ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Image Data Authentication using Watermarking Scheme by DWT based Data Embedding Approach

Ankita Pareek[1], Dr. Poonam Sinha[2]

PG Student [DC], Dept. of ECE, UIT, Barkatullah University, Bhopal, Madhya Pradesh, India[1]

Professor & Head ,Dept. of ECE, UIT, Barkatullah University, Bhopal, Madhya Pradesh, India[2]

ABSTRACT:In present world of electronic digital media the demand of high speed communication devices is increasing day-by-day. The security and authenticity of the information on internet is one of the most important issues of research. This paper presents a short review of Digital Watermarking and a Discrete Wavelet Transformation (DWT) based watermarking algorithm implementation using MATLAB programming. The effects of watermarking on digital image data are simulated and analysed in the present paper.

KEYWORDS: Digital Watermarking, Image Segmentation, Key-Encoding, DWT, MATLAB.

I.INTRODUCTION

Due to increasing applications of computer networking and internet, there is a need for securing the digital information from the effects of noise and also from unauthorized user interference. The digitalization of the data is helping the technology user to be able to handle more data with the help of computers and other electronic devices. The data that is available on internet is thus increasing the chance of being affected by the unauthorized means. So a need of securing the data authentication is emerging as very important requirement by the technology users. Especially the data that is intellectual property right of an individual or a body needs to be protected from others. Many technological researches have already been published to protect the data. Digital Signature, Cryptography, Encryption of data, Finger-Printing, Digital Watermarking, and some other techniques are very frequently used by the communication systems to fulfill the user requirement. There are various approaches that are used for securing data. The most effective methods among these are Encryption, Steganography and Watermarking. Steganography is similar to Watermarking. Comparative among the two, watermarking has more than one feature that led it to be better than Steganography. Watermarking has an additional advantage of data authentication that makes it useful at a much larger scale than Steganography. Watermarking can be defined as the practice of imperceptibly altering a Work to embed a message about that Work. Steganography can be defined as the practice of undetectable altering a Work to embed a secret message. In case of encryption the data is transformed into a secret code with the purpose of protecting the secrecy of the data. This protects the secrecy of the data when sent through an insecure channel; whereas in watermarking a media is embedded with data for the purpose of authentication and protection. Digital Watermarking is among the most effective among the existing techniques. In Digital Watermarking, the actual or original data is embedded with information to protect data from unauthorized copy and use. It is one of the most effective copyright protection methods in digital image processing.

The arrival of mobile communication gadgets and high-data communication requirement is replacing the conventional mode of information sharing. Books, personal meetings, media of entertainment, etc. can be obtained and managed using digital systems. The use of all these digital data has got wings with the high-end technological developments in hardware processing. But this increase in digital data has opened the need of technological advancements in the field of data security. Data security using Digital Watermarking is a frontier research area. The model of a watermarking system has two main operational blocks: the first one is the watermark embedder and the second one is the watermark detector. The watermark embedder block adds a watermark to the actual data. Thus the data gets encoded using a watermark that can be extracted by the watermark detector block using appropriate algorithm implementation. Thus,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

the watermarking technology helps to protect the digital data from malicious users and to identify whether the original data is being affected by noise. Watermarking focuses on the security of intellectual property right and authentication of data present in digital media. The main application of the watermarking is identified with the increasing worldwide use of internet. In the world of internet all the data is in the form of multimedia.

A simple watermarking based communication model is shown in Fig 1. In this simple elaboration the input message or data is encoded using a watermark and a key. This is then added to the original data for transmission through the communication channel. While transmission the channel signals gets added to the transmitted signals as noise. The receiver uses a watermark detector to decode the original message from the noisy watermarked data using the key. With the widespread use of internet based applications in around 1990, the concept of Image Watermarking got an importance in the transfer of digital information. The initial implementation of watermarking based data transfer involved insertion of invisible watermark message into image information such that the invisible message will survive in case of intended or unintended attacks. This concept leads to the development of a number of schemes that can recover the watermark data from the cover image data.

