1. Introduction

Many digital watermarking schemes have been proposed for still images and videos. Most of them operate on uncompressed videos, while others embed watermarks directly into compressed videos. Video watermarking introduces a number of issues not present in image watermarking. Due to inherent redundancy between video frames, video signals are highly susceptible to attacks such as frame averaging, frame dropping, frame swapping and statistical analysis [1]. Video watermarking approaches can be classified into two main categories based on the method of hiding watermark bits in the host video. The two categories are:

Spatial domain watermarking where embedding and detection of watermark are performed by directly manipulating the pixel intensity values of the video frame. Transform domain techniques, on the other hand, alter spatial pixel values of the host video according to a pre-determined transform and are more robust than spatial domain techniques since they disperse the watermark in the spatial domain of the video frame making it difficult to remove the watermark through malicious attacks like cropping, scaling, rotations and geometrical attacks. The commonly used transform domain techniques are Discrete Fourier Transform (DFT), the Discrete Cosine Transform (DCT), and the Discrete Wavelet Transform (DWT).

2. Statement and scope of the problem

The ideal properties of a digital watermark include the imperceptibility and robustness. The watermarked data should retain the quality of the original one as closely as possible. Robustness refers to the ability to detect the watermark after various types of intentional or unintentional alterations (so called *attacks*). Various watermarking schemes have been proposed in the present. Unfortunately, up to now there is no algorithm that perfectly fulfils the aforementioned fundamental watermarking requirements: the imperceptibility to the human visual perception and the robustness to any kind of watermarking attacks. Particularly this fact was a challenge to investigate the opportunities of designing watermarking techniques being capable to achieve the imperceptibility and robustness criteria.

The problems for video Watermarking are as follows:

- Video media is susceptible to increased attack than any other media.
- Video content is sensitive to subjective quality and watermarking may degrade over the time.
- Video compression algorithms are computationally intensive hence there is less headroom for watermarking.
- Video bandwidth hungry and that is why it is mostly carried in compressed domains.

Scope of the problem:

- Due to all of the above problems watermarking algorithm shall be adaptable for domain processing.
- Working with low bit rate video gives additional challenges as there is less room for watermark.
- During video transmission, frames drops are very usual. If data spreads over many frames, in case of frame drop, watermark data becomes irreversible, watermark should be robust against such phenomenon of watermarking in compressed domains. .

3. Literature Survey

Steganography is the act of adding a hidden message to an image or another medium file while watermarking is similar, but has a completely different purpose. Placing a watermark in an image or other media file serves to identify the artist or author of the work.

The main goal of steganography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d' while the main goal of watermarking is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace m in d'.

It is also often said that the goal of steganography is to hide a message in one-to- one communications and the goal of watermarking is to hide message in one-to- many communications.

Digital Robust Video Watermarking

IJAET/vol I/Oct.-Dec, 2010/101-113

Digital watermarking algorithms are widely applied to digital image, audio or video for ownership protection and tampering detection. Digital watermarking is the process of reversibly or irreversibly embedding information into a digital signal. In this paper, Video watermarking algorithm based on discrete wavelet transform scheme is proposed. In which, the video is firstly divided into frames and each frames are divided in to three images of red, blue and green, then DWT (Discrete Wavelet Transform) is performed on each digital image.

S.No.	Publisher and Date	Title	Objective	Method/ Algorithms/ Techniques	Future work
1	Chichester, U.K.: Wiley, 2003.[1]	H. 264 and MPEG-4 Video CompressionVideo Coding for Next-Generation Multimedia	Introduce the video coding tools that the standard supports and how these tools are organized into profiles. discuss how the various video coding tools of the standard work, as well as the related issue of how to perform encoding using these tools	DCT	A number of additional elements of the standard such as, tools that provide system support, details of levels of profiles, and the issue of encoder and decoder complexity.
2	IEEE, march,2007[2]	A framework for robust watermarking of H.264-encoded video with controllable detection performance	This paper proposes a robust watermarking algorithm for H.264. We employ a human visual model adapted for a 4* 4 discrete cosine transform block to increase the payload and robustness while limiting visual distortion	DCT	We only showed the robustness of our algorithm to a trivial deliberate attack. Implementing more complex adversary's attempts to erase the watermark is a subject of further study.
3	IEEE, Dec,2008[3]	Towards fast and robust watermarking scheme for H.264 video	we present a novel watermarking scheme, which satisfies with the requirements of both rapidity and robustness. The proposed scheme directly embeds watermarks into H.264 bitstreams at the decoder by modifying the quantized DC coefficients in luma residual blocks	DCT	A novel decoder-based watermarking scheme for H.264 is proposed. The watermarks are adaptively embedded into luma residual blocks after partially decoding the bitstream.Can be furtther improved for robustness and efficiency.
4	IEEE, Oct,2007[4]	Data hiding in H. 264 encoded video sequences	A new method for high capacity data hiding in H.264 streams is presented. The proposed method takes advantage of the different block sizes used by the H.264 encoder during the inter prediction stage in order to hide the desirable data	H.264 video encoder Algorithm.	In our current scheme we used only 4 different block types, namely 16*16, 16*8, 8*16,8*8.However the scheme can also use the sub partitions of the 8x8 type (8x4, 4x8, 4x4), thus increasing the available bits for coding to 8.

