



## MATLAB Implementation of Invisible Watermarking using LSB and Lifting Wavelet Transform Technique

S. SIVASANKARI<sup>1</sup>, S. R. SOPHIYA<sup>2</sup>

<sup>1</sup>Research Scholar, Arasu Engineering College, Kumbakonam, India, E-mail: Sivasankari2324@gmail.com.

<sup>2</sup>Asst Prof, Arasu Engineering College, Kumbakonam, India, E-mail: Prasop\_284@yahoo.co.in.

**Abstract:** Watermarking is a technique of embedding hidden information such as image into the cover video. The watermarking embedding is done by discrete wavelet transform based frequency domain. To get high performance, the proposed system architecture employs pipeline structure. Invisible digital watermarking process using discrete wavelet transform (DWT). Hiding of the image in an image of a video is done by using least significant bit algorithm. Mat lab has been done to increase the overall performance evaluation on video authentication. This result in minimum degradation of video quality and increase the speed, decrease the cost and power. And better resolution of PSNR and MSE Values.

**Keywords:** Watermarking, Least-Significant-Bit(LSB), Pixel-Value Differencing (PVD), Security, DWT.

### I. INTRODUCTION

The advance in electronic and information Knowledge, together with the hasty growth of techniques for vast digital signal and multimedia processing, has made the distribution of video data much easier and faster [1,2,3]. Digital watermarking is the route of embed information called a watermark into a Multimedia object such that watermark can be detected whenever necessary for DRM. The digital watermarking system essentially consists of a watermark embedder and a Watermark detector [4, 5]. The embedder inserts a watermark onto the host object and the detector detects the occurrence of the watermark. The goal is to develop low power, real time, trustworthy and safe watermarking systems. [6, 7] Digital data (image, audio, and video) is sent throughout World Wide Web (www) devoid of much stab and money. But protection is the main issue in digital multimedia. In the visage of these vivid changes, the activity industry has twisted to assume a slide of technology that permit it to hold the rights controls provided by the law and harness the new world to raise the industry size and develop the user experience. In recent years, the research community has seen much activity in the area of digital watermarking as an additional tool in protecting digital content and many tremendous papers have appeared over the years (Arun Kejariwal, 2003). Digital watermarking attempts to copyright the digital data that is freely available on the World Wide Web to protect the owner's rights [8].

### II. DATA HIDING TECHNIQUES

**Cryptography:** This scrambles a communication into a signs to unclear its meaning. Scrambling of message is done

with aid of secret key. Scrambling message called as encrypted and it is again decrypted with that secret key only. Cryptography provides safe maintenance to message.

**Steganography:** In this sender would cover the message in a horde file. The hordes file or cover message, is the file that anybody can see. When people use this method, they often hide the true intent for communicating in a more common place communication circumstances.

**Digital Watermarking:** This is the direct embedding of other information into the original content or host signal. Ideally, there should be no visible difference between the watermarked and original signal and the watermark should be difficult to eliminate or modify without harmful the host signal [8].

