Information Hiding in Video using CDCS and Adaptive Embedding

Asha P. Choudhari
(Asst. Prof)MITAOE Alndi

ABSTRACT
The widespread of the internet and World Wide Web has changed the way digital data is handled. The rapid growth of digital media and communication networks has created an urgent need for self-contained data identification schemes to create adequate intellectual property right (IPR) protection technology in particular for image and video data [13].. By embedding an invisible and robust watermark into the image or video data, unauthorized copies can be traced and copy protection schemes can be implemented. There are several approaches to embed a watermark into an image or video frame [1].
In Steganography embedded data is invisible to a human observer. Information Hiding refers to techniques which are used for embedding additional data in host media. Here blind data hiding technique in video is proposed. The main aim of the proposed system is to send text information behind a video which is invisible for human eye. Here the system is Proposed for high capacity, robust and blind Information Hiding The in DCT(Discrete Cosine Transform) 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[11]. On review, of a digitized video before and after a message was inserted, will show video files that appeared to have no substantial visual differences. The DCT 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.

General Terms
Security,Information Hiding

Keywords
Information Hiding, DCT, Video, CDCS

1. INTRODUCTION
Information Hiding is a recently rapidly developed technique in the field of information security and has received significant attention from both industry and academia. It contains two main branches: digital watermarking and Steganography. The former is mainly used for copyright protection of electronic products while the latter as a new way of covert communication, conveys data secretly by concealing the very existence of information [3].
In general, there are two ways of Information Hiding in video. Hiding video content itself (video encryption or scrambling) so that nobody understands what is being transmitted; and the other is Embedding external information into the video, hence utilizing video as the data host. Under this category, one of the basic requirements for a Data Hiding method is the ability to produce video of high image quality. On top of that, additional properties are desired, depending on the application in question. In case of watermarking, the information embedded into a video should be able to withstand some common image processing attacks such as re-compression at a different bitrates, random video frame dropping, resizing, etc. In case of Steganography, the embedded information should stay undetectable with respect to Steganalysis which is a process for revealing the existence of hidden information in a suspicious video [1].
In applications such as annotation or indexing, even though it is not a compulsory required property, it is usually preferable to achieve reversibility so that the embedded information could be removed to restore the original video. Some representative Data Hiding methods in video domain are video watermark technique in motion vectors, digital watermarking of raw and compressed video. For example, Kiya et al. embed information into an MPEG compressed video by modifying coefficients at selected location(s) in each 8×8 quantized DCT coefficients block [1].

2. STEGANOGRAPHY
Steganography, coming from the Greek words stegos, meaning roof or covered and graphia which means writing, is the art and science of hiding the fact that communication is taking place. Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. Table 1 compares steganography cryptography and watermarking. In some situations, sending an encrypted message will arouse suspicion while an invisible message will not do so[9].

3. IMPLEMENTING STEGANOGRAPHY

3.1 Hiding a message inside a text
The best way of removing hidden messages from a plain text might be rewriting and reformulating the contents. Rewriting it using different words and sentence constructions will most certainly remove all ways of reproducing a hidden message, since it will take care of almost every possible way data can be stored inside a plain text. The character position schemes will no longer work because the words have been changed, and the same is valid for the differentiations in whitespacing, since the text will have a new layout. The only method that will not be covered by this technique is the usage of a publicly available cover source. Since this source cannot easily be altered, there is no effective way of stopping this method, except for intercepting the secret key [10].

3.2 Hiding a message inside an Image
Hiding Information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups. The use of Steganography in newsgroups has been researched by

German Steganographic expert Niels Provos, who created a scanning cluster which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of Steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many color variations, so less attention will be drawn to the modifications. The most common methods which are used to make alterations on the cover image are usage of the least-significant bit (LSB), masking, filtering and transformations. These techniques can be used with varying degrees of success on different types of image files [9][10].

3.3 Audio and video

Hiding information inside audio files can be done in several different ways. Using the least-significant bit is possible, as modifications will usually not create audible changes to the sounds. Another method involves taking advantage of human limitations. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks[9] [10].

4. VIDEO STEGANOGRAPHY

The recent development, demand and consumption of the digital video data in recent years has come up with some issues that we need to face, such as content security, authenticity, and digital rights management. In a relatively short span, the use of digital Data Hiding has made a notable progress. In practical video storage and distribution system, the video sequences are stored and transmitted in compressed format. Video Steganography has wide range of applications like copyright protection and user identification, Covert Communication Source Tracking (Different recipients get differently Hidden content),Broadcast Monitoring, Information Hiding techniques that could be used in order to give a description of the scene i.e. could be used for video indexing, subtitling, multi-lingual services, teletext, etc. Despite 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. 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 selected frames[1][2][3].