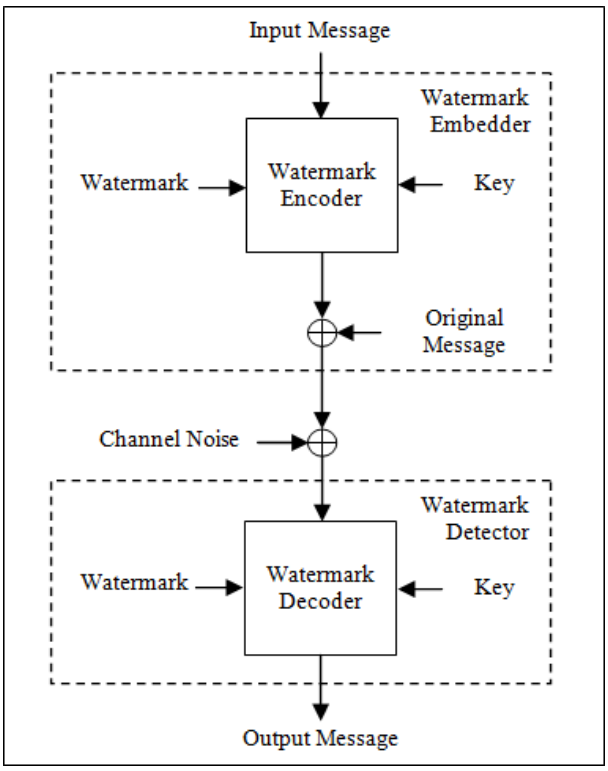


Fig. 1 Simple model of Watermarking of Digital Message

II. LITERATUREREVIEW

A number of researchers and scholars proposed digital data watermarking techniques. A forward-based image embedding scheme is proposed in [1]. In this paper the performance evaluation of the watermarking technique is based on imperceptibility, execution time and robustness against common signal processing operations using the proposed scheme in wavelet domain. Another discrete wavelet transform based multi-resolution decomposition algorithm is proposed in [2]. In this paper three level wavelet decomposition is employed and watermarking is embedded into the high-frequency coefficients of the wavelet image. This paper shows satisfactory simulation of the proposed algorithm for robustness and visual effects. Reference [3] presents a review to Digital watermarking and proposes a novel watermark positioning approach that uses the statistical characteristics of the pixels to locate the watermark into

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

brightness values of the pixels using image segmentation. Approach described in this paper in spatial domain provides robustness, invisibility, data capacity, security and provides the strong protection against theft of images over the network. A simple MATLAB based algorithm is implemented in [4,5] to watermark a digital image for copyright protection. The proposed schemes can be used to watermark images without distorting the vital regions that are of interest to the user. Discrete Wavelet Transform based various schemes are proposed in [6,7,8,9,10] for the copyright protection of digital image. These schemes are robust and effective implementations for image authentication.

An algorithm of DWT and Hankel Transform is combined in [11] to develop to integrate the authentication of color image contents through embedding watermark. In this proposed scheme, a new watermark image is generated by performing XOR between original binary watermark and the image and the brightness component is then decomposed into three discrete wavelets. The watermarking image is scrambled with Hankel Transform before embedding to make it more difficult that the attackers extract the watermark. Invisible watermarking based image authentication algorithm is implemented in [12] and [13]. IN [13] a secret key is used to embed and extract watermark. A robust hybrid watermarking scheme or gray scale digital images using block processing method is developed and proposed in [14] using DCT, SVD, DST, FFT and Edge Detection Method. This work analysis is presented for copyright protection and copy control applications. A digital video watermarking scheme based on DWT is addressed in [15] and the algorithm is analyzed against various attacks on watermarked video. In [16] the authors proposed two different watermarking schemes based on Discrete Cosine Transform (DCT) Discrete Wavelet Transform (DWT) singular value decomposition (SVD). The proposed first scheme is based on SVD of DC coefficients using decomposition at second level of DCT whereas the second scheme is based on SVD of all DCT values using cover image composition at second level DWT.

