Improved Protection In Video Steganography Using DCT & CDCS

Poonam V Bodhak, Baisa L Gunjal

Abstract- The widespread of the internet and World Wide Web has changed the way digital data is handled. The easy access of images, musical documents and movies has modified the development of data hiding by placing emphasis on copyright protection, content based authentication and covert communication. The embedded data is invisible or inaudible to a human observer. Information hiding refers to techniques for embedding additional data in host media. Most of the previous research has focused on still image Information Hiding. Although Information hiding in video has more potential for commercial applications, less research has been conducted on high capacity data hiding in video streams. Compared with still images, data hiding in video presents a much higher capacity or bandwidth. At the same time the computational complexity in video is higher due to the amount of data that need to be processed. Although most known techniques for information hiding in video are robust, the extraction process is not blind. Consequently, these methods are not suitable for applications like those mentioned previously. Here blind data hiding technique tailored to AVI video streams is proposed. The main aim of the project is to provide software that usually works by sending a text message or by sending an image behind a video which makes unable for a human eye or ear to detect. A novel approach is proposed to high capacity, robust and blind Data Hiding Technique in DCT domain. A new encoding technique called Class Dependent Coding Scheme (CDCS) is used to increase the embedding capacity, which can convey the same information using less number of bits. High imperceptibility is achieved by selecting efficient DCT blocks for Embedding data using energy thresholding scheme. On review, of a digitized video before and after a message was inserted, will show video files that appeared to have no substantial differences. The Discrete Cosine Transform is used to embed the file, which casts embedded data into the selected region in the DCT domain. Embedding the file in the selected region gives rise to invisibility.

Index Terms- Discrete Cosine Transform (DCT), CDCS, ROI, Steganography, Stego Image.

1 Introduction

The widespread of the internet and World Wide Web has changed the way digital data is handled. The easy access of images, musical documents and movies has modified the development of data hiding by placing emphasis on copyright protection, content based authentication and covert communication. Data hiding deals with the ability of embedding data in to digital cover with a minimum amount of perceivable degradation, i.e., the embedded data is invisible or inaudible to a human observer.

Information hiding refers to techniques for embedding additional data in host media. Most of the previous research has focused on still image Information Hiding. Although Information hiding in video has more potential for commercial applications, less research has been conducted on high capacity data hiding in video streams. Data embedded in a video stream can carry information about the content itself, low-level descriptors for video indexing, retrieval and segmentation. Other applications include annotation, subtitling, multi-lingual services, tele-text, etc. Due to the data intensive nature of video, in most applications it is required to hide data in the compressed stream.

Compared with still images, data hiding in video presents a much higher capacity or bandwidth. At the same time the computational complexity in video is higher due to the amount of data that need to be processed. Here blind data hiding technique tailored to AVI video streams is proposed. Although most known techniques for information hiding in video are robust, the extraction process is not blind. Consequently, these methods are not suitable for applications like those mentioned previously. Recently proposed methods hide data using the motion vectors of MPEG-1 or MPEG-2 compressed streams. First the optimum motion vector v*opt* is extracted from the coded frames. However, once the MPEG bit stream is re-encoded, the same motion vectors are not always detectable. As a result, the embedded information can easily get lost by simple re-encoding. The main aim of the project is to provide software that usually works by sending a text message or by sending an image behind a video which makes unable for a human eye or ear to detect. On review, of a digitized video before and after a message was inserted, will show video files that appeared to have no substantial differences. The Discrete Cosine Transform is used to embed the file, which casts embedded data into the selected region in the DCT domain. Embedding the file in the selected region gives rise to invisibility. Information is embedded in the host signal by modulating the quantized block DCT coefficients frames. The extraction process is blind.

2 Literature Survey

2.1 Video Steganography

The rapid growth in the demand and consumption of the video data in recent years has led some issues that we need to face, such as content security, authenticity, and digital rights

Poonam V Bodhak completed her Diploma From MIT Polytechnic,Pune, BE in Computer Engineering from GSMCOE, ,Balewadi,Pune.Presently working as a HOD of Computer Technology in Ajitdada Pawar College Of Polytechnic, Shrirampur, A'Nagar,Maharashtra. Pursuing in Second year of ME Computer Engineering.

Baisa L Gunjal completed her BE Computer from University of pune and Mtech in I.T from Bharti Vidhyapeth India.Working as PG Co-coordinator in AVCOE College of Engineering, Sangamner, India. Presently she is working on research project on “Image Water marking” funded by BCUD, University of Pune.

management. In a relatively short span, the use of digital data hiding for covert communication has made a notable progress. In practical video storage and distribution system, the video sequences are stored and transmitted in compressed format. in spite more potential for commercial applications, less research has been conducted on high capacity data hiding in video streams. Though video steganography presents a much higher capacity or bandwidth, computational complexity is higher due to the amount of data that need to be processed. Here a blind data hiding technique tailored to AVI video stream. Data embedding and detection are carried out using a technique similar to for still images.

