", in *IEEE Signal Processing Magazine,* Vol. 17, pp. 20 – 43, September 2000.

[8] Brani Vidakovic and Peter Müller, "Wavelets for kids," A Tutorial Introduction,Institute of Statistics and Decision Science, Duke University, Durham, NC, 1991.

[9] Chao, Hongyang; Fisher, Paul, "An Approach to Fast Integer Reversible Wavelet Transforms for Image Compression," Computer and Information Science Inc., 3401 E. University, Suite 104, Denton, TX 76208, in "Advances in Computational Mathematics: Guangzhou, China - The proceedings of Guangzhou International Symposium on Computational Mathematics," Guangzhou, P. R. China, August11-15, 1997.

[10] Eric J. Stollnitz, Tony D. DeRose and David H. Salesin, "Wavelets for Computer Graphics : A Primer Part 1," *IEEE Computer Graphics and Applications,* May 1995.