A new DWT based Fragile Watermarking scheme using Arnold Scrambling Algorithm is proposed in [17] that satisfactorily protects the data and also locates the various tampering efficiently. Reference [18] proposes a Digital Image Watermarking by using QR code as cover image and as secret image to protect it from other users. This paper presented a method in which the image is first encrypted in random matrix and invisibly watermarked in cover image. In this proposed method no information about the cover image and the secret image is required for extraction of secret image. A number of other proposals are also available regarding the security of digital information over high speed networks. These proposed methods have a good performance but the methods are complex to implement. Reference [19] proposed a MATLAB model for secure video and image streaming for remote access with the help of visible watermarking. Reference [20] presents a comparative analysis of digital image watermarking techniques in frequency domain. This analysis is based on the performance against robustness and computational complexity of different watermarking schemes after attacks. This paper presents a Digital Watermarking using Discrete Wavelet Transformation (DWT). Apaper with a general overview of image watermarking and highlighted different security issues is presented in [21]. This paper proposed an Image watermarking scheme using Least Significant Bit (LSB) algorithm for embedding the message into the image. A paper that proposes a method on how to analyse the watermarked images using MATLAB is present in [22]. This paper also presents the method of analysis of effects of attacks on a DWT-DCT hybrid algorithm. The previous work has led to the development of various methods that have their own benefits and limitations. These works have shown the importance of the digital watermarking in the security and authentication of digital data in the form of image. Thus, there is a large scope in this area to work on the digital watermarking technique that should have less computational complexity with high performance in high speed digital networks.

III.WATERMARKING OF DIGITAL IMAGES

In digital image watermarking scheme, a secret information or image is embedded in another image in invisible manner. The secret information is called watermark that has some copyrighted or secured information. The image in which the watermark image is embedded is known as cover image. In a watermarking system there are essentially a watermark embedder and a watermark detector. The watermark embedder performs the operation of inserting a watermark onto the cover image. A watermark embedder, sometimes, use a key in embedding watermark. This key has a one-to-one relation with the watermark information and it ensures that only desired users can detect the watermark.A watermarking can be classified on the basis of the property of the result of the watermarking process. In Visible

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Watermarking, the information is visible in the cover image after it is being watermarked. If, for example, the watermark is a logo then its presence can be identified in the watermarked image. In case of the Invisible watermark the embedded watermark cannot be seen in the watermarked image. The information from this watermarked image can be modified during attacks. In the Robust watermarking scheme the watermarked image is resistant to processing or modification by attacks. In Fragile Watermarking, the watermark gets easily destroyed by any attempt to tamper or manipulate it. The Semi-Fragile Watermarks contains features of both Robust and Fragile watermarking schemes. The properties that define the performance of a Watermarking Scheme are Effectiveness, Fidelity, Payload and Robustness. Effectiveness defines the probability of a message of getting correctly detected. Fidelity defines the amount of change in the quality of image that is being watermarked. Payload defines the amount of information that can be watermarked in a cover image. Robustness defines the sustenance of the watermark against the various types of attacks on the watermarked image information.