4.1 Video Basics

A compression encoder works by identifying the useful part of a signal which is called the entropy and sending this to the decoder. The remainder of the signal is called the redundancy because it can be worked out at the decoder from what is sent. Video compression relies on two basic assumptions. The first is that human sensitivity to noise in the picture is highly dependent on the frequency of the noise. The second is that even in moving pictures there is a great deal of commonality between one picture and the next. Data can be conserved both by raising the noise level where it is less visible and by sending only the difference between one picture and the next.In a typical picture, large objects result in low spatial frequencies whereas small objects result in high spatial frequencies. Human vision detects noise at low spatial frequencies much more readily than at high frequencies. The phenomenon of large-area flicker is an example of this. Spatial frequency analysis also reveals that in many areas of the picture, only a few frequencies dominate and the remainder is largely absent[12].

4.2 Frame/picture/block types

I-frames

I-frame is an abbreviation for Intra-frame, so-called because they can be decoded independently of any other frames. They may also be known as I-pictures, or keyframes due to their somewhat similar function to the key frames used in animation. I-frames can be considered effectively identical to baseline JPEG images. High-speed seeking through an MPEG-1 video is only possible to the nearest I-frame. When cutting a video it is not possible to start playback of a segment of video before the first I-frame in the segment (at least not without computationally-intensive re-encoding). For this reason, I-frame-only MPEG videos are used in editing applications. The length between I-frames is known as the group of pictures (GOP) size. MPEG-1 most commonly uses a GOP size of 15-18 i.e. 1 I-frame for every 14-17 non-I-frames (some combination of P- and B- frames). With more intelligent encoders, GOP size is dynamically chosen, up to some pre-selected maximum limit [12].

P-frames

P-frame is an abbreviation for Predicted-frame. They may also be called forward-predicted frames or inter-frames (B-frames are also inter-frames).P-frames exist to improve compression by exploiting the temporal (over time) redundancy in a video. P-frames store only the difference in image from the frame (either an I-frame or P-frame) immediately preceding it (this reference frame is also called the anchor frame).The difference between a P-frame and its anchor frame is calculated using motion vectors on each macroblock of the frame. Such motion vector data will be embedded in the P-frame for use by the decoder. A P-frame can contain any number of intra-coded blocks, in addition to any forward-predicted blocks. If a video drastically changes from one frame to the next (such as a cut), it is more efficient to encode it as an I-frame [12].

B-frames

B-frame stands for bidirectional-frame. They are also known as backwards-predicted frames or B-pictures. B-frames are quite similar to P-frames that except they can make predictions using both the previous and future frames (i.e. two anchor frames).It is therefore necessary for the player to first decode the next I- or P- anchor frame sequentially after the B-frame, before the B-frame can be decoded and displayed. This makes B-frames very computationally complex, requires larger data buffers, and causes an increased delay on both decoding and during encoding. This also necessitates the display time stamps (DTS) feature in the container/system stream.They are often avoided in videos, and are sometimes not fully supported by hardware decoders [12].

4.3 Related work

It is observed that information can be embedded or hidden in video stream by following different ways. One of them is to hide secret information before encoding 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. Then next is to hide secret information while video encoder and decoder are processing. So if it involves a large amount of video streams, the cost of such method is very high. The last is to embed secret information into the compressed video directly. The advantage of the method is It is not dependant on encoding and decoding, but as we are going to hide the information in compressed video it puts the

limitation on the capacity of information to be hidden and the also algorithm is more complex[3].
The methods in the compressed domains are. For example technique to embed a spread-spectrum watermark into MPEG-2 compressed video. A compressed domain watermark technique called Differential Energy Watermark (DEW) partitions video into groups of blocks and each of which is further divided into two sets of equal size as determined by the watermark embedding key but here also choice of the DEW standard is not easy [5]. Nakajima et al. proposed a high carrier capacity Data Hiding method utilizing the idea of zerorun length coding in MPEG domain. After zigzag scanning, a dummy nonzero value is inserted at a location that is x units away from the original last nonzero qDCTC, where x depends on the data to be embedded. Zhang et al. utilize (MV) motion vectors in P and B-pictures as the data carriers for data embedding. An MV is selected based on its magnitude, and its angle guides the modification operation. In these existing works, qDCTC or/and MV is/are usually utilized as the data carrier. Therefore, modifications done to the video during data embedding may alter the video bitrate [1].

