SVD based ECG Steganography to Protect Patient Confidential Information for Bio-Medical Datas

Dinesh.S [1], Rajeswari.S [2]

[1] PG Student, P.S.N College of Engineering and Technology, Tirunelveli, Tamilnadu, India.

[2] Assistant Professor, P.S.N College of Engineering and Technology, Tirunelveli, Tamilnadu, India.

[1] sdkdinesh007@gmail.com

Abstract—**We propose a video data embedding scheme in which the embedded signature data is reconstructed with the original host video. The proposed method enables high rate of data embedding and is robust to motion compensated coding, such as AVI. Embedding is based on quantization and utilizes a multi-dimensional lattice structure for encoding signature information. Signature data is embedded in individual video frames using the block DCT. The embedded frames are then AVI coded. At the receiver, both the host and signature images are recovered from the embedded bit stream. We present examples of embedding image and video in video.**

Keywords: Data hiding, Digital watermarking, Multidimensional lattice structure.

I. INTRODUCTION

The internet and the World Wide Web have revolutionalized the way in which digital data is distributed. The widespread and easy access to multimedia content has motivated development of technologies for digital steganography or data hiding, with emphasis on access control, authentication, and copyright protection. Steganography deals with information hiding, as opposed to encryption. Steganography is defined by Markus Kahn [3] as follows "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemies allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present" Much of the recent work in data hiding is about copyright protection of multimedia data. This is also referred to as digital watermarking. Digital watermarking for copyright protection typically requires very few bits, of the order of 1% or less of the host data size. These watermarks could be alpha-numeric characters, or could be multimedia data as well. One of the main objectives of this watermarking is to be able to identify the rightful owners by authenticating the watermarks. As such, it is desirable that the methods of embedding and extracting digital watermarks are resistant to typical signal processing operations, such as compression, and intentional attacks to remove the watermarks. The focus of this paper differs from typical watermarking. We consider applications that require significantly larger amounts of data embedding. Examples of such applications include embedded control to track the use of a particular video clip in pay-per-view applications , hidden communications, smart images/video that can self- correct under intentional attacks, to mention a few. The capability to hide large amounts of data will also enable robust hiding of digital watermarks by introducing redundancies in the data. We use the term data hiding to distinguish such applications/ techniques from traditional watermarking. As such, the requirements for data hiding differ from those of watermarking. For example, while transparent or visible watermarks are acceptable in many cases, hidden data for control or secure communication need to be perceptually invisible. The following terminology is used in this paper. The signature or message data is the data that we would like to embed or conceal. The source data is used to hide the signature data; we often refer to the source as the host data. After embedding a signature in to a host, we get the watermarked or embedded data. The recovered data, also referred to as the reconstructed data, is the signature that is extracted from the embedded data.

II. PREVIOUS WORK

One of the early techniques for watermarking is the spread spectrum method proposed by Cox *et al.* [2]. The basic idea is to distribute the message or signature information over a wide range of frequencies of the host data. Many researchers have used the discrete cosine or the discrete wavelet transforms coefficients to embed the signature data. For example, Swanson etal [1] proposed a data hiding algorithm to embed compressed video and audio data into video. The message data is embedded in the DCT domain, by modifying the projections of the 8x8 host block DCT coefficients. The data hiding rate is two bits per 8x8 blocks. In this paper, we describe a data hiding technique and demonstrate its robustness to AVI coding of the embedded video. A schematic of our embedding scheme is shown in Figure 1. A key component of this scheme is the use of multidimensional lattices. The signature image and host video frames are transformed using the 8x8 block DCT. The signature coefficients are quantized and then encoded using the multidimensional lattices and inserted into the host DCT coefficient. The embedded videos are then AVI compressed and the signature data is recovered from the compressed video.