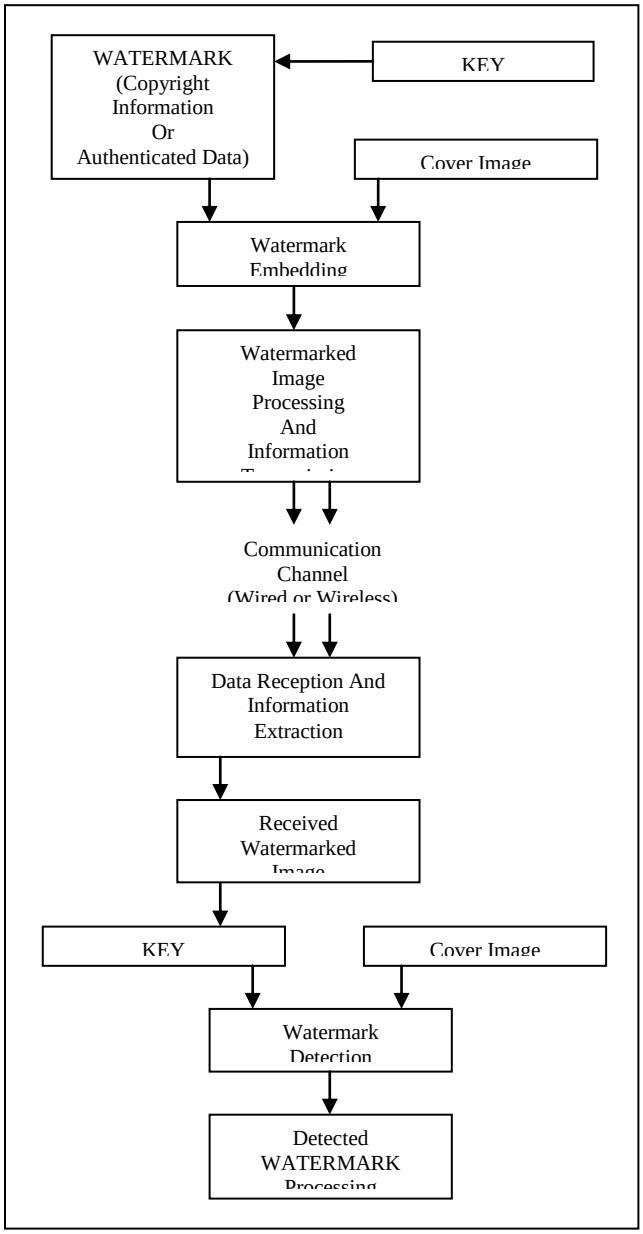


Fig. 2 Watermarking Model in Communication System

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

A watermark embedder and detector in a communication process based watermarking scheme can be modeled as shown in Fig2. In the beginning of watermarking process, if a key is used to encode the copyright image information then the key is one-to-one mapped with the watermark image. This data is then embedded with the cover image. The watermarked image is then processed as defined by the system. The decoder receives the watermarked image information and performs the reverse operation and extracts the copyright information. The watermarking can be performed in: (1) Spatial Domain, or (2) Frequency (Transform) Domain. In the Spatial Domain based watermarking schemes the pixels of the cover image are modified in randomly selected subsets of image area with respect to the watermark image whereas in Frequency Domain based watermarking schemes selective frequency based components of the cover image are modified with respect to the watermark image. Frequency Domain based watermarking schemes are more Robust than Spatial Domain based schemes.

IV. IMAGE WATERMARKING USING DISCRETE WAVELET TRANSFORM

The effective watermarking scheme should be robust and easy to implement in real time systems. The most common watermarking schemes under Spatial Domain are Least Significant Bit (LSB), Spread Spectrum Modulation (SSM), Texture Mapping Coding (TMC) and Patchwork Algorithm. These schemes can be used to spread information in the whole or in a specific part of the cover image. The most common watermarking schemes under Frequency Domain are Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) and Fast-Fourier Transform (FFT). The implementation of DCT based schemes is computationally complex and weak against geometric attacks like rotation, scaling, cropping and translation. Whereas DFT based schemes are invariant against such geometric attacks. DWT works on small waves that have varying frequency and limited duration. These small waves are called wavelet. DWT scheme involves division of image in three spatial directions i.e., horizontal, vertical and diagonal. The wavelets reflect the anisotropic properties of HVS more precisely. DWT uses multi-resolution description of an image and, hence, an image can be processed from low resolution to high resolution. The computational complexity of DWT is high as compared to DCT but it understands HVS more closely than DCT. The frequency domain processing using DWT decomposes the input signal sequence into two types of components: (1) average component, and (2) detail component. In 1-dimensional DWT the image signals are decomposed into two sub-bands/components using a low-pass filter and in 2-dimensional DWT the input image is decomposed into four sub-bands, one average component (LL) and three detail components (HL, LH, HH). In the component abbreviations the first letter represents the frequency offset of the row, either low or high, and the second letter represents to the filter applied to the column. In a level-2 DWT, The approximate part of the image is mentioned by lowest resolution level (LL) and the detail parts of the image is referred by the other parts, i.e., Vertical High (LH), Horizontal High (HL) and High (HH) frequencies. 1-D, 2-D and 3-D DWT decomposition of an input image is shown in Fig 3.

