Secure Data Hiding Technique Using Video Steganography and Watermarking

Shivani Khosla
M.Tech (CSE), Indo Global
College of Engineering, Abhipur,
Mohali- Punjab, India

Paramjeet Kaur
A.P (CSE), Indo Global
College of Engineering, Abhipur,
Mohali- Punjab, India

ABSTRACT
The rapid development of data transfer through internet made it easier to send the data accurate and faster to the destination. Besides this, anyone can modify and misuse the valuable information through hacking at the same time. This paper presents video steganography with digital watermarking techniques as an efficient and robust tool for protection. This paper is a combination of Steganography and watermarking; which provides a strong backbone for its security. Here considers video as set of frames or images and any changes in the output image by hidden data is not visually recognizable. This proposed system not only hides large volume of data within a video; but also limits the perceivable distortion that might occur while processing it.

Keywords
Steganography, Digital watermarking, Least Significant Bit, Discrete Wavelet Transform, Discrete Cosine Transform

1. INTRODUCTION
Data security means to protect a database from destructive forces and the unwanted actions of unauthorized users. Huge amount of confidential information is being exchanged over the Internet (publicly open medium) as this is the most cost-effective and widely available way. This technological progress has also made digital data very much vulnerable to interception and then possible unauthorized access / use and has caused significant economical losses for the content producers and rights holders. To protect data on public channels, the security measures need to be incorporated into data communication systems over the Internet [1]. Steganography is one of the promising technologies helping to achieve the overall goal of secure delivery of information from its source to the authorized end-users. Steganography is the art or practice of concealing a file, image, or message within another a file, image, or message. The word steganography is of Greek origin and means "covered writing" or "concealed writing"[2]. Steganography is changing the digital media in a way that only the sender and the intended recipient is able to detect the message sent through it. On the other side steganalysis is the science of detecting hidden message [3]. The objective of steganalysis is to break steganography system and that condition is met if an algorithm can judge whether a given image contains a secret message. To reduce the possibility of attack, security needs to be kept secret i.e. invisible security. The important data can be inserted into multimedia documents in a way that cannot be spotted i.e., imperceptible (invisible) insertion of information into multimedia data. Digital Watermarking technique is used to improve the imperceptibility (i.e. invisibility) and robustness. Digital watermarking can be used on any digital image, audio file or text file. Digital watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. The signal (also known as a watermark) can be used to identify the owner of the work, to trace illegal copies and to authenticate the content of the work.

Steganography and watermarking differ in a number of ways including purpose, specification and detection/extraction methods. The fundamental difference is that the object of communication in watermarking is the host signal with the embedded data providing copyright protection. In steganography, the object to be transmitted is the embedded message and the cover signal serves as an innocuous disguise chosen fairly arbitrarily by the user based on its technical suitability. In addition, in steganography, the third party cannot detect the message in stego media but in watermarking, the third party cannot remove or replace the message. It mainly prevents the illegal copy. Further, the existence of the watermark is often declared openly and any attempt to remove or invalidate the embedded content renders the host useless. The vitally important requirement for steganography is perpetual and algorithmic undetectability. Robustness against malicious attacks and signal processing is not the primary concern as it is for watermarking.

2. STEGANOGRAPHY
Steganography is changing the digital media in a way that only the sender and the intended recipient is able to detect the message sent through it. The following formula provides a very generic description of the pieces of the steganographic process [4]:

cover_medium + hidden data + stego_key = stego_medium

In this context, the cover_medium is the file in which is used to hide the hidden_data, which may be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium).

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Video and image files especially comply with this requirement that can be used for information hiding. In fig 1, shows the four main categories of file formats that can be used for steganography.

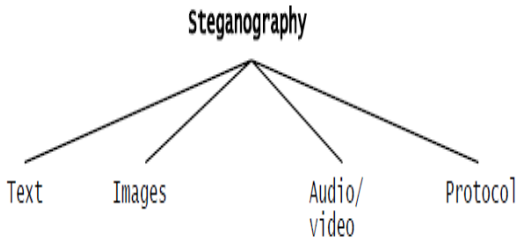

Fig 1: Categories of steganography

In text, hiding information is historically the most important method of steganography. This method was to hide a secret message in every nth letter of every word of a text message. In video steganography, a digital video consists of a set of frames (images) that are played back at certain frame rates based on the video standards. Video steganography hides the message in any one of the frames/images, after hiding, it is very difficult to examine in which the data/message is hidden [5].