5	IEEE Aug 2004[6]	A hybrid watermarking scheme for H.264/AVC Video.	By embedding the robust watermark into DCT domain and the fragile watermark into motion vectors respectively, the proposed method can jointly achieve both copyright protection and authentication.	DWT	the optimal selection of prediction mode and motion vectors in H.264/AVC is supported by slightly modifying the Lagrangian optimization functions in order to curb the bit-rate increase. The experiment results show that our method is able to withstand transcoding and at the same time cause unnoticeable quality degradation.
6	IEEE Feb,2007[5]	Robust video watermarking of H.264/AVC	The video watermarking scheme can achieve high robustness and good visual quality without increasing the overall bit-rate.	DWT	Detailed copyright information, such as textured company trademarks or logos can be used as watermark to further protect ownership and defend against the illegal attacks. To protect copyright, how to combine the proposed embedding techniques with noninvertible watermarking will be future research.
7	IEEE Aug 2002[10]	Compressed-domain video watermarking of MPEG streams	The watermarking scheme operates directly in the domain of MPEG program streams. Perceptual models are used during the embedding process in order to preserve the video quality. The watermark is embedded in the compressed domain and is detected without the use of the original video sequence	DWT	Due to its speed, the resulting system is suitable for real-time content authentication applications. Experimental evaluation showed that the proposed watermarking scheme is able to withstand a variety of attacks.

4. Motivation

Since ancient times, there has been an effort to hide information within seemingly harmless information to avoid unwanted attention. The science of concealing information was later to be known as “steganography” and the current technology of “Digital Watermarking” has taken its root from it. The term “watermark” in terms of digital data was taken from the concept of watermarks used to prevent faking of currency notes.

“Watermarking” deals with embedding information like name of the creator, status, recipient, etc. into the host data in such a way that it remains transparent or undetectable. The watermark information should be embedded in such a way that this should not be detectable and removable even after many spurious or innocuous attempts. Watermarking can be done for any form of digital data – text, image, audio, or video where copyright needs to be protected.

Methods for embedding watermark information may vary between types of media, but the basis of these methods remain more or less same.

Digital media (image, video, audio, etc.) are now widely distributed on the Internet. Because of easy reproduction and manipulation of digital media, the protection of intellectual property rights has become an important issue. Digital watermarking is expected to be a perfect tool for protecting the intellectual property rights. The main advantages of the watermarks over other techniques are:

- They are imperceptible.
- They are not removed when the data are converted to other file formats.
- They undergo the same transformations as the data in which they are embedded.

5. Proposed Approach and Methodology

The GOP structure:

GOP denotes the group of pictures. Since the MPEG-1 standard, several types of frames are used: I, B, and P frames. I frames are transmitted encoded using the algorithms used for the JPEG files. It is the so-called intra-frame encoding, because an I frame contains the full picture information and does not need other frames in the GOP. Each GOP must start with an I frame. A GOP is defined to be a sequence of frames between two succeeding I frames. The video stream is composed of GOPs. A GOP is formed by sequence of frames. Each frame consists from the slices of macroblocks, and each macroblock is a set of four 8x8 matrices.

P frames and B frames are outer-frame encoded. It means, they do not contain the full picture information, but only references to parts of the previous or succeeding frames. Each P frame is created using the previous I or P frame, the so called forward prediction. Moreover, there is also the backward prediction used for the B frames. B frames are created using the bidirectional interpolation prediction. Firstly, the forward prediction is determined, then the backward. The encoder then makes a decision about the ratio for calculating the average from both of these predictions. The B frames are then not used for further predictions due to a large number of errors (the largest in comparison with I and P frames) they bring into the picture.