Since a video can be viewed as sequences of still images, video steganography is an extension of image steganography. The applications can thus be extended to video by embedding data in single frames.

2.2 The Related Work

There are three opportunities to hide information in video stream. The first opportunity is to hide secret information before encoded. Such method will encode and decode video sequences while hiding information. Thus, the hiding information is easy lost, and it is not convenient for extracting and detecting the hiding information. The second opportunity is to hide secret information while video encoder and decoder are processing. Facing a large amount of video streams, the cost of such method is very high. The third opportunity is to embed secret information into the compressed video directly. The advantage of the method is needless of encoding and decoding, but compressed ratio confine the capacity of hiding information and the designer of algorithm is more complex. So based on MPEG video structure and research of considering practical situation, here a method is presented that makes use of compressed DCT coefficients to hide information in video sequences.

The methods in the compressed domains are. For example techniques to embed a spread-spectrum watermark into MPEG-2 compressed videos. The basic ideas are generating a watermark signal for each frame of the video sequence exactly at the same manner, and arranging the watermark signal into a two-dimensional signal as the video frames. The capacity of hiding information is not large by the method. A compressed domain watermark technique called Differential Energy Watermark(DEW) in which the video is partitioned into groups of blocks each of which is further divided into two sets of equal size as determined by the watermark embedding key. The choice of the DEW standard is not easy. An algorithm dividing the 4*4 blocks into sub-blocks and modify only the coefficients within possibly as few as only one sub-block. It hides information within low-frequency coefficients. The method is just suitable for H.264 embeds information based on DCT coefficients, but each four MBs is embedded one bit, so the capacity of hiding is not large. And the method need insert stuffing bits in each MB in order to keep its original size another approach is the algorithm by adopting process quantify to dither modulate of double polarity parameter of DCT coefficient. When adopting quantifying to embed information, the selection of quantifying parameter is the linchpin, if the parameter is too small, then robustness is bad; if the parameter is too big, then imperceptibility is not good.

2.2 Data Hiding in GrayScale AVI Video:

In watermarking method needs to keep the three factors (capacity, imperceptibility and robustness) reasonably very high. Robustness is the ability to recover the data in spite of the attacks in the marked image, imperceptibility is the invisibility of the water- mark and capacity is the amount of data that can be embedded. These requirements are hindering each other. There must be some trade off among these requirements according to the applications. For medical images, in addition to the requirement on these factors, the region of interest (ROI) of the image must be particularly kept intact. This is an additional challenge to the researchers in this field.

- Imperceptibility:

Watermark embedded in the image must be invisible to humane eye for the secrecy and confidentiality.

- Robustness:

Robustness of the watermark is its ability to survive various image processing attacks. A secure watermark withstands against any purposeful attacks incurred on that. It should be able to recover information from the images.

- Capacity:

The data pay load that can be hidden must be as high as possible. This will make intender free from the restriction on the availability of space to write the data.

- Authenticity:

The data must be accessible only by the authentic users. Secret keys are used for this purpose.

- Reversibility:

The reverse should exist for the system of embedding to decipher the data from the image by the authentic user.

- Complexity:

The algorithm should be less complex to save execution time.

3 METHOD USED FOR DATA HIDING

Image Adaptive Data Hiding in Fixed DCT Locations using CDCS

Here a robust, blind data hiding scheme for images using new CDCS text characters. The proposed scheme also takes care of multiple levels of security and robustness of information while embedding.All embedding factors are further shared with the decoder (another doctor in this case) through embedding key which is automatically generated while executing the process of embedding. Therefore, even the person embedding the EPR information does not have explicit knowledge of places in medical images where the data is embedded.

AVI (Audio Video Interleave):

Audio Video Interleave (also **Audio Video Interleaved**), known by its acronym **AVI**, is a multimedia container format introduced by Microsoft in November 1992 as part of its Video for Windows technology. AVI files can contain both audio and video data in a file container that allows synchronous audio-with-video playback. Like the DVD video format, AVI files support multiple streaming audio and video, although these features are seldom used. Most AVI files also use the file format extensions developed by the Matrox OpenDML group in February 1996. These files are supported by Microsoft, and are unofficially called "AVI 2.0".

AVI is a derivative of the Resource Interchange File Format (RIFF), which divides a file's data into blocks, or "chunks." Each "chunk" is identified by a FourCC tag. An AVI file takes the form of a single chunk in a RIFF formatted file, which is then subdivided into two mandatory “chunks" and one optional "chunk".