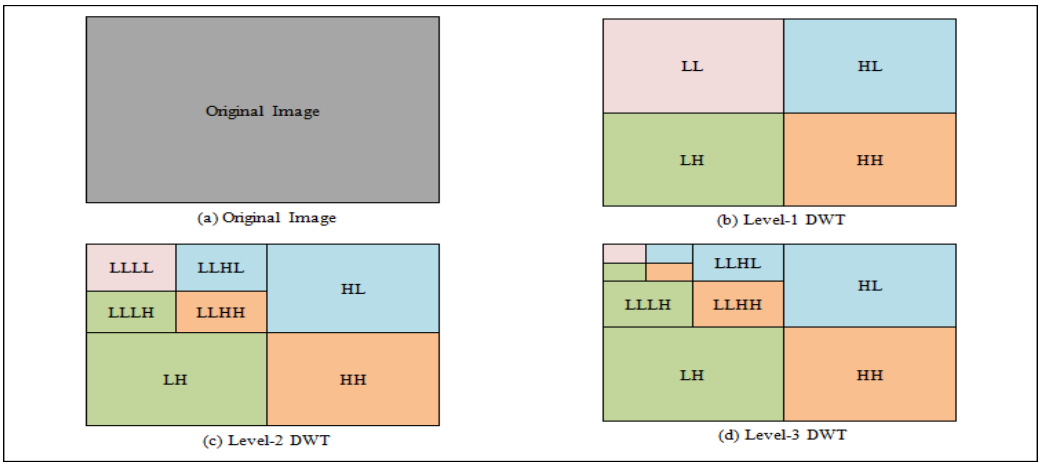


Fig. 3DWT based Image area decomposition in Digital Watermarking Scheme

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

In the present work the watermarking algorithm is performed using following algorithmic steps:

1. Select source image (cover image)
2. Select the authenticated information image (watermark Image)
3. Separate source image into 4 bands using DWT basedQuad Tree Decomposition (LL, HL, LH, HH)
4. Select the band to embed the watermark
5. Insert the watermark in the source image
6. Apply Inverse DWT
7. Transmission of Watermarked Image
8. Perform DWT on watermarked image
9. Subtracting the cover image from the output of above step
10. Perform Inverse transformation
11. Output is Watermark image

A good algorithm shows high performance against high noise level. The calculation of Peak Signal-to-Noise Ratio (PSNR) gives the most important performance analysis of any scheme. The quality of extracted watermark can be measured by PSNR. PSNR give us a rough approximation of the quality of the watermark. PSNR is measured in db. It is given by equation(1):

$$PSNR = 10 \log10[(Image_{peak})^2 / MSE] \quad - (1)$$

Where, MSE is Mean Squared Error between source image and the distorted image, and it is given by equation (2):

$$MSE = \sum \left((\text{Source Image} - \text{Distorted Image})^2 / (M * N) \right) \quad - (2)$$

Here, $Image_{peak}$is the peak values of the input signal. Usually it has a value of 255, i.e., the maximum value of luminance level. This peak signal value to noise ratio to evaluate the quality of image after embedding the watermark. In general, human eyes can accept a processed image if its PSNR is greater than 30 db. Greater the PSNR means greater is the image quality.

V. RESULT AND DISCUSSION

In the proposed execution, random disturbance or noise is added in the watermarked image to analyze the performance of the proposed scheme. The source image in coloured and grey-scale are shown in Fig 4. Fig 5 shows the watermarked image and the difference between the original and the watermarked image.