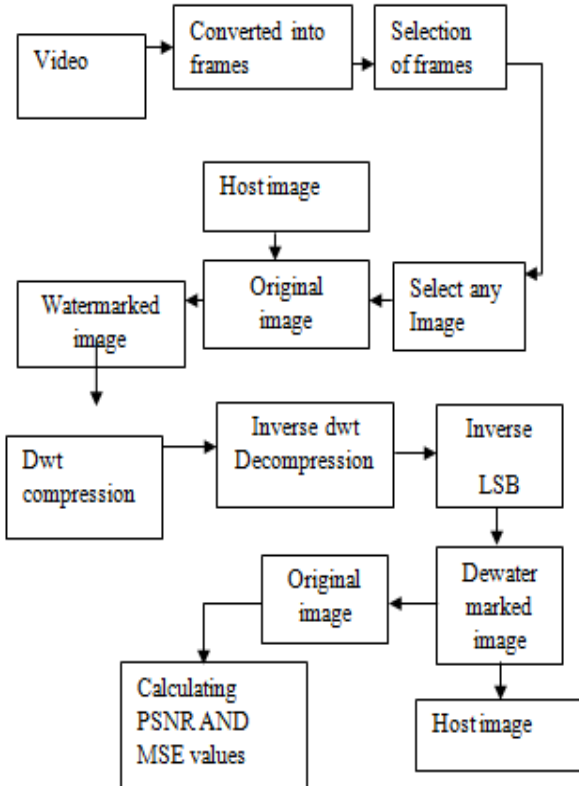
### III. RELATED WORK ON WATERMARKING SYSTEMS

The robustness of the WM can be branded into three core divisions: fragile, semi fragile, and robust. A watermark is called fragile if it fails to be measurable after the least modification. A watermark is known as robust if it resists an elected class of transformations. A semi fragile watermark is the one that is able to hold out definite valid modifications, but cannot stand firm wicked transformations [9, 10]. Frequency-domain WM methods are more robust than the spatial-domain techniques [11]. Later on Roy et al. reported the mean and performance of hardware based imperceptible and semi-fragile video recorder watermarking arrangement for video certification in [12]-[13], where non-pattern MJPEG and status-of-the-skill MPEG-4 indoctrination method be elected respectively. In [14] Roy et al. reported

the hardware based watermarking solutions for 18 CMOS based figure sensors starting beginning the JPEG based watermarking devise, through an MJPEG one, the watermarking result for the regularly used MPEG encoded video was also reported there. In all these works, we concentrated on the hardware operation of an unseen semi-fragile watermarking arrangement for confirmation of scrutiny camera footage.

**IV. PROPOSED SYSTEM**

**A. Block Diagram**



**Fig 1: Hardware Implementation Block Diagram.**

This paper proposed LSB Information hiding algorithm which can lift wavelet convert image. The proposal after the LSB algorithm is to insert the bits of the buried meaning into the least significant bits of the pixels. Achieving the purpose of information hiding with the underground bits of information to swap the chance sound, using the least plane embedding secret information to avoid noise and attacks, making use of job loss to enhance the sound embedded in the way environment to be addressed. DCT and DWT are the most accepted techniques for image compression. Mutually techniques are frequency based techniques, not spatial based. Both techniques have its' own advantages and disadvantage. Like DWT gives improved compression ratio without losing added information of figure but it want more processing authority. While in DCT need low Down processing power but it has blocks artifacts means loss of

some information. Our main purpose is to analyze both techniques and comparing its marks [15]. We conclude that in DWT information loss is less than information loss in DCT. So quality wise the DWT technique is better than DCT technique, but in performance time wise DCT is better than DWT technique. The above diagram shows the block diagram of proposed system.

**V. LEAST SIGNIFICANT BIT (LSB) SUBSTITUTION**

As shown in the figure 2 in LSB algorithm the messages are encoded in the least significant bit of every byte in an image. By doing so, the value of each pixel is changed slightly, but not enough to make significant visual changes to the image, even when compared to the original.

**Cover image**

25	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

Secret data= "A"

0	0	1	0	0	0	1
---	---	---	---	---	---	---

25→00011001

26→00011010

**Watermarked image**

24	26	27	28	29
35	31	32	33	34
42	43	44	45	46
49	50	51	52	53
54	55	56	57	58

-Compare 0 from secret data and 1 from pixel value(25)

-After watermarking the pixel value may be changed to 24 or it remains as such.

-This LSB can store one bit in each pixel

**Fig 2: LSB Algorithm.**

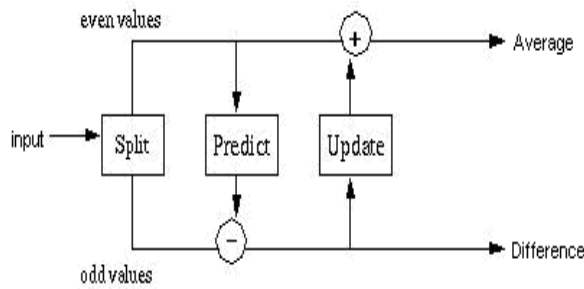
**VI. LIFTING SCHEME**

The lifting scheme (see fig 3) is a well known method for constructing bi-orthogonal wavelets [16]. The main difference with the classical construction is that it does not rely on the Fourier transform. This way, lifting scheme can be used to construct second generation wavelets, wavelets which are not necessarily translates and dilates of one function. The lifting scheme can be used in situations where no Fourier transform is available. Thus the Fourier transform can thus no longer be used as the construction tool. The lifting scheme provides an alternative. It is composed of three basic operations:

- **Split:** where the signal is split into even and odd.
- **Predict:** Even samples are multiplied by a predict factor.
- **Update:** The detailed coefficients computed by the predict step are multiplied by the update factors and

# MATLAB Implementation of Invisible Watermarking Using LSB and Lifting Wavelet Transform Technique

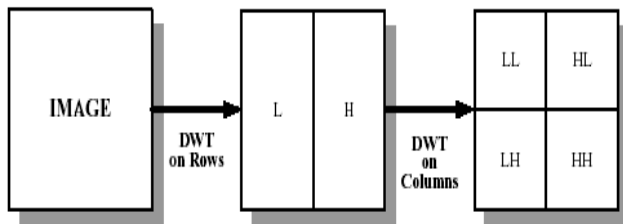
then the results are added to the even samples to get the coarse coefficients.



**Fig 3: Lifting Scheme Process Flow.**

## A. 1D Discrete Wavelet Transform

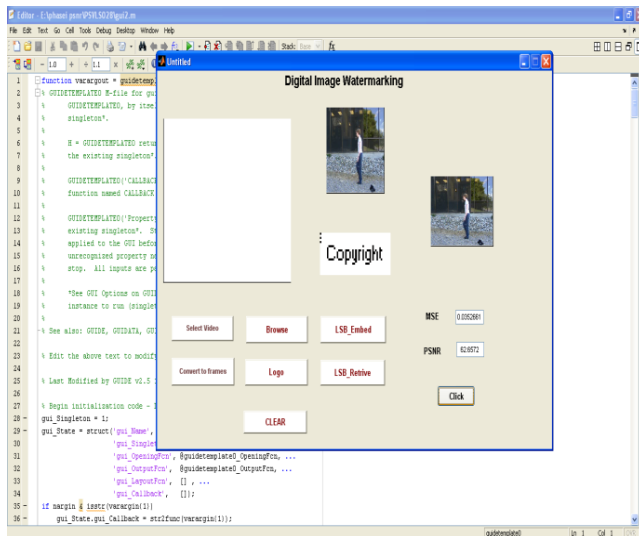
The splitting of image is done by using dwt lifting scheme. An image of 512\*512 get transferred into 256\*512 by using low and high pass filters on rows and again 256\*256 on columns . The following figure 4 shows the DWT transform.



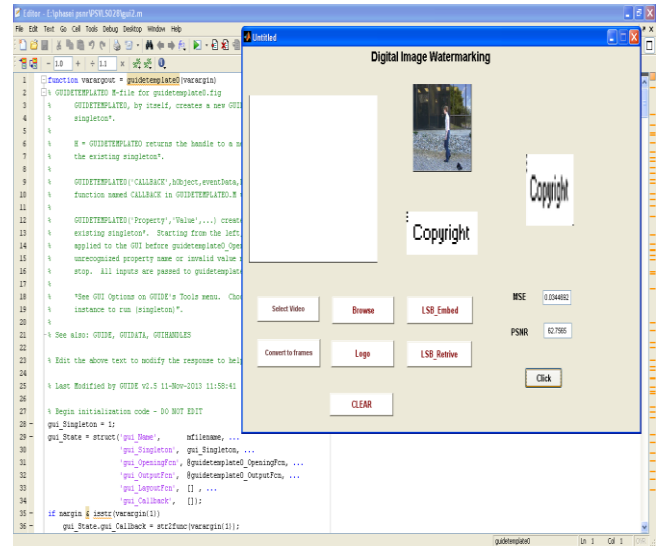
**Fig 4: DWT Transform.**

## VII. SIMULATION AND RESULT

Both the figures 5 and 6 depict the simulation results of the proposed system for embedded image and retrieving image.