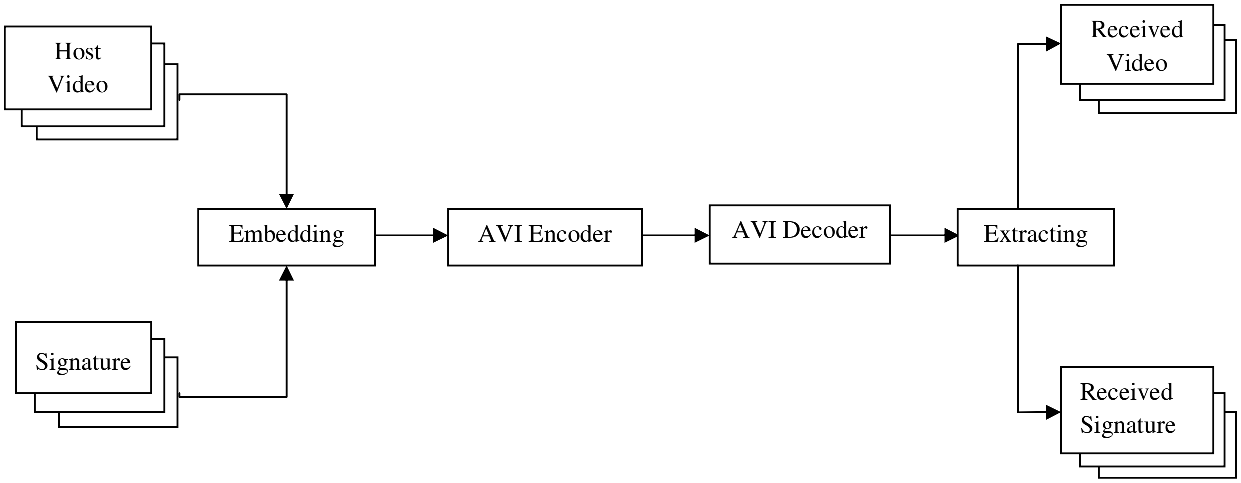


Figure 1: Schematic of video embedding technique

III. Signature Image Quantization

There is clearly a trade-off between quantity of the data one can hide and quality of the embedded and reconstructed signals. We propose a simple scheme here for quantizing signature image data using the block DCT quantization matrix. This approach enables, as demonstrated later in the experimental results, robust recovery of signature data when the embedded image is subject to JPEG/AVI compression.

The signature coefficients are quantized in two steps: first, by using the standard JPEG quantization matrix, and then by a user-specified signature quantization matrix. The signature quantization matrix determines the relative size of signature data compared to the host data, thus controlling the quantity and quality of the embedded data. These quantized signature coefficients are then encoded using the multidimensional lattices and inserted into the host DCT coefficients.

Consider an 8 x 8 DCT coefficient matrix. The low frequency coefficients, obviously, require more bits than the high frequency ones. One such quantization matrix indicating the number of quantization levels for each of the 64 coefficients is shown in Figure 2(a).

These quantized coefficients are embedded in a lattice structure, as described in. For simplicity, we will consider only those shells in the lattice structure whose elements are $\{0, \pm1, \pm2\}$. One way of distributing these coefficients is as follows:

Quantization Level=1232. Use Lattice typeE8: The first and second shells of E8 lattice combined have 2400 code words. Since an E8 code has eight components, it requires 8 host coefficients to embed one E8 code. There are 6 coefficients with this quantization (see Figure 2(a)), requiring 48 host coefficients to embed.

Quantization Level=342 E6. Use Lattice type of E6 lattice contain 342 code words. Six host coefficients are needed to embed an E6 code.

Quantization Level =48. Use Lattice type D4: The first two shells of D4 are used to encode 48 levels. The quantized coefficients are transformed to a lattice code, and the code is embedded into a partitioning of the host DCT block (shaded regions in Figure 2(b)).

1232	1232	1232	342	342	342	48	48
1232	1232	342	342	342	48	48	0
1232	342	342	342	48	48	0	0
342	342	342	48	48	0	0	0
342	342	48	48	0	0	0	0
342	48	48	0	0	0	0	0
342	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Figure 2(a): Signature quantization

						▨	▨
						▨	
				▨	▨		
				▨			
		▨	▨				
		▨					
▨	▨						
▨							

Figure 2(b): Selected coefficients for embedding

The human visual system is more sensitive to the changes in low frequency regions than in high frequency regions. Thus insertion in the high frequency region is less likely to result in visible distortions. Thus we are using user-specified signature quantization matrix, where signature is embedded in high frequency region. This user-specified signature quantization matrix is as shown in the figure 3.

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	0
1	1	1	1	1	1	0	0
1	1	1	1	1	0	0	0
1	1	1	1	0	0	0	0
1	1	1	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	0	0	0	0	0	0

Figure 3: Signature Quantization figure

IV. DATA EMBEDDING

We now summarize the various steps in the embedding procedure. Figure 4 gives the details of the encoder block

1. The host frame and signature image are transformed to the DCT domain. A block size of 8x8 is used in the experiments below.