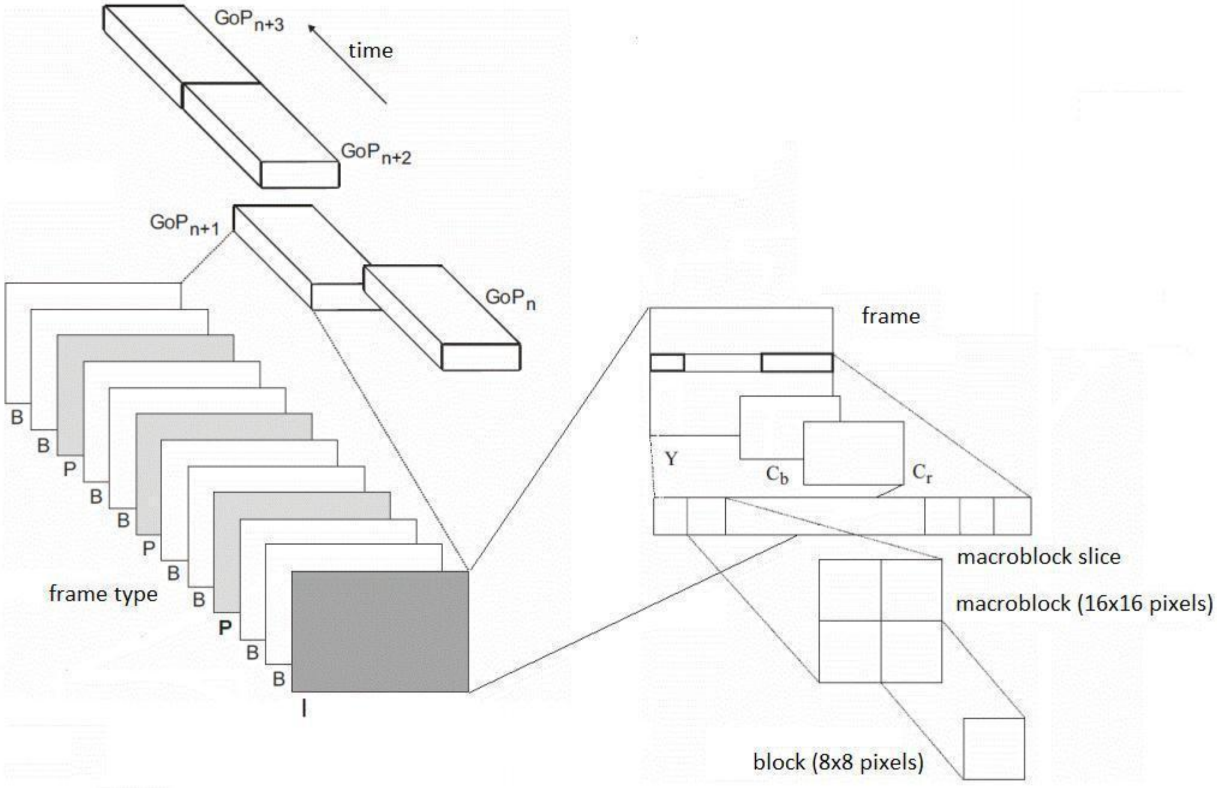


Fig 1.The encapsulation of the GOP into video stream in MPEG-1 standard.

Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT)[4] is used in a wide variety of signal processing applications. 2-D discrete wavelet transform (DWT) decomposes an image or a video frame into sub-images, 3 details and 1 approximation. The approximation sub-image resembles the original on 1/4 the scale of the original. DWT separates the frequency band of an image into a lower resolution approximation sub-band (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components[3]. Embedding the watermark in low frequencies obtained by wavelet decomposition increases the robustness with respect to attacks that have low pass characteristics like filtering, lossy compression and geometric distortions while making the scheme more sensitive to contrast adjustment, gamma correction, and histogram equalization. Since the HVS is less sensitive to high frequencies, embedding the watermark in high frequency sub-bands makes the watermark more imperceptible while embedding in low frequencies makes it more robust against a variety of attacks on the output video given by the dwt program.

6. Development of Software

Introduction to Matlab:

MATLAB® is a high-level language and interactive environment for numerical computation, visualization, and programming. Using MATLAB, you can analyze data, develop algorithms, and create models and applications. The language, tools, and built-in math functions enable you to explore multiple approaches and reach a solution faster than with spreadsheets or traditional programming languages, such as C/C++ or Java™.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems.

Image Processing Toolbox™ provides a comprehensive set of reference-standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. You can perform image enhancement, image deblurring, feature detection, noise reduction, image segmentation, geometric transformations, and image registration. Many toolbox functions are multithreaded to take advantage of multicore and multiprocessor computers.

Image Processing Toolbox supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and tomographic. Visualization functions let you explore an image, examine a region of pixels, adjust the contrast, create contours or histograms, and manipulate regions of interest (ROIs). With toolbox algorithms you can restore degraded images, detect and measure features, analyze shapes and textures, and adjust colorbalance.

Functions Used:

A = **imread**(filename,*fmt*) reads a grayscale or color image from the file specified by the string filename. If the file is not in the current folder, or in a folder on the MATLAB$^{®}$ path, specify the full pathname.

imwrite(A,filename,*fmt*) writes the image A to the file specified by filename in the format specified by *fmt*.

obj = **VideoReader**(filename) constructs obj to read video data from the file named filename. If it cannot construct the object for any reason, VideoReadergenerates an error.

writerObj=**VideoWriter**(filename)constructs
a VideoWriterobject to write video data to an AVI file with Motion JPEG
compression.

[cA,cH,cV,cD] = **dwt2**(X,*'wname'*)computes the approximation coefficients matrix cA and details coefficients matrices cH, cV, and cD(horizontal, vertical, and diagonal, respectively), obtained by wavelet decomposition of the input matrix X. The *'wname'*string contains the wavelet name.

X = **idwt2**(cA,cH,cV,cD,*'wname'*)uses the wavelet *'wname'*to compute the single-level reconstructed approximation coefficients matrix *X*, based on approximation matrix cA and details matrices cH,cV, and cD (horizontal, vertical, and diagonal, respectively.

implay(filename) opens the implaymovie player, displaying the content of the file specified by filename. The file can be an Audio Video Interleaved (AVI) file. implayreads one frame at a time, conserving memory during playback. implaydoes not play audio tracks.