4 System Implementation

Transmitter

1. Input AVI video file
2. Extract video frames
3. Randomly Select frames (Images) to hide the information
4. Select the text file to be embedded
5 .The DCT is applied separately to 8 x 8 blocks of the image i.e. called Block DCT.
6. Data is embedded in the host by modulating the quantized
7. Blocks DCT coefficients of frames.
8. Reconstruct the video from stego frames
9. Save the stego video file

Receiver

1. Input stego video file name
2. Extract frames from video file
3. Select the stego frames to extract the information
4. Provide stego key
5. Extract the information
6. Save the message files at receiver

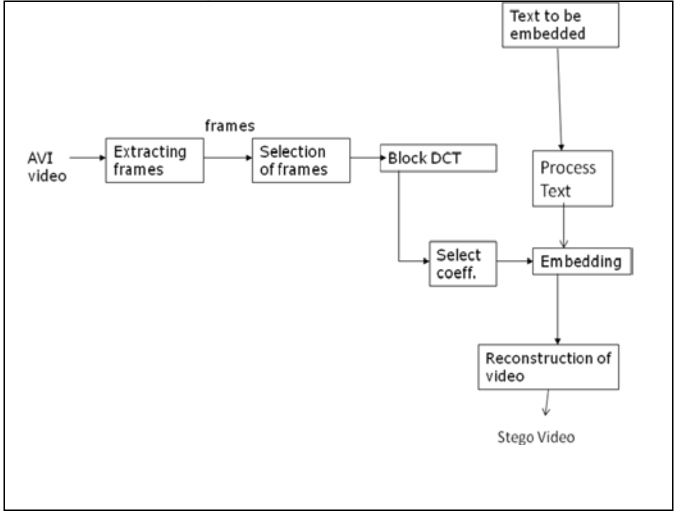


Fig. 1. Block Diagram

4.1 Embedding Scheme

As a avi video is composed of raw uncompressed bmp frames the technique used for hiding data in bmp image can be applied to frames. So here onwards first it is discussed how to hide the data in frame i.e image and then how to integrate the frames in to an stego video.The proposed embedding scheme consist of first text processing step which makes the stream of encoded bits of text ready for embedding and second image processing steps which actually embeds these bits into corresponding image. While doing so the embedding parameters provided as an input gets reflected in automatically generated embedding key. Both the steps along with extraction process have been explained in the following subsections.

4.2 Text Processing CDCS Encryption

> Read text file containing information to be hidden.
$T_t = \{t_1, t_2, ...t_h\}$ (1)
Where h= Total number of characters to be embedded.

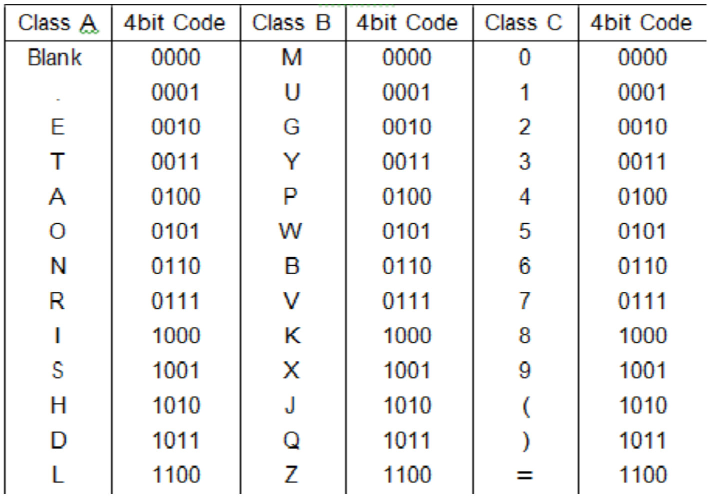
>Encrypt frequently appearing) and Class C (Less frequently appearing characters) depending upon previous fixed decimal codes or weight age.
Assuming only capital letters, alphanumeric and few special characters will further reduce number of bits needed to represent each character in each class. Based on Huffman encoding, we have designed variable length code to represent each class as given in following Table 1

Table 1
Class Dependent Codes Table

Class	Class Code	Length
A	1	1 bit
B	00	2 bit
C	01	2 bit

Each character in each Class will represented by only 4 bits, so in overall all classes can able to represent total 48 different characters which is sufficient for representing data. So this CDCS scheme combines advantages of both fixed length and variable length coding so to have less number of bits to represent same information compared to using fixed 7 bit ASCII codes. On the other hand Huffman encoding not only gives complexity but also assign a code word more than 32 bits for non-repeating characters.Division of characters in each class are given in Table 2 .If N1, N2 and N3 are the total number of characters belonging to Class A, Class B and Class C respectively, Total number of bits to be embedded is given by,

Table. 2
Fixed Codes within the Class Table



Class A	4bit Code	Class B	4bit Code	Class C	4bit Code
Blank	0000	M	0000	0	0000
.	0001	U	0001	1	0001
E	0010	G	0010	2	0010
T	0011	Y	0011	3	0011
A	0100	P	0100	4	0100
O	0101	W	0101	5	0101
N	0110	B	0110	6	0110
R	0111	V	0111	7	0111
I	1000	K	1000	8	1000
S	1001	X	1001	9	1001
H	1010	J	1010	(	1010
D	1011	Q	1011	)	1011
L	1100	Z	1100	=	1100

$$M = (N1 + 2N2 + 2N3) + 4 * H\text{bits} \qquad (2)$$

Where, $H = N1 + N2 + N3$ (3)

For a message "telemedicine" the number of 52 bits with CDCS as compared to 84 bits with ASCII. Here we have saved 32 bits (38.09% saving). This can further increase with message length as well as redundancy. This scheme not only saves number of bits to be embedded but also provides first level of security by assigning fixed codes to characters which is some sort of encryption that has to be predefined by both the transmitter and the receiver.