3. DIGITAL WATERMARKING

Digital watermarking is the process of inserting a digital signal or pattern (indicative of the owner of the content) into digital content. Watermark can be used later to identify the owner of the work, to trace illegal copies and to authenticate the content, of the work. Watermarks of varying degrees of obtrusiveness are added to presentation media as a guarantee of authenticity, quality, ownership, and source. To be effective in its purpose, a watermark should adhere to a few requirements. In particular, it should be robust and transparent. Robustness means it should be able to survive any alterations or distortions that the watermarked content may undergo, including common signal processing alterations and intentional attacks to remove the watermark and used to make the data more efficient to store and transmit. This is so that afterwards, the owner can still be identified. In transparent, requires a watermark to be imperceptible so that it does not affect the quality of the content and makes detection

4. LEAST SIGNIFICANT BIT

Least significant bit (LSB) insertion is a simple approach for embedding information in a cover image. The least significant bit (i.e. the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. In this 24-bit image, a bit of each of red, green and blue color components can be used, and they are each represented by a byte. In this example, a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

If the number 200, the binary representation is 11001001, is embedded into the least significant bits of this part of the cover image, then resulting grid is:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

So if the number was embedded into the first 8 bytes of the grid, only the three in bold and underlined bits needed to be changed according to the embedded message. On average, only half bits in an image will need to be modified to hide a secret message using the maximum cover size.

5. DISCRETE WAVELET TRANSFORM

DWT is used for digital images. Many DWTs are available. Like to hide text message, integer wavelet transform can be used. The simplest transform is haar transform. DWT is the multi resolution description of an image. DWT splits the signal into high and low frequency parts. The low frequency part is split again into high and low frequency parts, while the high frequency part contains information about the edge components. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges. DWT transform is applied to an image it is decomposed into 4 sub bands: LL, HL, LH and HH. To perform a second level decomposition, again DWT is applied to LL1 which decomposes the LL1 band into the 4 sub bands [6]. Fig 2 shows a second level decomposition.

Haar Transform decomposes each signal into two components, one is called average (approximation) or trend and the other is known as difference (detail) or fluctuation.

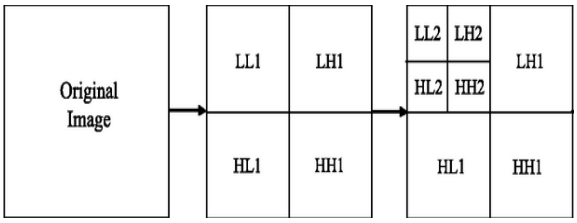

Fig 2: Level 2D – DWT

A precise formula for the values of first average sub signal,$a = a_1, a_2, a_3 \ldots\ldots\ldots a_{N/2}$ at one level for a signal of length N i.e. f = (f1, f2.....fn) is [6]

$$a_n = \frac{f_{2n-1} + f_{2n}}{\sqrt{2}}, n = 1,2,3, \ldots . N/2$$

and the first detail sub signal, $d^1 = d_1, d_2, d_3 \ldots\ldots\ldots d_{N/2}$, at the same level is given as

$$a_n = \frac{f_{2n-1} - f_{2n}}{\sqrt{2}}, n = 1,2,3, \ldots . N/2$$

6. DISCRETE COSINE TRANSFORMATION

DCT has strong robustness and is widely used in digital image watermarking. DCT transforms a time domain signal into its frequency components. Many frequency coefficients are obtained from DCT, such as single direct current DC coefficients, low frequency, mid frequency coefficients, and high frequency coefficients. These middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high Frequency).