5. SYSTEM DESIGN & IMPLEMENTATION

Steganographic methods generally need 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 information hidden 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.
The process of embedding information in video is broken down into information embedding in image because a video stream can be considered as a sequence of still images. Here the proposed method uses uncompressed AVI video as an input since it is the stream of raw Bit Map Picture (BMP) images. The message data is embedded in the DCT domain, by modifying the projections of the 8x8 host block DCT coefficients. It is desirable that the methods of embedding and extracting are resistant to typical signal processing operations, such as compression, and intentional attacks to remove the hidden information.
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. An AVI file may carry audio/visual data inside the chunks in virtually any compression scheme, including Full Frame (Uncompressed), Intel Real Time (Indeo), Cinepak, Motion JPEG, Editable MPEG, VDOWave, ClearVideo / RealVideo, QPEG, and MPEG-4 Video[14].
Figure 1 shows steps involved in the proposed method. First step is video processing where the frames are extracted from input AVI video. Then frames are selected. Image Processing steps which actually embed bits are performed on each selected frame (image). Text processing step is the one which makes the stream of encoded bits of text ready for embedding. While doing so the embedding parameters provided as an input gets reflected in automatically generated embedding key.

As AVI video is composed of raw uncompressed bmp frames the technique used for hiding data in bmp image is applied to the selected frames. So first it is discussed how the data is hidden in frame i.e. image and ultimately how the frames and stego frames are used to reconstruct to get stego video.

5.1 CDCS

we have assigned fixed decimal codes in CDCS to each character by considering their relative frequency of occurrences. We categorized them in three different non overlapping special classes as Class A (most frequently appearing character set), Class B (Average frequently appearing) and Class C (Less frequently appearing characters). Assuming only capital letters, alphanumeric and few special characters will further reduce the 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 Table 2.Any character in each Class will be represented by only 4 bits. Therefore, Class Code along with character code can distinguish 48 different characters which are sufficient for normal data. In other words proposed CDCS combines the advantages of both fixed length and variable length coding to get lesser number of bits to represent same information compared to using fixed 7 bit ASCII codes. On the other hand Huffman coding is complex and also assigns codes with more than 32 bits for non repeating characters. Division of characters in each class is given in Table 3. If N_1, N_2 and N_3 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,

$$m = (N_1 + 2N_2 + 2N_3) + 4h \qquad (1)$$

where, $h = N_1 + N_2 + N_3$,
i.e. total number of characters in data fie. A message "telemedicine" needs only of 61 number of bits with CDCS as compared to 84 bits with ASCII. Here we have saved 23 bits (27.38 % saving). This saving can further be increase with increase in message length as well as increase in number of redundancy. The CDCS scheme is not only saving the number of bits per character but also provides security[11].

5.2 Redundancy and Interleaving

Robustness against various attacks such as image compression, resizing and tampering 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 and second level of security (S1 and S2) respectively[11].

5.3 Energy Thresholding

A sequence of lower and middle frequency non-zero DCT2 coefficients of randomly generated 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. The blocks having energy greater than threshold energy (E_t) will only be considered for embedding[11].

$$E_t = \hat{w} \cdot MVE \quad (2)$$

where, ŵ = Energy Threshold Factor and MVE = Mean Value of Energy given by,

$$MVE = \frac{1}{z} \sum_{k=1}^{z} E_k \quad (3)$$

where, z = Total number of 8 x 8 non-overlapping blocks of the image and E_k = Energy of k^{th} block which is given by,

$$E_k = \sum_{i=1}^{7} \sum_{j=1}^{7} \| C_{ij} \|^2 \quad (4)$$

where C_{ij} = DCT2 coefficients.

(DC coefficient is neither taken for the calculation of energy nor is it used for embedding). The blocks having more energy can embed information bits with minimal distortion. Therefore, block having energy more than E_t will only be considered for embedding and treated as Valid Blocks (*VB*).

5.4 Adaptive Energy Threshold Factor ($\hat{w}$)

There is always a trade-off between ŵ and number of VB. As the value of ŵ increases, we get lesser and lesser number of VB. However, more the value of ŵ more will be the perceptual quality of the image. Therefore, more the value of ŵ, more will be the values of Peak Signal to Noise Ratio (PSNR). In our proposed scheme, we are adaptively modifying the value of ŵ by monitoring the PSNR of reconstructed image with respect to the set value of PSNR. The value of ŵ 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 ŵ gives flexibility to quantify the perceptual quality of the stego image. The obtained energy threshold factor ŵ is also act as another embedding parameter and gives third level of security (S3)[11].