4.1 WATERMARK EMBEDDING ALGORITHM

Input: *Original Video and a random watermark vector **W**. **Output**:* *Watermarked video.*

```
-The video is partitioned into frames.
for each scene do
    1- Metricize the frame into a matrix M.
    2- Apply DWT ( Haar wavelet) to the converted matrix M to obtain 4 sub-band matrices of each frame (LL, LH, HL, HH).
    3- Metricize the watermark into the matrix W as well as the HH sub-band HH.
    4- Choose n random positions having values with in the dimensions of HH sub-band, save the values in vector V .
    5- Embed the watermark W at the corresponding positions of HH depicted in vector V.
    6- For the watermarked image take their Inverse wavelet transform (Haar wavelet).
end for
7- Produce the watermarked video using the frames.
```

4.2-WATERMARK DETECTION ALGORITHM

Input: *Watermarked video.*

Output*: Watermark detected*.

-The video is partitioned into frames.

for each scene **do**

1- Metricize the frame into a matrix **M.**

2- Apply DWT (Haar wavelet) to the converted matrix **M** to obtain 4 sub-band matrices of each frame (**LL**, **LH**, **HL**, **HH**).

3- Generate the n random positions using the same algorithm used while embedding, save the values in vector **V.**

4- Retrieve the watermark values using the position depicted in **V.** Save them to matrix **RW.**