Consider a subimage g(x,y) of size n×n whose discrete transform T(u,v), can be expressed in terms of general relation [7],

$$T(u,v) = \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} g(x,y) r(x,y,u,v)$$

$$r(x,y,u,v) = s(x,y,u,v) = \alpha(u)\alpha(v)\cos\left[\frac{(2x+1)u\pi}{2n}\right]\cos\left[\frac{(2x+1)v\pi}{2n}\right]$$

Where

$$\alpha(u)\alpha(v)=\begin{cases}\sqrt{\frac{1}{n}} & for\ u=0\\ \sqrt{\frac{2}{n}} for\ u=1,2,\ldots..,n-1\end{cases}$$

Given T(u,v) , g(x,y) similarly can be obtained using inverse discrete transform

$$g(x,y)=\sum_{x=0}^{n-1}\sum_{y=0}^{n-1}T(u,v)s(x,y,u,v)$$

7. PROBLEM FORMULATION

Many Video Steganography techniques have been proposed earlier but they were not secure enough and can be temporarily tampered with so the task was not fulfilled. Even if the message is encoded before sending the message, this can be decoded by the hacker by making use of certain algorithm. Video Steganography alone could not provide better results as technique used for video steganography with LSB was not good enough. Results of previous PSNR obtained were poor and unsatisfactory. Many problems exist with the already proposed algorithm in the literature. To overcome these problems this thesis work designing a new algorithm for data security.

8. OBJECTIVE FOR STUDY

- To analyze different techniques proposed in literature for data security during message transmission.
- To provide better security and transfer of data from source to destination
- To improve robustness without perceptible distortion.
- To provide a better PSNR and MSE results of proposed algorithm.

9. PROPOSED ALGORITHM FOR DATA SECURITY

In this paper, a new algorithm is proposed for better data security and transferring of data from source to destination. A good approach to video steganography with watermarking should aim at concealing the highest amount of data possible in a cover video while maintaining imperceptibility, that is, an acceptable level of visual quality for the watermarked video.

9.1 Hiding technique for hidden information (Embedding Process)

The embedding process takes a cover video and a secret message as the inputs.

Step 1: First take an original video as cover video. Then convert it into number of frames or images. Then select a particular frame/image; this will act as cover image.

Step 2: Add a password graphically for more security.

Step 3: Load a secret text which embed into the cover image and convert it into binary form.

Step 4: Then apply the LSB technique. The LSB bit of the image pixel is replaced by the binary data. Then get a stego-image.

Step 5: Apply the combined DWT and DCT technique to stego-image. Get the watermarked image.

Step 6: At last, have a watermarked video. This video is ready for the transmission through the internet.

9.2 Recovery technique of hidden information (Extracting Process)

It basically follows the reverse process of the hiding algorithm to obtain the secret message.

Steps to recover the hidden information:

Step 1: Load the watermarked video.

Step 2: Enter the password to get the secret message.

Step 3: Apply the inverse DWT and inverse DCT technique to get the stego image.

Step 4: Apply the LSB technique on the stego image.

Step 5: Get the secret message and original video.

Step 6: Finally, we analyze the result on the basis of PSNR, MSE and histogram.

10. RESULT AND DISCUSSION

In previous work, Sunil K. Moon et. al (2013) [8] used cryptography and steganography. In proposed algorithm, steganography with watermarking are used which provides more security than in previous work. In this, results of all the intermediate steps of the proposed methods are highlighted. Implementation is done on MATLAB Experimental results of intermediate steps show the efficiency of the proposed approach. Results includes following steps:

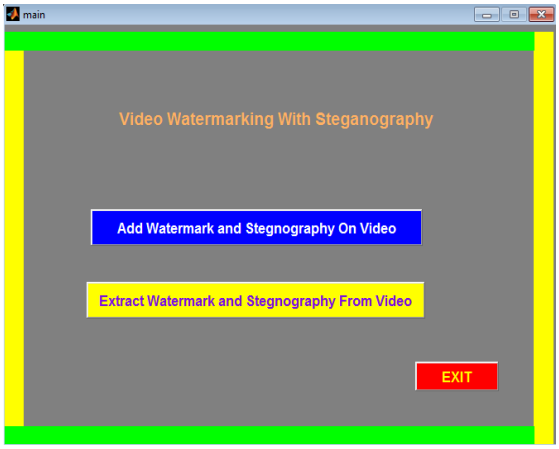

Fig 3: Opening GUI

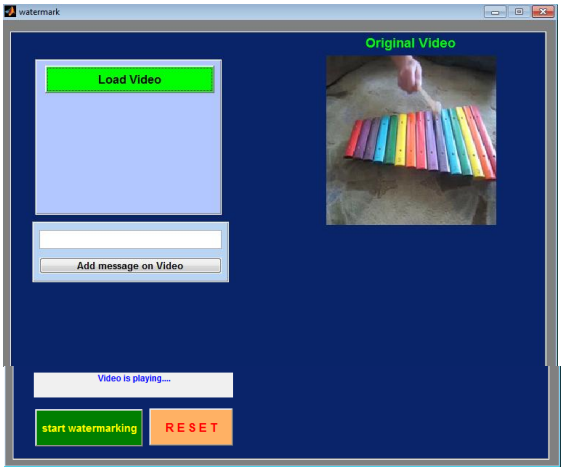

Fig 4: Input Video is loaded

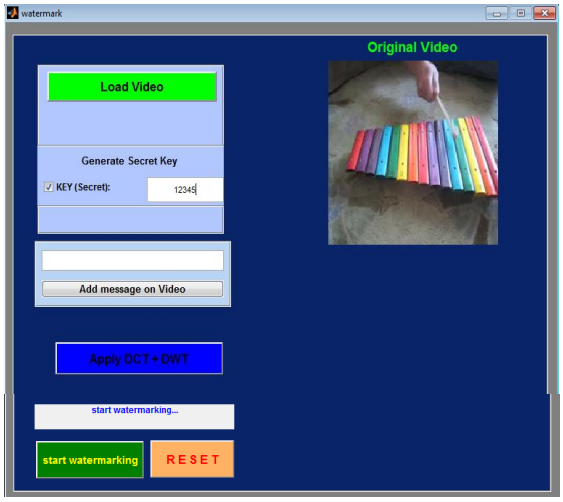

Fig 5: Password is added

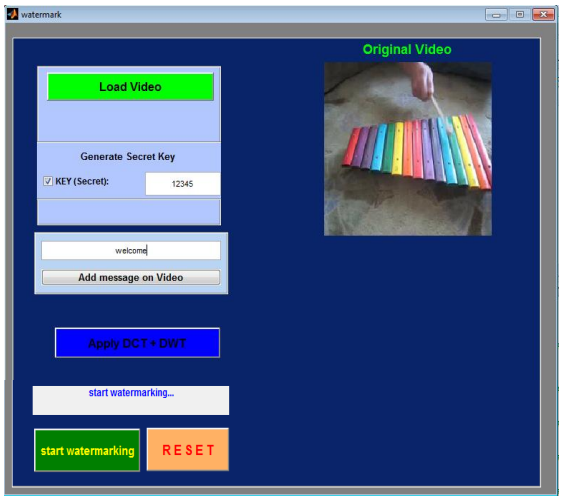

Fig 6: Secret message is added

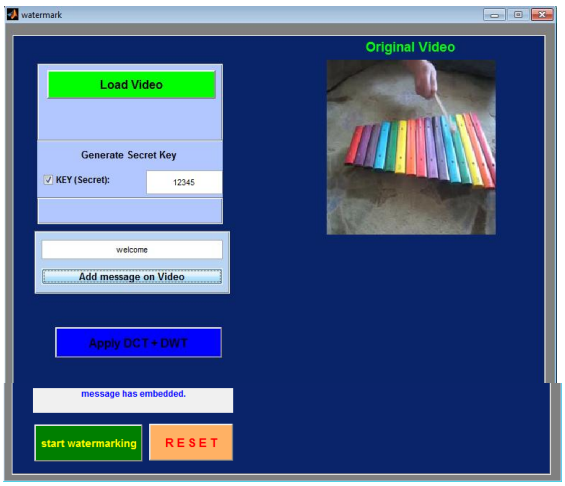

Fig 7: Steganography is applied

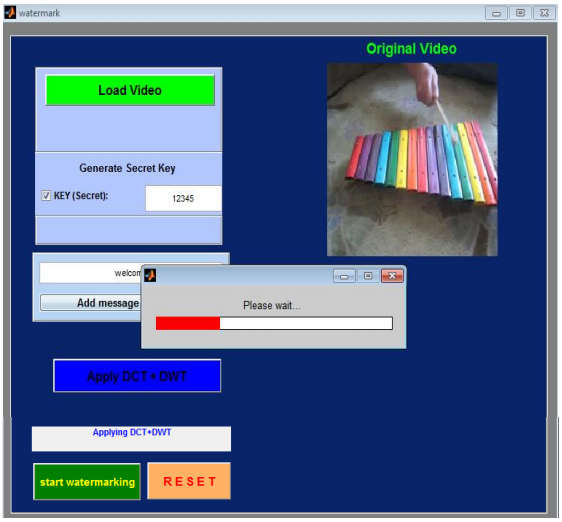

Fig 8: Applying DCT +DWT

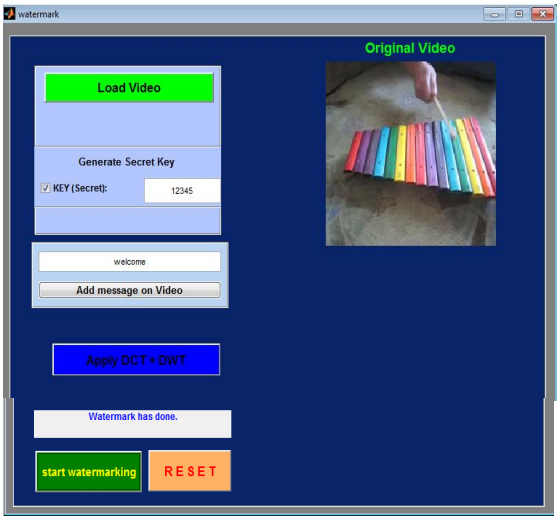

Figure 9: Watermarking is applied

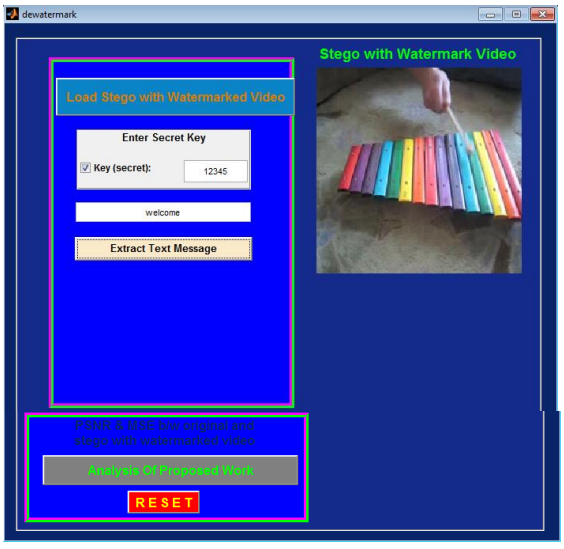

Fig 10: Decoder Side, Message is extracted

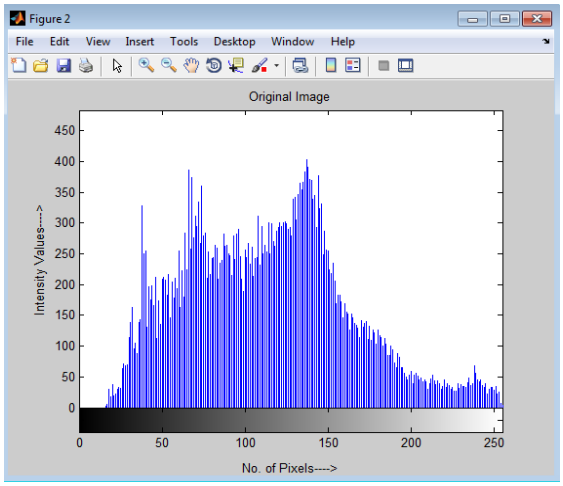

Fig 11: Histogram of Original image/Frame

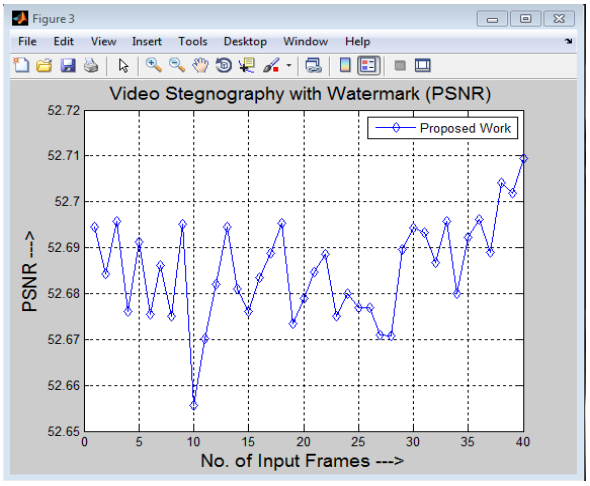

Fig 14: Graph of PSNR values for proposed work

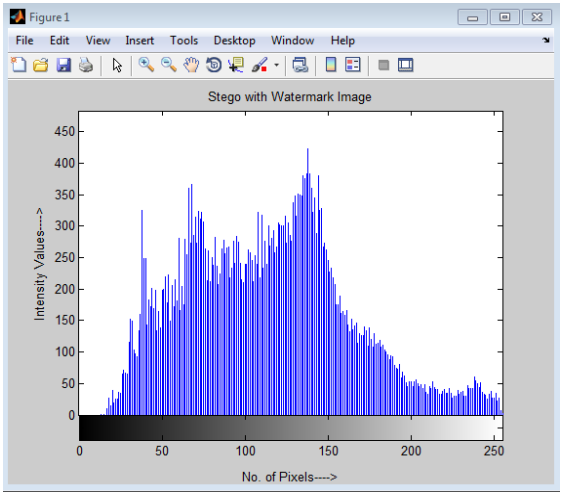

Fig 12: Histogram of watermarked image/Frame

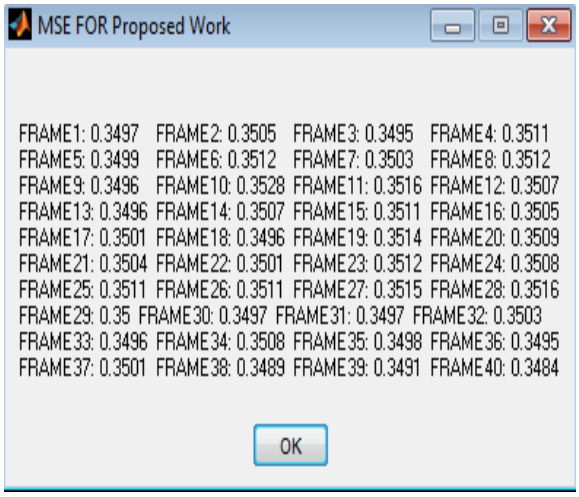

Fig 15: MSE for Proposed work

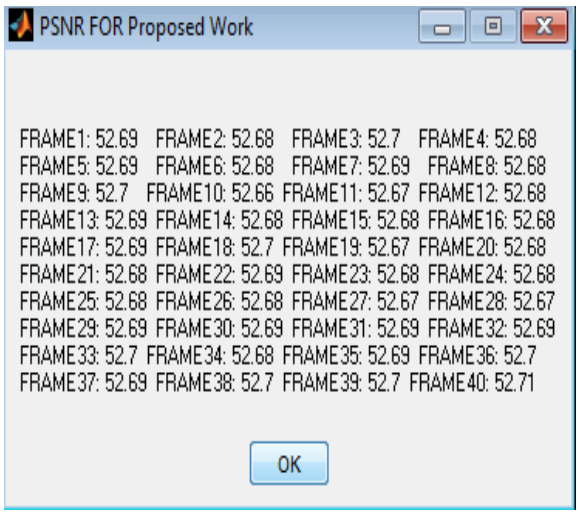