Algorithm:

Transmitter

accept Input AVI video file
extract video frames
select frames (Images) automatically to hide the information
select the text file to be embedded
select the Energy threshold value
process text information to make it suitable to be embedded in frame
applie DCT to 8 x 8 blocks of each image i.e. called Block DCT.

It is observed that if the frames used from original video for hiding the information are kept constant and number

embed in the host by modulating the quantized blocks DCT coefficients of Frame.
stego key is generated which will be used at receiver for extracting information
save the stego frame
repeat the steps from calculation of Block DCT to save stego frame for each selected frame in video
reconstruct Stego video from stego frames and original frames
end

Receiver
accept stego video file
stego keys are selected
extract all frames and select stego frames from stegovideo file
extract the information
save the message files at receiver
end

6 EXPERIMENTAL RESULTS

Embedding capacity depends on allowable distortion. But increased by representing each character with CDCS technique in Text processing step. Stego Video should give acceptable results for the video quality metrics like PSNR Drop Frame Metric, Brightness Flickering Metric or Mean Square Error .It should sustain Steganalysis attacks, which mostly depends on amount of payload. More the data embedded, more will be easy to get detected by present Steganalysis methods. So this puts constraints for embedding capacity. This Current system works on uncompressed grayscale avi video, but as the video is uncompressed file size is more this puts limitation on memory. This system is not lossless and reversible as embedding data in frame results in a permanent distortion of the original frame or hidden data but within acceptable range.

The System Provides entry to the application only after correct username and Password are entered. The main module in the application as shown in figure 2 which performs the actual process of embedding and extraction. Video and text file is provided as input by the user. This module embeds the text information in selected frames of the video. The user will also select Energy threshold factor initially that will be applied for remaining selected frames also.Video Extractor module Extract the frames from avi video and display the video to the user It also provide frame wise view and separate panels to display the first and last frame.Video Quality Measurement Tool is used.The test analysis is presented. Experiments are carried out on different video files.The details of video used for hiding the information are given below. It is observed that if the frames used from original video for hiding the information are kept constant and number of frames available in video are more the average PSNR of video is also more.In current video there are 11 frames so the average value of PSNR is less compared to the video with 16 frames. The graph and PSNR Values for individual frames of original video and stego video are shown in Table 4 and the corresponding graph is shown in fig.3.

Original Video : Airtel.avi Stego Video : stegoairtel.avi
Airtel.avi video frames : 11 stegoairtel.avi video frames: 11
Threshold factor : 0.4 Quality factor (Fixed) :70
Redundancy : 1 Data hidden in frame nos. :1,5,10

of frames available in video are more the average PSNR of video is more. The major advantage of Information Hiding in

video sequence is that there is no visual distortion in video. The changes are made only too few frames of the video so it is left unobserved by viewer. PSNR After compression of video. The Compression attack is performed on stegoAirtel.avi. File is compressed and uncompressed to observe any loss or change in data hidden. It is observed that the data remains intact under compression attack and there is no change in the value of PSNR of stego video without compression and with compression as shown in.Table 5.Here we can see the perceptual transparency of each frame. In the current system three frames i.e. frame1 frame5 frame10 are used to hide the information and the remaining frames are untouched so when the stego video is reconstructed there is no visible distortion or change in stego video. This is the major advantage only video can provide because of large number of frames available in it.

Comparision ASCII and CDCS Information Hiding depicts that Information Hiding with CDCS gives better PSNR for ndividual frames in video and also for the video as a whole than Information Hiding with ASCII.Details of parameter which are used while performing experiment kept constant in both the techniques **.**

7. CONCLUSION AND FUTURE SCOPE

An Integrated data hiding method that completely preserves the image quality of the host video has been proposed in the uncompressed video domain.During video playback, the modified video completely reconstructs the original video even. The proposed method is a blind Information Hiding technique for uncompressed AVI stream which provides high Information Hiding capacity and robustness against the attacks such as compression and tampering . It is theoretically and experimentally verified that CDCS outperforms ASCII in terms of PSNR and embedding efficiency. As future work, we seek for possible extensions of our data hiding method to withstand Video compression.The advantage of the proposed method is that the embedded message could still be extracted after common image processing attacks like compression done at video level and tampering done at frame level.