end for

5- Produce the watermark using the matrix **.**

7. Expected Outcome

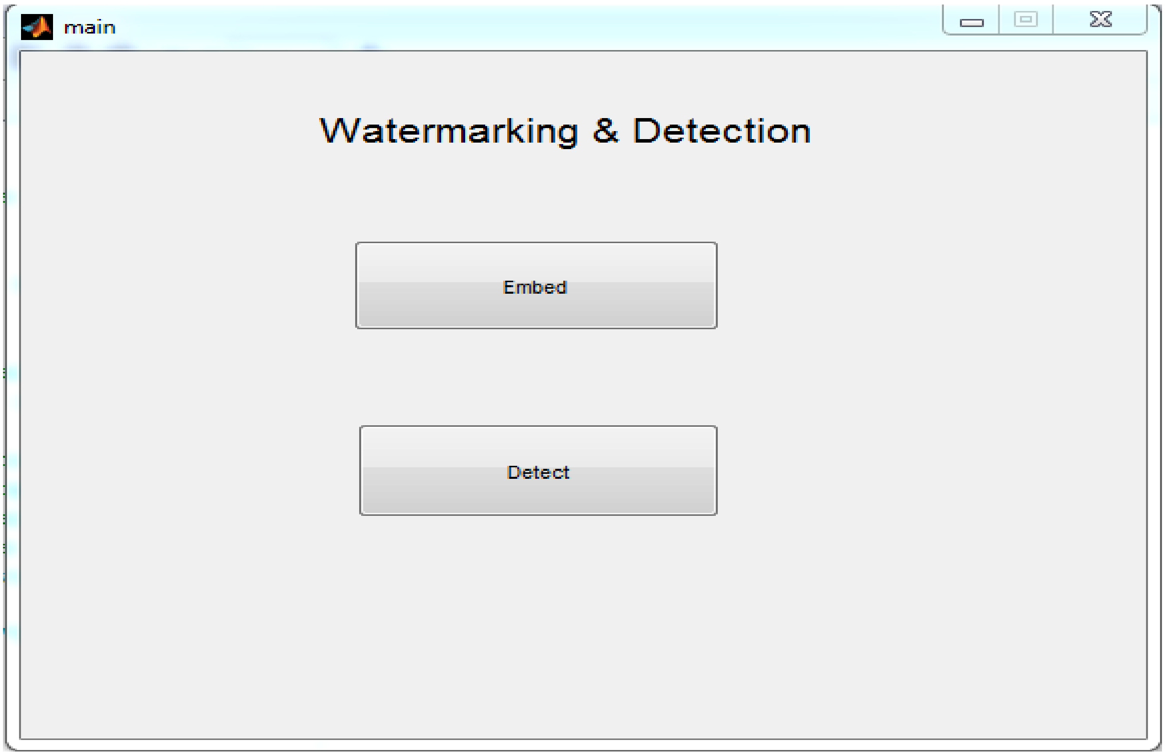


Fig 1.Initial Snapshot of the Program

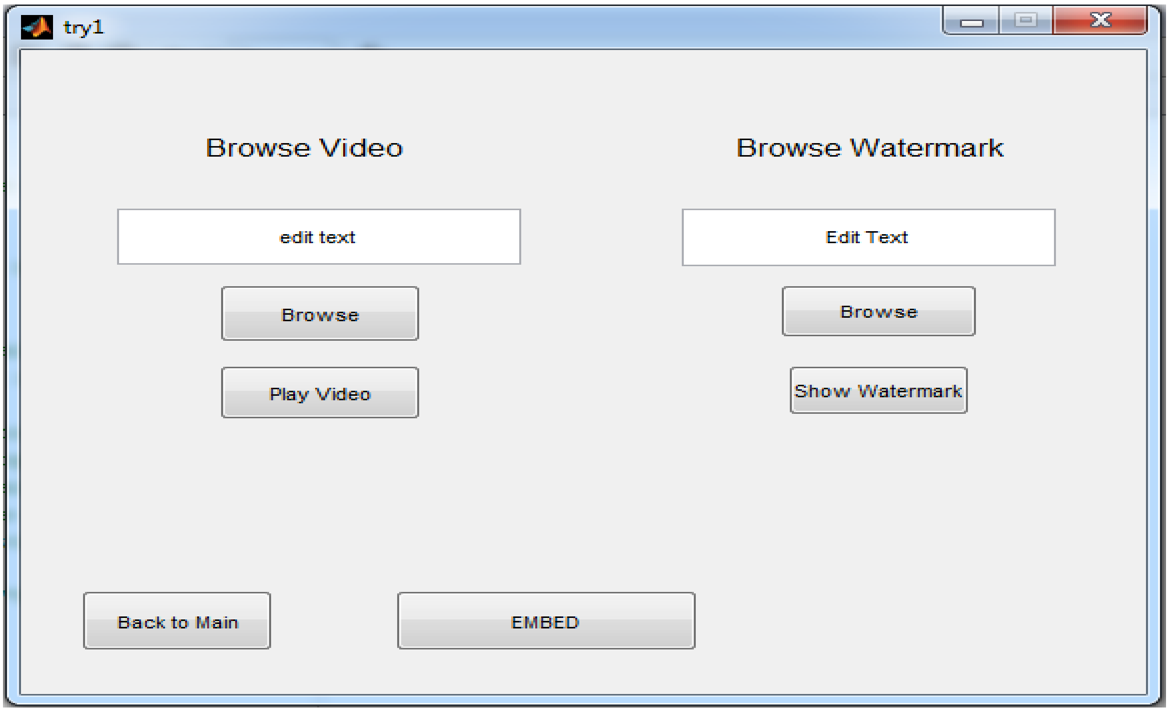
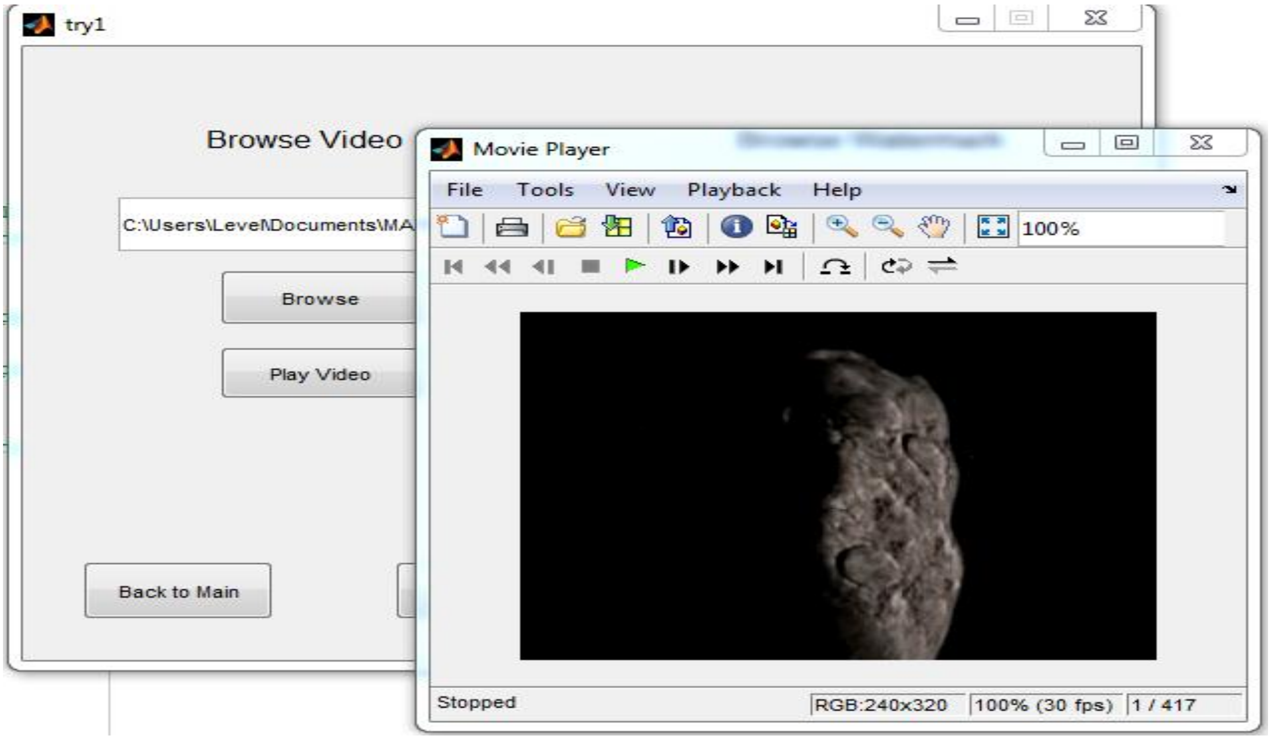