Our experimentation shows that embedding capacity can be increased up to 20% without any redundancy and upto 30% with redundancy of 3 bits with the help of this proposed effective CDCS technique.

- Add Bit Redundancy and Bit Interleaving to have robust recovery and error correc- tion. Add Redundancy to each bit of character for error correction and robust recovery [3] i.e. bits is replicated number of times decided by code rate so even if few bits are corrupted, others may be recovered successfully.

$Ter = \{e11, e12, ...e1r, e21, e22, ...e2r, ...em1, em2, ...emr\}$ (4)

Where r= Number of redundant bits.

- Interleave the information to disperse subsequent bits from each other [3] i.e. Sub- sequent bits are embedded in different blocks such that even if any block gives an error, other blocks can successsively recover the information.

Let, pn=Total number of bits after addition of redundancy, therefore equation (4) can be written as,

$Ter = \{b1, b2, ...bpn\}$ (5)

Let us divide this bit stream into p lines with n bits per line as,

$Ter = \{\{b1, b2, ...bn\}, \{bn+1, bn+2, ...b2n\}, ...\{b(p-1)n+1, b(p-1)n+2, ...bpn\}$ (6)

While embedding read the bits column wise so no subsequent bits should be em- bedded in same DCT blocks. So the final bit stream for embedding will be as given by equation (7).

$Ter = \{b1, bn + 1 ...b\ (p - 1)\ n + 1, b2, bn + 2 ...b(p - 1)n + 2, ..., ...bpn\}$ (7)

Robustness against various attacks such as image compression, resizing and tam- pering can be achieved by adding redundancy for each bit before it gets actually embedded. The bits are then read as a bit stream (B) in a particular way called interleaving of bits. This Interleaving of the bits will disperse subsequent bits from each other, i.e. subsequent bits are embedded in different blocks such that even if any block gives an error, other blocks can successfully recover the information. The number of redundancy to be added and number of interleaved bits has to be specified as embedding parameters. CDCS encryption along with specified number of redundancy bits added (r) and number of interleaving bits (n) gives first, second and third level of security (L1, L2 and L3) respectively.

Image processing steps Image Adaptive Embedding

A sequence of lower and middle frequency non-zero DCT2 coefficients of randomly gener- rated valid blocks are used to embed the bit stream (B). After dividing the image into 8 x 8 non overlapping blocks two dimensional DCT (DCT2) of each 8 x 8 block is taken. Then we calculate energy of each block [8]. The blocks having energy greater than threshold energy (Et) will only be considered for embedding.

- First divide the image into 8 x 8 non overlapping blocks.
- First take two dimensional Discrete Cosine Transform (2DCT) of each 8 x 8 blocks.

C = DC T 2(A)

Correspond to high frequencies tend to be zero or near zero for most natural images

- Calculate the Energy (E) of each 8 x 8 block [1] using following equation.

$$E_k = \sum_{i=1}^{7}\sum_{j=1}^{7}\left\| c_{ij} \right\|^2 \quad (3.4)$$

Here DC coefficient (i = j = 0) is not used.

- Find mean value of Energy (MVE) [3] and Energy Threshold (Et) [3] as,

$$MVE = \frac{\sum_{k=1}^{z} E_k}{z}$$

Where z= total number of 8*8 blocks (3.5)

Et = w * MV E

Where, w = Energy Threshold Factor

Find set of blocks having Energy greater than Et as embedding data in these blocks will cause minimal distortion. As the value of w increased, we get less number of valid blocks for embedding but perceptual quality increases. This Et need to be sent to receiver side as pa t of stego key [3]. This is second level of security.

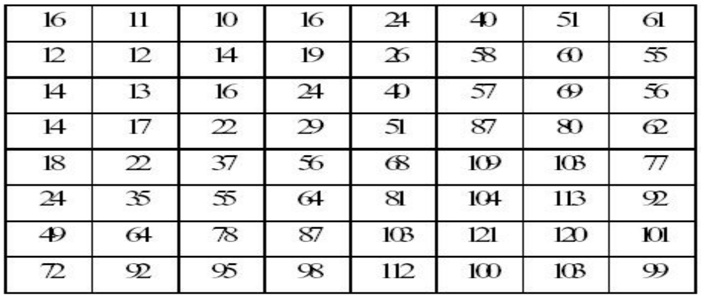
There is always a tradeoff between w and number of VBs .As the value of w increases, we get lesser and lesser number of VBs . However, more the value of w more will be the perceptual quality of the image. Therefore, more the value of w, more will be the values of Peak Signal to Noise Ratio (PSNR). In our proposed scheme, we are adaptively modifying the value of w by monitoring the PSNR of reconstructed image with respect to the set value of PSNR as shown in figure ??. The value of w for which stego image gives more than set value of PSNR will be consider as an embedding parameter and the reconstructed image will be treated as final stego medical image. This automatic adaptive selection of w gives flexibility to the doctors to quantify the perceptual quality of the stego image. The obtained energy threshold factor w is also act as another embedding parameter and gives fourth level of security (L4). Randomly select the valid blocks with random number generation whose seed value is given as a part of stego key. Fifth level of security (L5) is achieved by randomly selecting the VB. The random number generator based on a seed is used to select random VB. The seed value can be given as another embedding parameter. At this stage, even transmitter does not have explicit knowledge of blocks where the data is hidden. At this stage the selected block will undergo the process of quantization that have satisfied the following conditions are checked:

– Energy greater than Et for set value of PSNR

– Selected after Randomization

– Not coming under ROI

• Quantize above valid blocks with JPEG quantization so to select proper nonzero coefficients within the selected blocks. Quality Factor (QF=1 to 100) decides how much compression to be done.QF=100 refers to best quality image. As QF increases, number of valid coefficient needed for embedding decreases but QF also decides robustness required against JPEG compression attack. Table 2 shows values for standard JPEG quantization matrix when quality factor is 50. This table will be taken as reference for calculating quantization matrix for any other quality factor QF.



16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Table. 3
JPEG Standard Quantization Matrix for QF=50

Quantization Matrix value at i, j for Quality Factor QF.

After quantization if the block has all non-zero predefined DCT2 coefficients, then and then only the block will be consider for embedding the EPR bits. This gives robustness against natural JPEG compression attacks [8]. The quantization factor (QF) given for quantization is also acting as another embedding parameter and gives seventh level of security (L7).

• Hide data in each predetermined middle frequency band nonzero quantized DCT coefficient. After experimentation, it has been found that even after embedding in DCT locations like (2, 0), (0, 2), (2, 2), (3, 0), (0, 3) will give PSNR more than 40DB as well as moderate capacity. Hide bits given by equation (7) in all such fixed valid coefficients.The embedding is carried out by suitably modifying the predefined DCT2 coefficient of the blocks finally selected after the process of quantization. According to logical value of a bit to be embedded the rounded value of predefined DCT2 coefficient gets modulated. If the bit is logically ’zero’, then the coefficient is rounded to even number whereas the bit is logically ’one’, then the coefficient is rounded to odd number. While embedding, care taken that no VC becomes zero after embedding any bit as at receiver we are considering only nonzero coefficients and extracting bit from it.

• This final stage of embedding process consist of the reconstruction of stego image using Inverse DCT2 (IDCT2). Figure 3.1 shows all the steps of the proposed scheme. The reconstructed medical image is called as stego medical image. The PSNR of this image with respect to original medical image is calculated and compared with set value of the PSNR.

• At receiver, the extraction algorithm consists of all the image processing steps [10] that are carried out at the time of embedding the bit stream. After the process of quan- tization of DCT2 coefficients the EPR data bits are extracted. If the rounded value of predefined DCT2 coefficient is even, the bit is logically ’zero’ and if the rounded value of predefined DCT2 coefficient is odd, the bit value is logically ’one’. Once all the bits are extracted the characters of EPR information can be constructed using CDCS.

5 System specifications

• Hardware and Software:
Pentium-4(2.66GHz, 504 Mbytes Memory) with Windows XP, Java ,Java Media Framework Java media package and Video Quality Measurement Tool, Net Beans. Implemented in Java and results for DCT conversion in java verified with Matlab standard DCT functions. For quality assessment PSNR, MSE, metric used.
Source code = 2346 lines with 4 different modules consisting total 35 different functions: Extract frames from video,Text Process, DctModule, Transmitter, Receiver, convert frames to stego video.

• Database used:
Avi video which is created by using gray scale images of 512 * 512 size of different types.
• Preprocessing if needed: All images assumed to be noise free, distortion less and preprocessed.
• Input Given:

– To Transmitter: System specifications

• Hardware and Software:
Pentium- 4(2.66GHz, 504 Mbytes Memory) with Windows XP, Java and Matlab. Implemented in Java and results for DCT conversion in java verified with Matlab standard DCT functions. For quality assessment PSNR metric used.
Source code = 2346 lines with 4 different modules consisting total 35 different functions: Text Process, DctModule, Transmitter, Receiver.

• Database used:
Used standard grayscale potempkin.avi AVI video.

• Preprocessing if needed: All images assumed to be noise free, distortion less and preprocessed.

• Input Given:
– To Transmitter: EPR Text data file and(Randomly selected frame/Image file.
– To Receiver: Stego Frame/Image file and stego key.

• Output Produced:
– By Transmitter: Embedded final Stego frame/image file and stego key.
– By Receiver: Embedded text data.

• Criteria for acceptable output:
– PSNR of Stego medical image file should be >=40db.

– Embedding capacity depends on allowable distortion. But increased by rep- resenting each character using 5 or 6 bits with CDCS in Text processing step.

– It should sustain against certain common image processing attack up to certain extent. So BER acceptable is upto 5% maximum.