Fig 13: PSNR for Proposed work

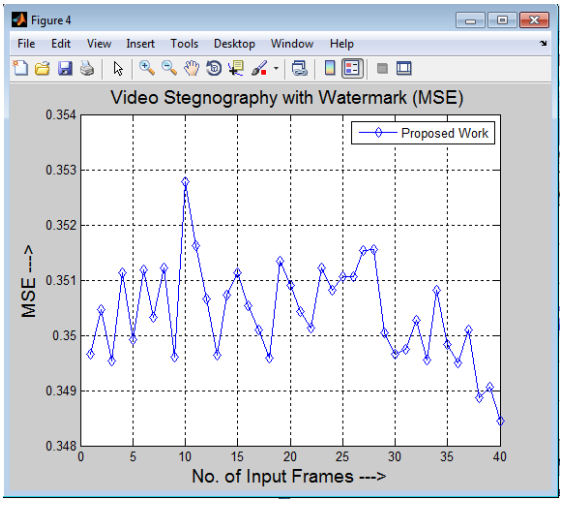

Fig 16: Graph of MSE values for proposed work

11. CONCLUSION AND FUTURE SCOPE

In this thesis we have presented a new system for the combination of Steganography with watermarking which could be proven as a highly secured method for data communication in near future. The proposed High secured system using steganography and watermarking is tested by taking message and hiding them in images/frames of input video. The results that are obtained from these experiments are recorded. The Proposed algorithm provides more security in comparison to previous algorithm proposed by Sunil. K. Moon et. al.(2013). Future Work may be further enhancement of results by applying some other algorithm than used in this thesis. We can also take two videos as input and can embed secret message in both. Other quality metrics can be used to judge the performance of the algorithm.