(A) Source Image Coloured (B) Source Image Grey-Scale

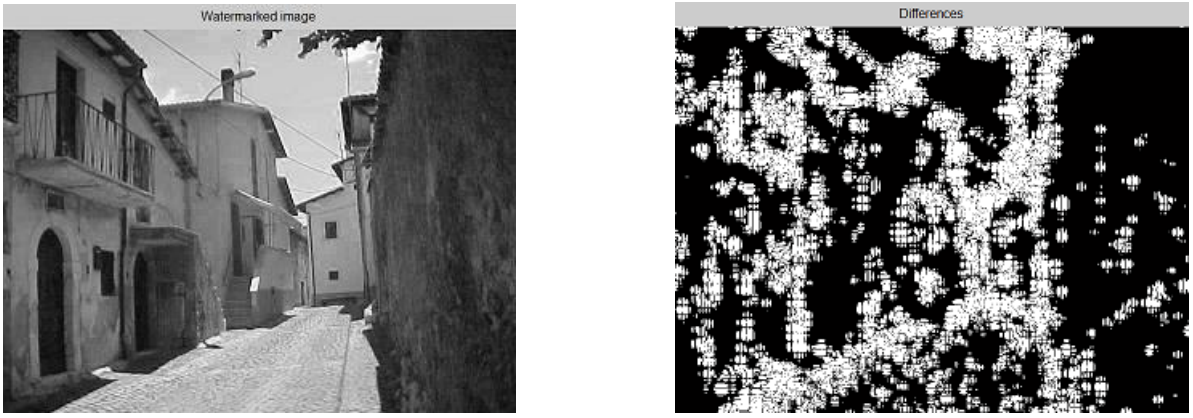
Fig. 4Source Image used for Watermarking in Proposed Work

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015



(A) Watermarked Image (B) Difference between Watermarked Image and Source Image

Fig. 5Watermarked Image and its difference from Source Image

After the series of Experiments performed on Images in MATLAB, PSNR values are analysed to determine the Quality of Watermarked Object. Calculation of PSNR values by applying various amount of noise on watermarked image is analysed and presented in Fig 6. A high value of PSNR indicates higher efficiency of the proposed algorithm. A comparison of proposed algorithm is present in Table I. The comparative analysis concludes that the proposed algorithm is effective in handling the noise better than the referenced works.