Information Hiding in video with CDCS not only increases the embedding capacity but provides one level of security by encrypting the text information at early stage of embedding process also. Various Experiments are performed for the Video Quality metrics e.g Brightness Flickering Metric,PSNR,MSE and it is observed that its values are in acceptable limits with the proposed method. As we are using energy thresholding and JPEG quantization matrix for qualifying the coefficients of information embedding, the possibility of loss of information gets drastically reduced. However, as level of compression increases, the number of valid coefficients gets reduced which intern reduces the data hiding capacity.This method is secured because of three reasons :Randomization used while selecting the valid blocks for embedding.The seed provided by the person embedding the information decides the specific random sequence of blocks selected for embedding.Energy thresholding allows the scheme to select valid blocks having energy greater than threshold.This thresholding gives another randomization in which even the person embedding the information does not have explicit knowledge of blocks having information embedded in it. Quantization does not allow all the DCT2 coefficients from selected block for embedding.This gives another constraint for the coefficients to be become eligible for embedding.The Information hiding in uncompressed avi video though require more memory to store, but is a simple implementation without visible distortion.The method takes the advantage of large number of frames present in video.The method is also found robust against attacks such as tampering and compression In case of tampering the data is lost only for the loactions where frame is tampered, remaining parts information is retrived successfully.

There are various Video compression techniques available and the method needs to be enhanced in order to work on them .The work is more challanging as video involves two levels of compression intraframe and interframe.The approach can also be applied to color video.Content Authentication.Verifying data integrity with watermarking is part of the broader area of content authentication. This is continually becoming more of a challenging area as it is very easy to modify multimedia content. For example,digital information can be tampered with modern software in ways that are difficult to detect.

TABLE 1 Comparision Steganography,Watemarking, Cryptography

Criterion/Method	Steganography	Watermarking	Encryption
Carrier	any digital media	mostly image/audio files	Usually text based ,
Secret data	payload	watermark	plain text
Key optional	optional	optional	Necessary
Input files	at least two	at least two	One
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	secrete communication	copyright preserving	data protection
Result	Stego file	Watermarked file	cipher-text
Concern	delectability/ capacity	robustness	Robustness
Type of attacks	Steganalysis	image processing	Cryptanalysis
Visibility	never	sometimes	Always

Table 2: CDCS: Class code

Class	Class code	Length
A	1	1-bit
B	00	2-bit
C	01	2-bit

Table 3: Fixed Codes within Each Class

Class A	Class B	Class C	4-Bit Code
Blank	M	0	0000
.	U	1	0001
E	G	2	0010
T	Y	3	0011
A	P	4	0100
O	W	5	0101
N	B	6	0110
R	V	7	0111
I	K	8	1000
S	X	9	1001
H	J	(	1010
D	Q	)	1011
L	Z	=	1100
F	,	*	1101
C	-	%	1110
:	_	+	1111

Table 4 : PSNR comparision between original and stego video

Frame No	PSNR
1	43.51383
2	No change
3	No change
4	No change
5	43.62121
6	No change
7	No change
8	No change
9	No change
10	44.21612
11	No change