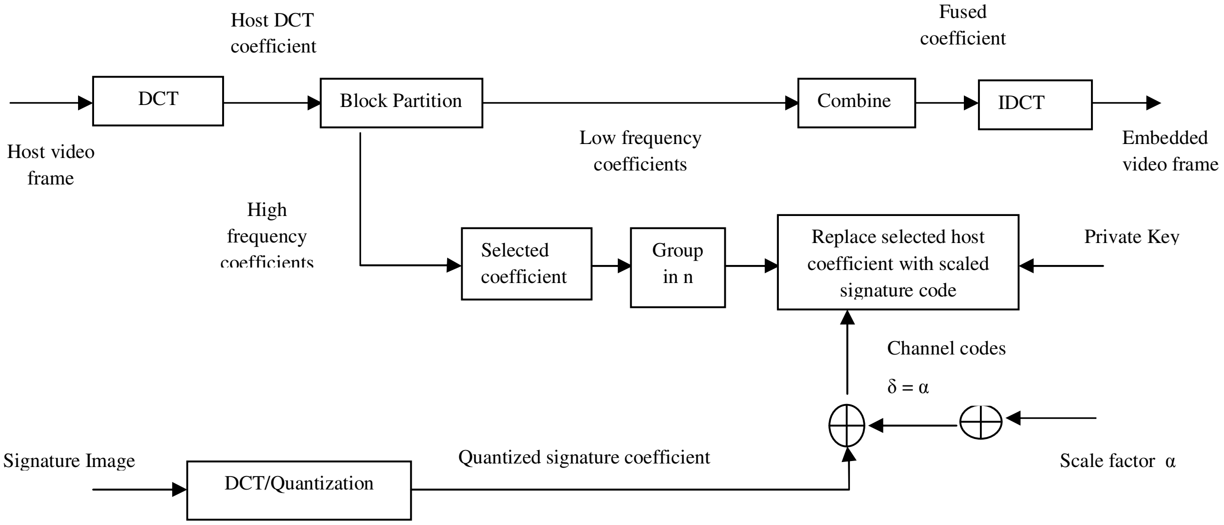


Figure 4: A schematic of encoder in figure 1

2. The signature coefficients are quantized according to the signature quantization matrix and the resulting quantized coefficients are encoded using lattice codes.

3. The signature codes are then appropriately scaled using the total scale factor α.

4. The selected host coefficients are then replaced by the scaled signature codes and combined with the original (unaltered) DCT coefficients to form a fused block of DCT coefficients. Note than more than one host coefficient is needed to encode a single signature code. A private key can be used to select the ordering of the host/ signature blocks as well as in selecting the coefficients for embedding.

5. The fused coefficients are then inverse transformed to produce an embedded frame.

VI.EMBEDDING IN VIDEO

Since a video can be viewed as a sequence of image frames, video water- marking can be viewed simply as hiding the signature image in any one component of a YUV color space representation. We use the Y component of a YUV color space representation for data hiding. In this paper we are hiding the signature in the video frame depending on the user choice, for example after every Nth frame from available number of video frames.

Here we have planned to calculate the parameters such as percentage error rate, Signal to Noise Ratio and Entropy for number of video frames entered. From those results it is very easy for comparison of original video and extracted video. Figure 5 shows samples of the test images

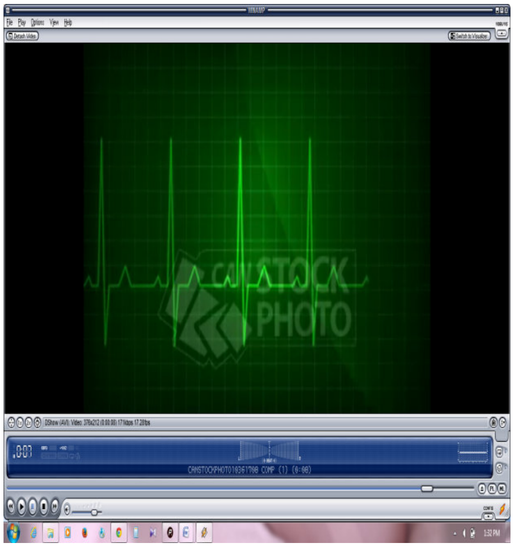
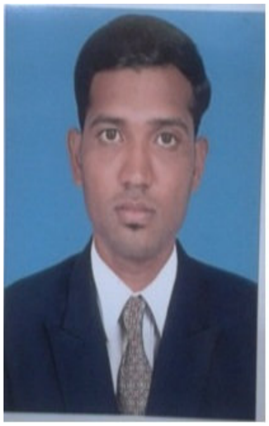