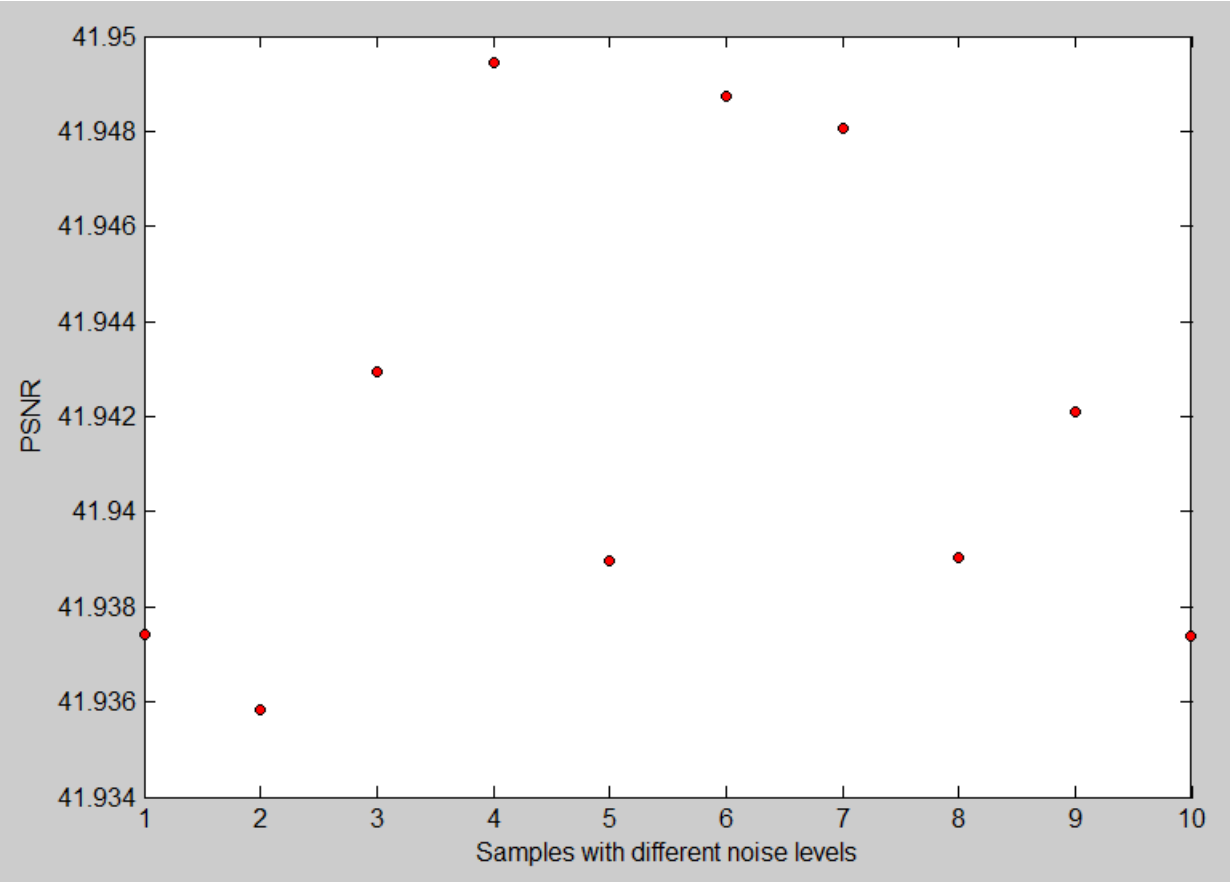


Fig. 6PSNR Value observation graph for various amount of noise on Watermarked Image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Table I Comparison of PSNR Values of Proposed Design with existing Designs

Reference Design	PSNR
Proposed Scheme	41.9
[1]	37.2
[2]	35.2047
[9]	35.123
[16]	41.4765
[20]	36.38

VI. CONCLUSION

This paper presents simulation and analysis of digital image watermarking using discrete wavelet transform based algorithm which is less complex to implementation on MATLAB software. After embedding the secret data in the cover image, we got watermarked image with noticeable distortion in the cover image. The performance of the algorithm is analyzed in this work. Our Purposed technique is useful in insertion of watermark in such a way such that intruder cannot trace it easily and there is less quality of loss after the insertion of watermark inside the images. With the increase in the application of digital media communication through internet it has now become more difficult to secure the authenticity of communicated media. So, involvement of the watermarking algorithms, like the one presented in this paper, using small applications can be helpful to setup a secure data communication. Watermarking can also be used to store the data to avoid its use by malicious users. The present work is among the basic algorithm implementation for protecting data authenticity. The present algorithm can be combined with existing encryption algorithms to develop a complex algorithm for data security.