**Fig 5: Embedded Image.**



**Fig 6: Retrieve Image.**

## VIII. CONCLUSION

In this paper we have presented a new method of adaptive watermarking with higher embedding capacity. The embedding capacity of the approach is controlled through the filter cut-off frequency. The approach was analyzed and shown to have a very high confidentiality due to the sharpness of information recovery with the cut-off frequency. And the PSNR and MSE value of 62.6572 and .0352661.

## IX. REFERENCES

- [1] V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," in Proc. IEEE Int. Conf. Ind. Informatics, Aug. 2005, pp. 709–716.
- [2] A. D. Gwenaél and J. L. Dugelay, "A guide tour of video watermarking," Signal Process. Image Commun., vol. 18, no. 4, pp. 263–282, Apr. 2003.
- [3] A. Piva, F. Bartolini, and M. Barni, "Managing copyright in open networks," IEEE Trans. Internet Comput., vol. 6, no. 3, pp. 18–26, May–Jun. 2002.
- [4] Memon, N., Wong, P.W.: Protecting Digital Media Content. Communications of the ACM **41** (1998) 35–43.
- [5] Mohanty, S.P.: Digital Watermarking of Images. Master's thesis, Department of Electrical Engineering, Indian Institute of Science, Bangalore, India (1999).
- [6] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G.: Information Hiding – A Survey. Proceedings of the IEEE **87** (1999) 1062–1078.
- [7] Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J., Su, J.: Attacks on Digital Watermarks: Classification,

- Estimation-based Attacks and Benchmarks. IEEE Communications Magazine **39** (2001) 118–126.
- [8] Real Time Implementation of Digital Watermarking Algorithm for Image and Video Application. Amit Joshi<sup>1</sup>, Vivekanand Mishra<sup>1</sup> and R. M. Patrikar<sup>2</sup> <sup>1</sup>Sardar Vallabhbhai National Institute of Technology Surat <sup>2</sup>Visvesvaraya National Institute of Technology Nagpur India.
- [9] (2012, Jul. 28) [Online]. Available: <http://en.wikipedia.org/wiki/Digital-watermarking>.
- [10] S. Saha, D. Bhattacharyya, and S. K. Bandyopadhyay, "Security on fragile and semifragile watermarks authentication," Int. J. Comput. Applicat., vol. 3, no. 4, pp. 23–27, Jun. 2010.
- [11] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
- [12] S. D. Roy, X. Li, Y. Shoshan, A. Fish and O. Yadid-Pecht, "Hardware Implementation of a Digital Watermarking System for Video Authentication", IEEE Transactions of Circuits and Systems for Video Technology, vol. PP, no. 99, pp. 1, 2012.
- [13] S. D. Roy and O. Yadid-Pecht "Low Power and Low Hardware MPEG-4 Video Watermarking System for CMOS Image Sensor Based Surveillance Cameras", in IEEE Sensors Journal. (Revised version submitted, 2012).
- [14] S. D. Roy and O. Yadid-Pecht, "Design and implementation of hardware based watermarking solutions for CMOS image sensors," in New Circuits and Systems Conference (NEWCAS), 2012 IEEE 10th International, 2012, pp. 341-344.
- [15] Comparative Analysis between DCT & DWT Techniques of Image Compression.
- [16] Anilkumar Katharotiya<sup>1\*</sup> Swati Patel<sup>1</sup> Mahesh Goyani<sup>1</sup> <sup>1</sup>. Department of Computer Engineering, LDCE, GTU, Ahmedabad, Gujarat, India. E-mail of the corresponding author: anil\_katharotiya2000@yahoo.com.
- [17] [www.iiste.org](http://www.iiste.org) ISSN 2224-5758 (print) ISSN 2224-896X (online) Vol 1, No.2, 2011.
- [18] Mrs.Mugdha M. Dewasthale, Mrs.P.Mukherji, "FPGA implementation of Wavelet Transform based on Lifting Scheme" in IEEE Conference on Information Management