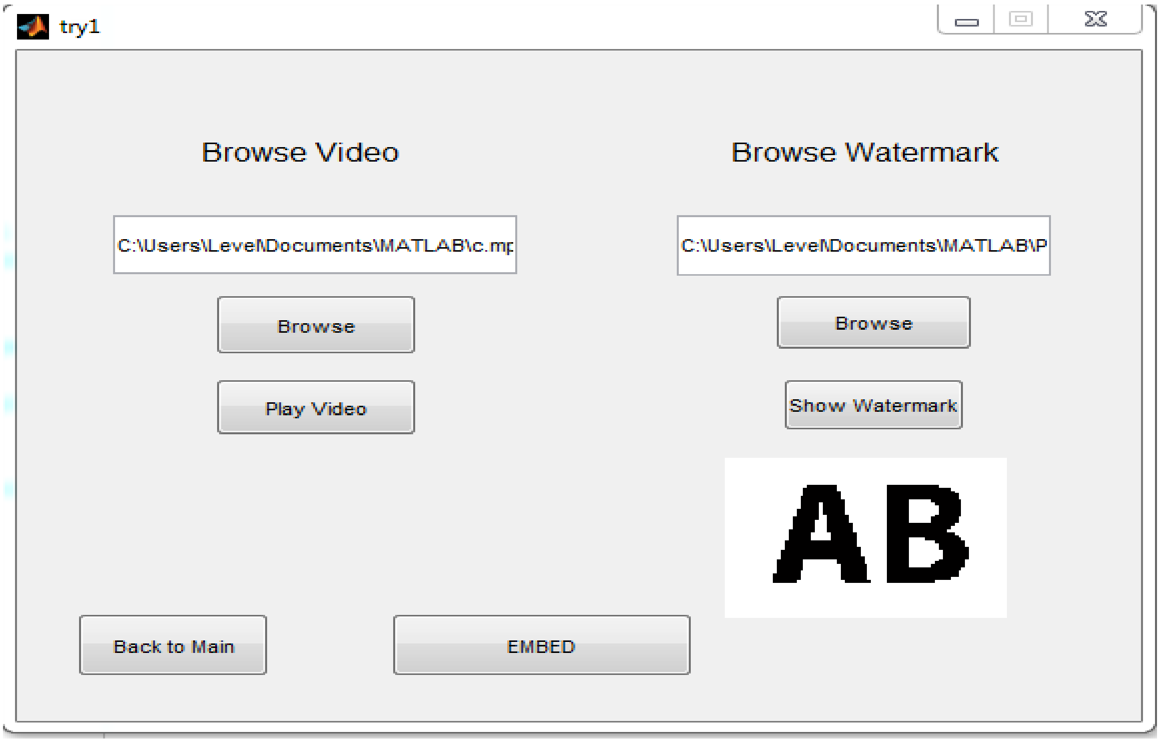
Fig 2.Watermarking Module



C:\Users\Level\Documents\MA

Stopped RGB:240x320 100% (30 fps) 1 / 417

Fig 3.Host Video



C:\Users\Level\Documents\MATLAB\c.mp

C:\Users\Level\Documents\MATLAB\P

Fig 4.Watermark to Embed.