– It should be secure against steganalysis attacks, which mostly depends on amount of payload. More the data embedded, more will be easy to get de- tected by present steganalysis methods. So this puts constraints for embedding capacity.

6 Modules

• Text **Process Module** contains following functions,
– setFile function - reads data text file. – addTemplate function - adds fixed template to text file.
– addRedundancy function - adds 3/5/7 bits of redundancy to text data.
– forwardlookup function - converts ascii character into CDCS bit representation using fixed lookup table.
– reverse lookup function - converts CDCS bit representation into corresponding ASCII character using fixed reverse lookup table.
– Encode function - convert each message byte to CDCS bits representation.
– Decode function - convert retrieved bits back to one byte representation.

• **DctModule** Module contains following functions,

– readImage function - reads grayscale image data into 1D byte array.
– applyforwarddctfunc function - apply forward DCT to each 8 by 8 pixel block.
– applyinversedctfunc function - apply inverse DCT to each 8 by 8 DCT block.
– applyforwardembedfunc function - embed 1 bit of message in lsb of one fixed

DCT coefficient in each 8 by 8 DCT block.
– applyinverseextractfunc function - extracts 1 bit of message from lsb of one fixed DCT coefficient in each 8 by 8 DCT block.
– initMatrix function - initializes cosine basis matrices.
– applyQuantize function - Quantize DCT blocks using standard JPEG quanti- zation table for Quality factor=50.
– applyDeQuantize function - Dequantize DCT blocks back using same standard.
– Write Image function - writes final stego image in given directory.

• **DctModuleTest Module** -main class that calls functions of different modules for testing the output.
Text data file and Image file.
– To Receiver: Stego Image file and stego key.

• **Output Produced:**
– By Transmitter: Embedded final Stego image file and stego key.
– By Receiver: Embedded text data.

• Criteria **for acceptable output**:

– PSNR of Stego image file should be >=40db.

– Embedding capacity depends on allowable distortion. But increased by rep- resenting each character using 5 or 6 bits with CDCS in Text processing step.

– It should sustain against certain common image processing attack up to certain extent. So BER acceptable is upto 5% maximum.

– It should be secure against steganalysis attacks, which mostly depends on amount of payload. More the data embedded, more will be easy to get de- tected by present steganalysis methods. So this puts constraints for embedding capacity.

Randomization, Region of Interest (ROI) and Quantization

1. Energy greater than Et for set value of PSNR
2. Selected after Randomization

After the process of quantization if the block has all non-zero predefined DCT2 coefficients, then and then only the block will be consider for embedding the information bits. This gives robustness against natural JPEG compression attacks .The quantization factor (QF). Given for quantization is also acting as another embedding parameter and gives sixth level of security

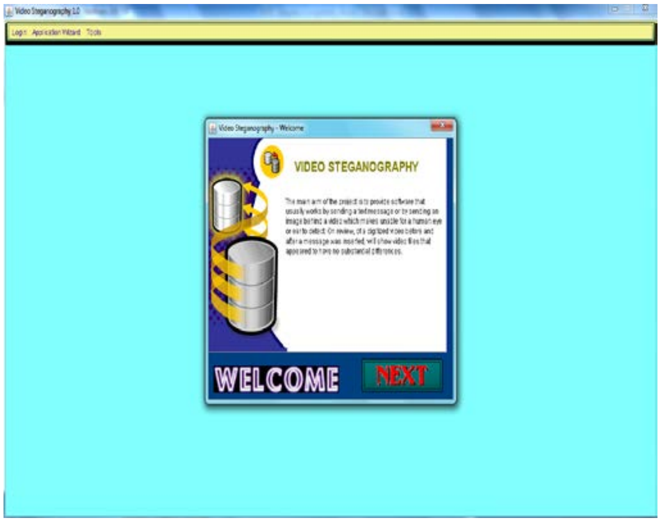
The embedding is carried out by suitably modifying the predefined DCT2 coefficient of the blocks finally selected after the process of quantization. According to logical value of a bit to be embedded the rounded value of predefined DCT2 coefficient gets modulated. If the bit is logically 'zero', the coefficient is rounded to even number whereas the bit is logically 'one'; the coefficient is rounded to odd number. That final stage of embedding process is the reconstruction of stego-image using inverse DCT2 (IDCT2). Fig. 1 shows all the steps of the proposed scheme.

The reconstructed medical image is called as stego medical image. The PSNR of this image with respect to original medical image is calculated and compared with set value of the PSNR. Our experimentation shows that after embedding entire EPR bits of information, the stego-medical images can give PSNR more than 40 dB.As mentioned in the previous sections, the embedding key plays an important role in extracting the EPR characters from stego-medical images. Fig. 2 gives embedding key automatically generated during the process of embedding. This embedding key has to be shared with the receiver through a secret channel as in case of normal blind steganographic techniques. However, the embedding key is not only just used as security key but also used to specify the embedding parameters to the receiver. These parameters are intern used by the data retrieval algorithm.