REFERENCES

1. Y. RaghavenderRao, E. Nagabhooshanam and P. Nikhil, "Directional based Watermarking Scheme using a Novel Data Embedding Approach", Advanced Computing An International Journal, Volume-3 No.-5, pp. 63-71, September 2012.
2. Gou Xin-ke and Lu Ran-ni, "Study of Algorithm of Digital Image Watermarking based on DWT", International Journal of Education and Management Engineering, pp. 20-26, July 2011.
3. Prabhishek Singh and R. S. Chadha, "Review to Digital Watermarking and a Novel Approach to Position the Watermark in the Digital Image", International Journal of Engineering and Advanced Technology, Volume-2 Issue-4, pp. 24-27, April 2013.
4. JahnviSen, A. M. Sen and K. hemchandran, "An Algorithm for Digital Watermarking of Still Images for Copyright Protection", Indian Journal of Computer Science and Engineering, Volume-3 No.-1, pp. 46-52, February-March 2012.
5. P. Ramana Reddy, Munaga V. N. K. Prasad and D. SreenivasaRao, "Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent Trends in Engineering, Volume-1 No.-1, pp. 334-338, May 2009.
6. Monika Patel and PritiSrinivasSajja, "The Significant Impact of Biometric Watermark for Providing Image Security using DWT based Alpha Blending Watermarking Technique", International Journal of Innovative Research in Computer and Communication Engineering, Volume-3 Issue-5, pp. 3943-3952, May 2015.
7. Nikhil Nigam and Yogendra Kumar Jain, "Encoded Hybrid DWT based Watermarking Scheme based on Singular Matrix Decomposition", International Journal of Computer Applications, Volume-110 No.-14, pp. 37-44, January 2015.
8. IshaGarg and AnchitBijalwan, "Digital Image Watermark Key Extraction with Encryption and Decryption Scheme in MATLAB", International Journal of Computer Applications, Volume-105 No.-10, pp. 7-11, November 2014.
9. Chirag Sharma and Deepak Prashar, "DWT based Robust Technique of Watermarking applied on Digital Images", International Journal of Soft Computing and Engineering, Volume-2 Issue-2, pp. 399-402, May 2012.
10. Pravin M. Pithiya and H. L. Desai, "DWT based Digital Image Watermarking De-marking and Authentication", International Journal of Engineering Research and Development, Volume-7 Issue-5, pp. 104-109, June 2013.
11. M. V. S. S. Babu, "A Robust Watermarking Algorithm for Image Authentication", International Conference on Information and Network Technology, Volume-37, pp. 220-227, 2012.
12. Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B. C. and Anil Gupta, "LSB based Digital Image Watermarking for Gray Scale Image", IOSR Journal of Computer Engineering, Volume-6 Issue-1, pp. 36-41, September-October 2012.
13. Mustafa Osman Ali, Elamir Abu Abaida Ali Osman and Rameshwar Row, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization", International Journal of Engineering and Innovative Technology, Volume-2 Issue-5, pp. 227-231, November 2012.
14. T. Sreelekha, M. Dhamodhar Reddy and T. Ramashri, "Watermarking Algorithm using Edge Detection Technique and DCT DST FFT", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Volume-2 Issue-12, pp. 5982-5989, December 2013.
15. Prachi V. Powar and S. S. Agrawal, "Design of Digital Video Watermarking Scheme using MATLAB SIMULINK", International Journal of Research in Engineering and Technology, Volume-2 Issue-5, pp. 826-830, May 2013.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

16. Riteshpatel and A. B. Nandurbarkar, "Implementation of DCT DWT SVD based Watermarking Algorithms for Copyright Protection", International Research Journal of Engineering and Technology, Volume-2 Issue-2, pp. 340-344, May 2015.
17. KrisdaKhankasikam, "A New Fragile Watermarking Scheme based on Wavelet Edge Feature", International Journal of Future Computer and Communication, Volume-4 No.-4, pp. 270-274, August 2015.
18. SumedhaNishane and V. M. Umale, "Digital Image Watermarking based on DWT using QR Code", International Journal of Current Engineering and Technology, Volume-5 No.-3, pp. 1530-1532, June 2015.
19. Ranjith Kumar S., Krishna BhushanVutukuru, Lourts Deepak A. and Chaitra S. K., "Implementation of Watermarking Techniques in Images and Videos using 2D-DWT-IDWT Compression and Decompression Methods", International Conference on Advances in Computer Science and Electronics Engineering, pp. 253-257, 2012.
20. Mandeep Singh Saini, VenkataKranthi B. and Gursharanjeet Singh Kalra, "Comparative Analysis of Digital Image Watermarking Techniques in Frequency Domain using MATLAB SIMULINK", International Journal of Engineering Research and Applications, Volume-2 Issue-4, pp. 1136-1141, May-June 2012.
21. Puneer Kr. Sharma and Rajni, "Analysis of Image Watermarking using Least Significant Bit Algorithm", International Journal of Information Sciences and Techniques, Volume-2 No.-4, pp. 95-101, July 2012.
22. Lalit Kumar Saini and Vishal Shrivastava, "Analysis of Attacks on Hybrid DWT-DCT Algorithm for Digital Image Watermarking with MATLAB", International Journal of Computer Science Trends and Technology, Volume-2 Issue-3, pp. 123-126, May-June 2014.