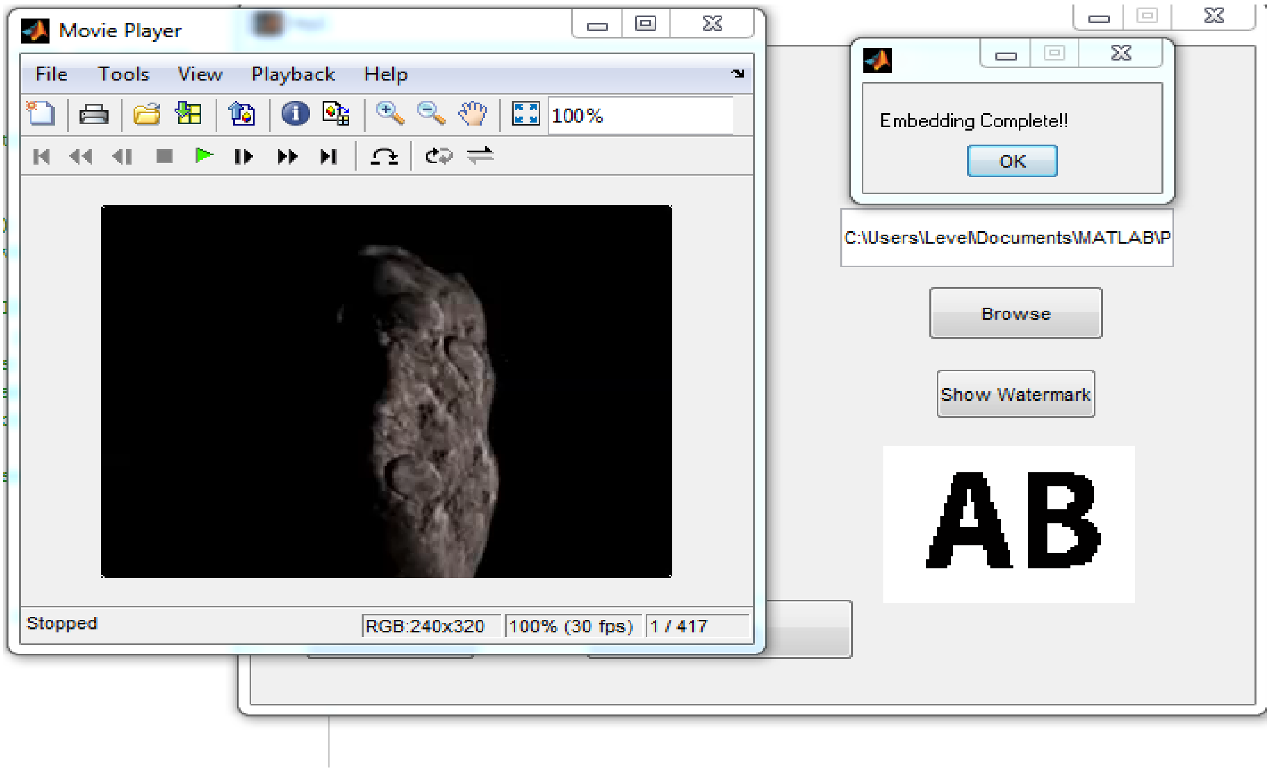


Fig 5.Watermarking Process

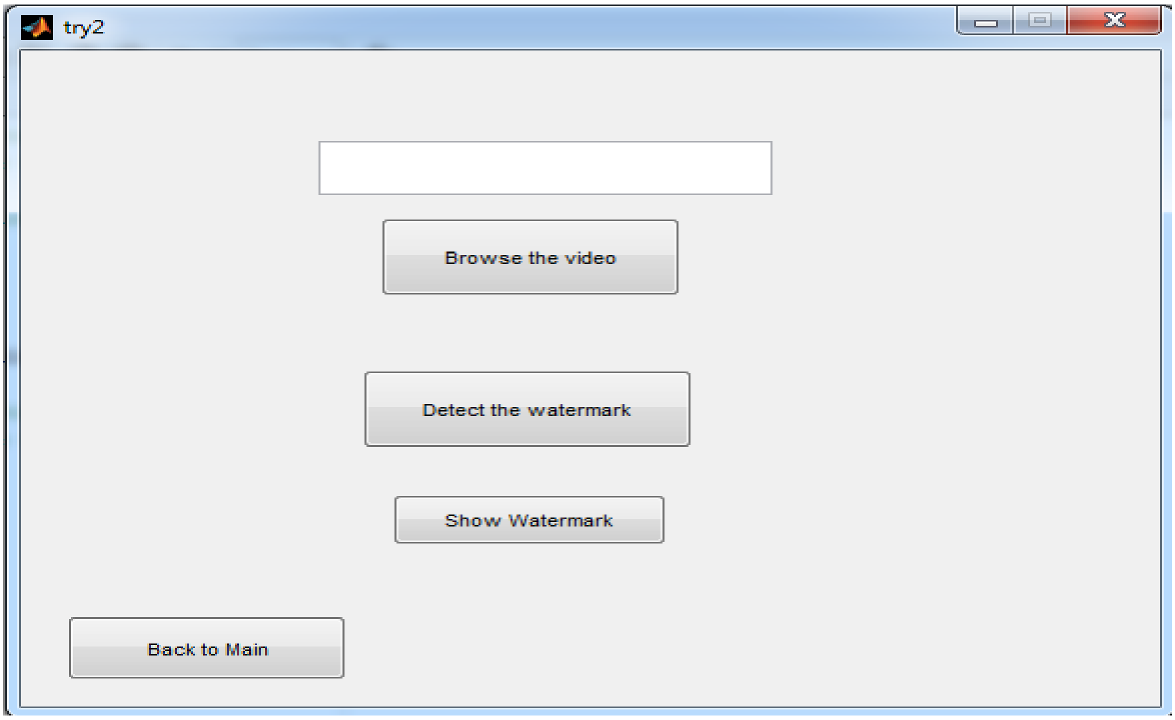
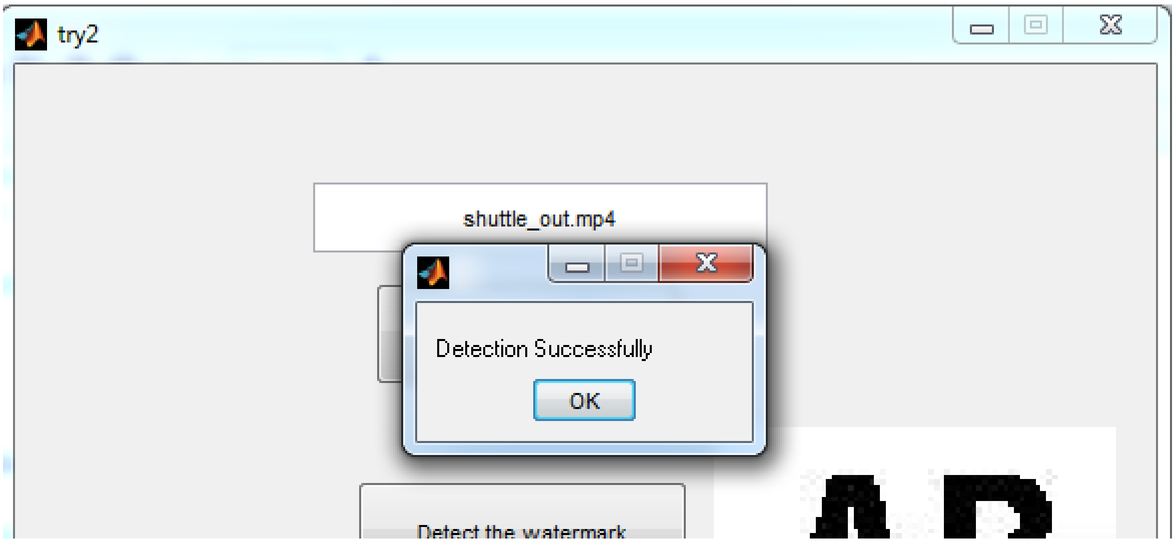