7 Advantages

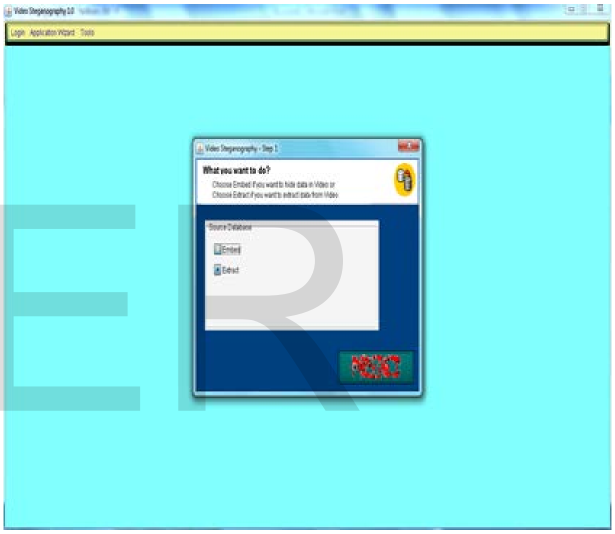
- Method is blind so no need of cover video at receiver end
- Effective means for covert communication.
- Provides Better security As selection of frames is random and .information can be extracted only after providing the stego key.

8 Results



The main aim of the project is to provide software that usually works by sending a textmessage or to sending an image behind a video which makes unable for a human eye or ear to detect. On review, of a digitized video before and after a message was inserted, will show video files that appeared to have no substantial differences.

Fig.2. Login Screen



What you want to do?

Choose Embed if you want to hide data in Video or
Choose Extract if you want to extract data from Video

○ Embed
● Extract

Fig.3. Options Embed & Extract

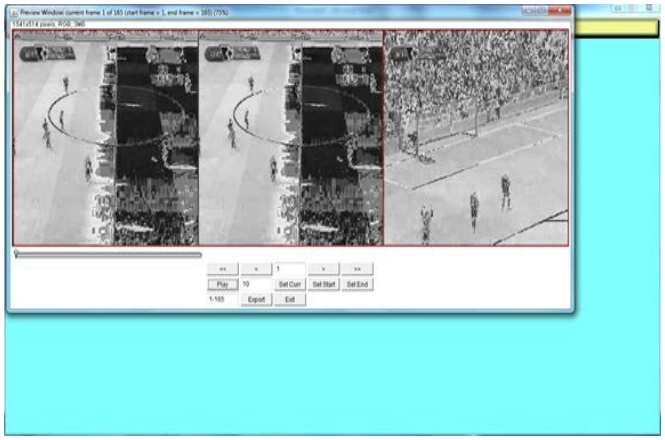

Preview Window (current frame 1 of 165 (start frame = 1, end frame = 165) (75%)
Play
Set Curr
Set Start
Set End
Export
Exit

Fig.4. Video Extraction

Fig.4. Video Extractor

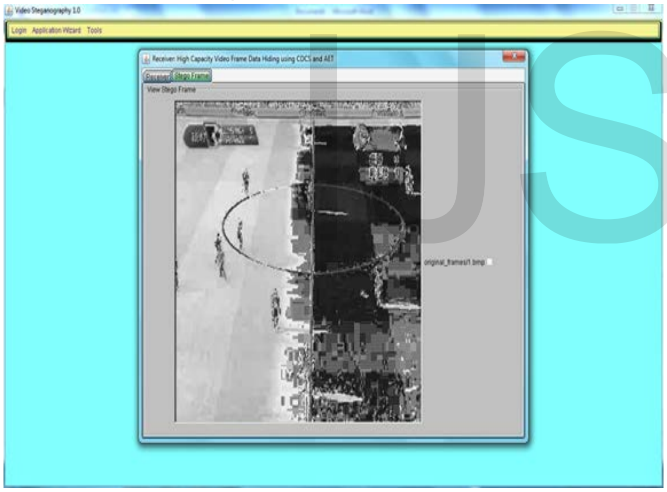
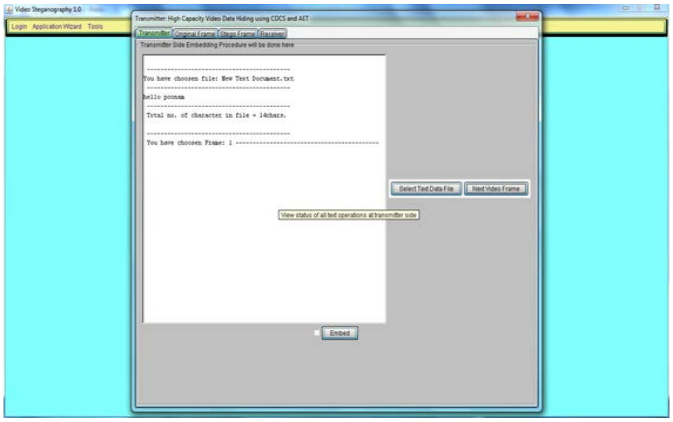