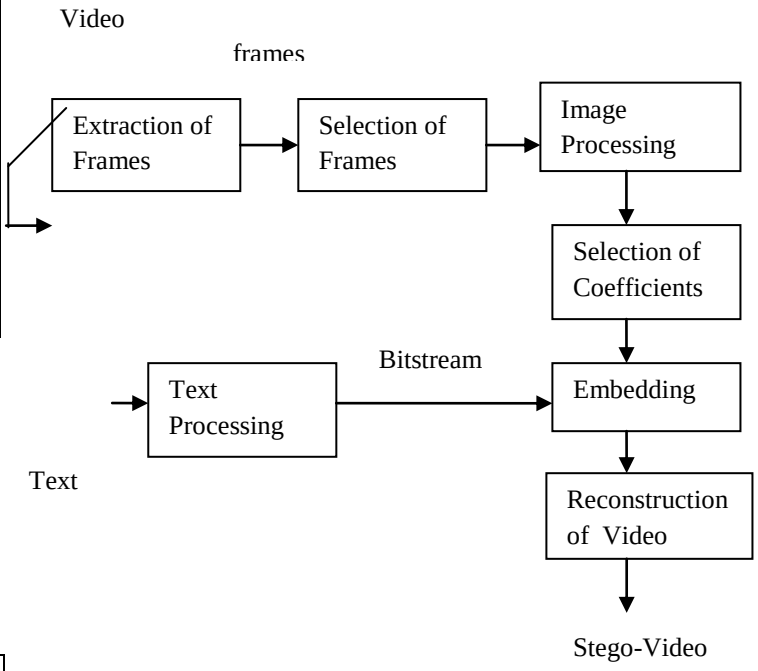

Figure 1: System Block Diagram

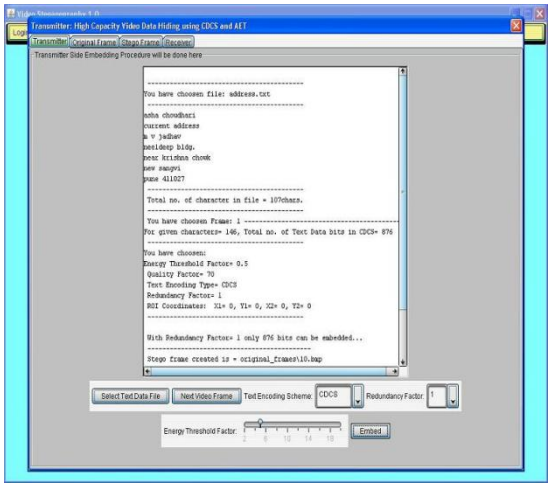

Figure 2: Main Panel

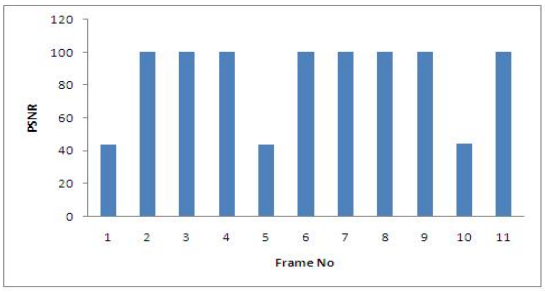

Figure 3: Graph showing PSNR of Stego and untouched frames

Table 5: PSNR comparision between original video and stego video after uncompression

Frame No	PSNR
1	43.51383
2	No change
3	No change
4	No change
5	43.62121
6	No change
7	No change
8	No change
9	No change
10	44.21612
11	No change

7. REFERENCES

[1] KokSheik Wong and Kiyoshi Tanaka , Complete Video Quality-Preserving Data Hiding , IEEE Transactions on Circuits and Systems For Video Technology,vol. 19, 2009.

[2] F.A.P.Petitcolas, R.J.Anderson and M.G.Kuhn, `Information Hiding-A Survey ,Proceeding of the IEEE, vol. 87, pp.1062-1078 , 1999, .

[3] Changyong Xu and Xijian Ping, Steganography in Compressed Video Stream , Proceedings of the First International Conference on Innovative Computing, Information and Control, (ICICIC'06),IEEE 2006.

[4] Peng Zheng , Bo Zhao and Min-zhong Liu, An Efficient Method to Hide Information in MPEG Video equences, International Conference on Multimedia Information Networking and Security, 2009.

[5] Y.Wang and E.Izquierdo, High-Capacity Data Hidingin MPEG-2 Compressed Video, Proceeding of the 9th International Workshop on Systems, Signals and Image Processing, Manchester, U.K, pp.212-218, 2002 .

[6] S. Katzenbeisser and E A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking , Artech House, Boston, MA, 2000.

[7] Suresh N. Mali and Rajesh M. Jalnekar, ``Imperceptible and Robust Data Hiding using Steganography Against Image Manipulation, International Journal of Emerging Technologies and Applications in Engineering, Technology and Sciences,(IJ-ETA- ETS) pp.84-91, 2008.

[8] Kaushal Solanki , Noah Jacobsen and Upamanyu Madhow, Robust Image-Adaptive Data Hiding using Erasure and Error Correction, IEEE Transactions on image processing, Volume 13, pp.1627-1639, 2004 .

[9] J.R. Krenn ,Steganography and Steganalysis , 2004.

[10] N. F. Johnson and S.Jajodia Information Hiding: Steganography and watermarking attacks and countermeasures, Kluwer academic Publishers 2000.

[11] Dr. Suresh N. Mali ,Content Security Enhancement by Effective Encryption and Sealed Steganography, Ph.D. Thesis.

[12] SNELL & WILCOX , MPEG Encoding Basics .

[13] Gerrit C. Langelaar and Reginald L. Lagendijk, Optimal Differential Energy Watermarking of DCT Encoded Images and Video ,IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 1, JANUARY 2001

[14]http://en.wikipedia.org/wiki/Audio_VideoInterleave .