Fig 6.Detection Module



shuttle_out.mp4

Detection Successfully

Fig 7.Detection and the watermark.

Limitations of the watermark size:

Video size	*Size(kb)*	*Frames*	*Watermark size**
320 X 240	549	377	40 X 40
320 X 240	1486	630	50 X 50
300 X 240	3000	1440	75 X 75
400 X 224	3178	2150	90 X 90

8. Work and Time Schedule

S.No	Module	Date
1	Formulation of the Topic	13th-21st Aug
2	Literature survey	22nd -2nd Sept
3	Frames Extraction using Matlab	3rd -12th Sept
4	Embedding of the watermark	13th -25th Sept
5	Creation of the Random Positions	8th -25th Oct
6	Detection of the watermark	25th-31st Oct
7	Calculating Efficiency of code	1st-10th Oct
8	Finalizing the work	10th-15th Oct

Activity time chart

Before Mid-Sem	Date	Before End-Sem	Date
Formulation of the Topic	13th-21st Aug	Creation of the Random Positions	8th -25th Oct
Literature survey	22nd -2nd Sept	Detection of the watermark	25th-31st Oct
Frames Extraction using Matlab	3rd -12th Sept	Calculating Efficiency of code	1st-10th Oct
Embedding of the watermark	13th -25th Sept	Finalizing the work	10th-15th Oct

9. Conclusion and Future work

Proposed work an innovative video watermarking scheme with Watermarking as video. The process of this video watermarking scheme, including watermark preprocessing,, video preprocessing, watermark embedding and original video recovery is described in detail. Simulators are performed to demonstrate that our scheme is robust against various video attacks because of immediate watermark changing on every frame.

Further work is necessary to improve the reliability of watermark systems to protect intellectual property and copyrights. Attacks on watermarks are being considered in current development of watermarking tools. Areas for development include watermark detection, recovery, and authentication. One possible approach for authentication is to apply public-key steganography as introduced in and further explored.

10. Refrences

1] I. E. G. Richardson, H. 264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia. Chichester, U.K.: Wiley, 2003.

[2] M. Noorkami and R. M. Mersereau, “A framework for robust watermarking of H.264-encoded video with controllable detection performance,” IEEE Trans. Inform. Forensics Security, vol. 2, no. 1, pp. 14–23, 2007.

[3] X. Gong and H.-M. Lu, “Towards fast and robust watermarking scheme for H.264 video,” in Proc. 10th IEEE international conference on ISM, pp. 649–653, 2008.

[4] S. Kim, Y. Hong, and C. Won, “Data hiding on H.264/AVC compressed video,” Image Anal. Recog., vol. 4633, pp. 698–707, 2007.

[5] S. Kapotas, E. Varsaki, and A. Skodras, “Data hiding in H. 264 encoded video sequences,” in Proc. IEEE 9th Workshop MMSP, pp.373–376, 2007.

[6] G. Qiu, P. Marziliano, A. Ho, D. He, and Q. Sun, “A hybrid watermarking scheme for H.264/AVC video,” in Proc. 17th IEEE on ICPR, pp.865–868, 2004.

[7] J. Zhang, A. T. S. Ho, and G. Qiu, “Robust video watermarking of H.264/AVC,” IEEE Trans. Circuits Syst. II: Express Briefs, vol. 54, no.2, pp. 205–209,2007.

[8] M. Noorkami and R. Mersereau, “Compressed-domain video watermarking for H.264,” in Proc. IEEE journal on ICIP, vol. 2. pp. 11–14,2010.

[9] C.-V. Nguyen, D. Tay, and G. Deng, “A fast watermarking system for H.264/AVC video,” in Proc. IEEE international conference on APCCAS, pp. 81–84, 2006.

[10] D. Simitopoulos, S. A. Tsaftaris, N. V. Boulgouris, and M. G. Strintzis, “Compressed-domain video watermarking of MPEG streams,” inProc. IEEE Int. Conf. Multimedia and Expo, Lausanne,Switzerland,,vol.1,no.1,pp.569–572,2002.