Figure 5(a): Host Video



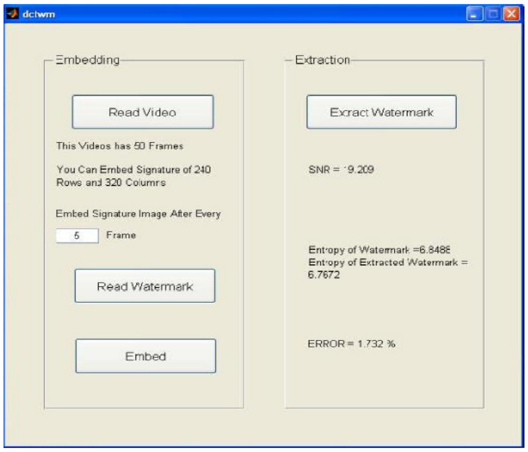
Name : S.Dinesh
Age : 23
Patient ID : HD177
Location : Alangulam
Temp : 97 F
Blood Pressure : Normal

Figure 5(b): Signature Image

VII. RESULTS AND DISCUSSION

In this paper we are hiding the signature as shown in the figure 5(b) in the video frame as shown in figure 5(a).

Embedding was done after every 5th frame from available 50 numbers of video frames. The Matlab User interface is shown in figure 6. By using below User interface user can read the Host video and embed watermark image in desired frame. While after extracting user can get parameters such as Signal to Noise Ratio (SNR), MSE and percentage error rate for number of video frames entered.



This Videos has 50 Frames

You Can Embed Signature of 240 Rows and 320 Columns

Embed Signature Image After Every 5 Frame

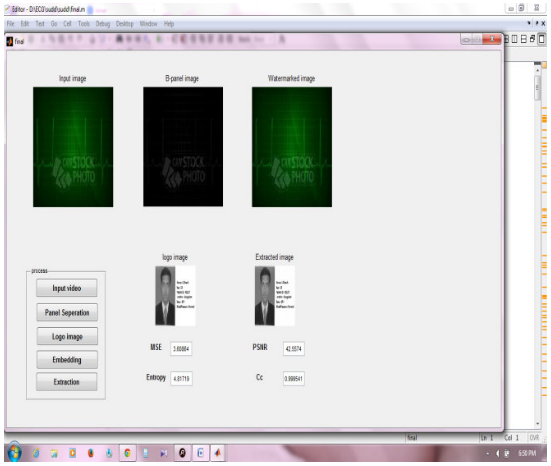
SNR = 19.209

Entropy of Watermark =6.8488
Entropy of Extracted Watermark = 6.7672

ERROR = 1.732 %

Figure 6: Matlab User Interface

The result can be given as,



MSE 3.60864
PSNR 42.5574
Entropy 4.81719
Cc 0.999541

Figure 7: Extracted Output

REFERENCES

[1] M. D. Swanson, B. Zhu and A. H. Tewfik, "Data Hiding for Video-in-Video," Proceedings of IEEE International onference of Image Processing (ICIP '97), Vol. 2, pp. 676-679, Santa Barbara, California, October, 1997.

[2] J. J Chae, D. Mukherjee and B. S. Manjunath, "A Robust Data Hiding Technique using Multidimensional Lattices," Proceedings of the IEEE Forum on Research and Technology Advances in Digital Libraries, pp. 319-326, Santa Barbara, April 1998.

[3] Bret Dunbar "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment" SANS Institute InfoSec Reading Room, January 2002.

[4] J. J. Chae and B. S. Manjunath " Data Hiding in Video" Department of Electrical and Computer Engineering University of California, Santa Barbara.

[5] www.google.com

[6] www.data-hiding.com steganography links and white papers.

[7] Rafael C. Gonzalez & Richard E. Woods, "Digital Image Processing",Pearson and Prentice Hall Publication(Third Edition).

.