12. REFERENCES

[1] Muhammad Abdul Qadir, Ishtiaq Ahmad (2005) "digital text watermarking: secure content delivery and data hiding in digital documents "IEEE.

[2] Jayeeta Majumder, Sweta Mangal (2012) "An Overview of Image Steganography using LSB Technique "IJCA.

[3] Vladimír BÁNOCI, Gabriel BUGÁR, Dušan LEVICKÝ (2011) "A Novel Method of Image Steganography in DWT Domain" IEEE.

[4] Arvind kumar, km. Pooja (2010) "Steganography – A Data Hiding Technique" IJCA volume 9, issue 7.

[5] Hamdy M. Kelash , Osama F. Abdel Wahab ,Osama A. Elshakankiry ,Hala S. El-sayed (2013) "Hiding Data in Video Sequences Using Steganography Algorithms" IEEE.

[6] Nikita Kashyap, G. R. Sinha (2012) "Image Watermarking Using 3-Level Discrete Wavelet Transform (Dwt)" IJMECS.

[7] Blossom Kaur,Amandeep Kaur2, Jasdeep Singh (2011) "*steganographic approach for hiding image in dct domain*" IJAET, Vol. 1,Issue 3.

[8] Sunil. K. Moon , Rajeshree. D. Raut (2013) "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security" IEEE

[9] Anuj Bhardwaj and Rashid Ali (2009) "Image Compression Using Modified Fast Haar Wavelet Transform" World Applied Sciences Journal 7 (5).

[10] Rini T Paul (2011) "Review of Robust Video Watermarking Techniques" IJCA.

[11] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain (2011) "A New Approach for LSB Based Image Steganography using Secret Key" IEEE.

[12] Masoud Nosrati Ronak Karimi Mehdi Hariri (2012) "Audio Steganography: A Survey on Recent Approaches" World Applied Programming, Vol (2), No (3).

[13] Munesh Chandra", Shikha Pandel, Rama Chaudhar (2010) "Digital Watermarking Technique for Protecting Digital Images" IEEE.

[14] Reena Anju and Vandana (2013) "Modified Algorithm for Digital Image Watermarking Using Combined DCT and DWT" IJICT Volume 3 number 7.

[15] Usha Pal , Dinesh Chandra (2012) "Survey Of Digital Watermarking Using Dct" IJCSE Volume 4.