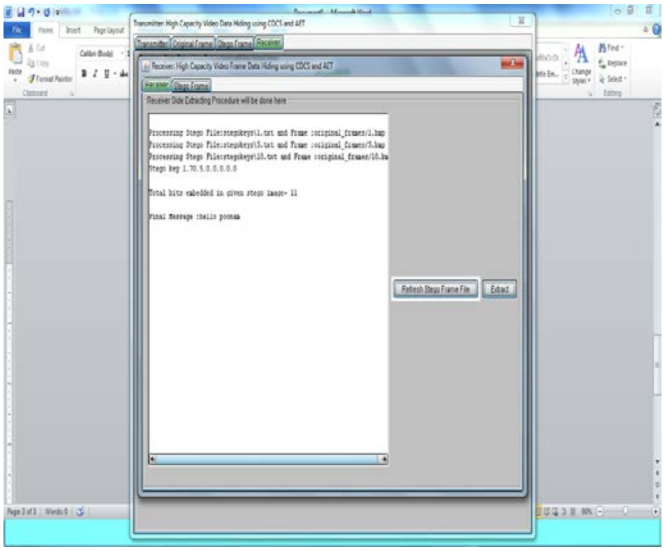
Fig.5. Stego frame


Video Steganography 1.0
Login
Application Wizard
Tools
Transmitter: High Capacity Video Data Hiding using CDCS and AET
Transmitter
Original Frame
Stego Frame
Receiver
Transmitter Side Embedding Procedure will be done here
Select Text Data File
Next Video Frame
View status of all text operations at transmitter side
Embed

```
 ----------------------------------------
You have choosen file: New Text Document.txt
 ----------------------------------------
hello poonam
 ----------------------------------------
 Total no. of character in file = 14chars.

 ----------------------------------------
 You have choosen Frame: 1 ----------------------------------------
```

Fig.6. Embedding data in the AVI File


Transmitter: High Capacity Video Data Hiding using CDCS and AET
Transmitter
Original Frame
Stego Frame
Receiver
Receiver: High Capacity Video Frame Data Hiding using CDCS and AET
Receiver
Stego Frame
Receiver Side Extracting Procedure will be done here
Refresh Stego Frame File
Extract

```
Processing Stego File:stegokeys\1.txt and Frame :original_frames/1.bmp
Processing Stego File:stegokeys\5.txt and Frame :original_frames/5.bmp
Processing Stego File:stegokeys\10.txt and Frame :original_frames/10.bm
Stego key 1.70.5.0.0.0.0.0.0

Total bits embedded in given stego image= 11

Final Message :hello poonam
```

Fig.7. Output at the Receiver End

CONCLUSION

The proposed System is based on the research findings developed an application which would be able to hide data into video images (AVI) that provides a robust and secure way of data transmission. This Stego system implements steganography in video image and reveal process without restarting a different application. Also this system is Platform Independent application with high portability and high consistency.

ACKNOWLEGEMENT

Thanks To IJSRT for accepting this paper. We are very thankful to Amrutwahini College of Engineering, Sangamner, and Ahemadnagar, India for providing us the opportunity to work on this project.

REFERENCES

[1] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, “Information Hiding—A Survey,” Proc. IEEE, 1999

[2] Niels Provos and Peter Honeyman, “Hide and Seek: An Introduction to
Steganography”, University of Michigan, IEEE 2003.

[3] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia,”Application of LSB Based Steganographic Technique for 8-bit Color Images”, WASET 2009

[4] Sutaone, M.S.; Khandare, ”Image based Steganography using LSB insertion technique”, IET, 2008.

[5] Mazdak Zamani, Azizah A. Manaf, and Shahidan Abdullah, “A Genetic- Algorithm-Based Approach for Audio Steganography” WASET 2009.

[6] Neeta Deshpande, Kamalapur Sneha, Daisy Jacobs, —Implementation of LSB Steganography and Its Evaluation for various Bits_ Digital Information Management, 2006 1st

International Conference on. 06/01/2007; DOI: 10.1109/ICDIM.2007.369349

[7] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image steganography: Concepts and practice. In WSPC Lecture Notes Series.

[8] Neil F. Johnson, Duric, Z., Jajodia, S. Information Hiding Steganography and Watermarking Attacks and Countermeasure. Kluwer Academic Press. Norwrll, MA, New York, The Huague, London vol 32.8(2010) 79-94

[9] Neil F. Johnson and S. Jajodia Exploring Steganography. Seeing the Unseen, IEEE Computer, vol. 31.2 (2010) 26 - 34.

[10] Min. Wu Joint Security and Robustness Enhancement for Quantization Embedding. IEEE Transactions, vol 0-7803-7750-8/03 (2012) 483-486.

[11] C. E. Shannon A mathematical theory of communication. Bell System Technical journal, vol. 27 (1948) 379-423.

[12] G. J. Simmons the prisoners' problem and the subliminal channel, in Advances in Cryptology. Proceedings of Crypto 83 (D. Chaum, ed.), Plenum Press vol 12.9(2010)51-67.

.