International Journal of Engineering Innovation & Research
Volume 3, Issue 2, ISSN: 2277 – 5668

Digital Image Watermarking using Adaptive DCT-DWT

Anshul Nema, Prof. Ravi Mohan

***Abstract* – Digital Image Watermarking is one such technology that has been developed to protect digital images from illegal manipulations. In particular, digital image watermarking algorithms which are based on the Adaptive discrete continuous transform and discrete wavelet transform (Adaptive DCT-DWT) have been widely recognized to be more prevalent than others. This is due to the wavelets' excellent spatial localization, frequency spread, and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. This method of watermarking is found to be robust and the visual watermark is recoverable without only reasonable amount of distortion even in the case of attacks. Thus the method can be used to embed copyright information in the form of a visual watermark or simple text.**

***Keywords* – Wavelet Transform, Compression Technique, GUI, Adaptive DCT-DWT, Digital Image Watermarking, MSE, PSNR.**

I. INTRODUCTION

In the modern era where things have been patented or the rights more modern techniques to establish the identity and leave it unhampered have come into picture. Digital watermarking includes a number of techniques that are used to imperceptibly convey information by embedding it into the cover data. There has always been a problem in establishing the identity of the owner of an object. In case of a dispute, identity was established by either printing the name or logo on the objects. Unlike printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that they are completely invisible. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image in such a way that they cannot be identified and show resilience against attempts to remove the hidden data.

II. CRYPTOGRAPHY, STEGANOGRAPHY

Cryptography as the study of secret (crypto) writing (graphy) can be defined as the science of using mathematics to encrypt and decrypt data back. It allows two people, commonly known as Alice and Bob, to communicate with each other securely. This means that an eavesdropper known as Eve will not be able to listen in on their communication. Cryptography also enables Bob to check that the message sent by Alice was not modified by Eve and that the message he receives was really sent by Alice.

While cryptography is about protecting the content of the messages, Steganography is about concealing their very existence. Steganography comes from a Greek word that means covered writing (Stego = covered + graphy = writing). Examples can be thought as messages exchanged between drug dealers via emails in encrypted forms, or messages exchanged by spies in covert communication.

III. DIGITAL WATERMARKING (ENCODING-DECODING)

Steganography and watermarking both describe techniques used for covert communication; Steganography typically relates only to covert point to point communication between two parties. Steganography methods are not robust against attacks or modification of data that might occur during transmission, storage or format conversion.

Watermarking, as opposed to Steganography, has an additional requirement of robustness against possible attacks. An ideal Steganography system would embed a large amount of information perfectly securely, with no visible degradation to the cover object.

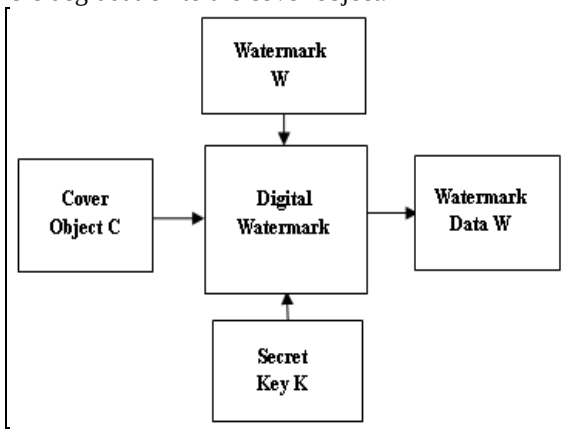


Fig.1. Digital Watermarking – Embedding

An ideal watermarking system, however, would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness.

The working principle of the watermarking techniques is similar to the Steganography methods. A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in Figure 1 and 2.

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data W.

The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark W.

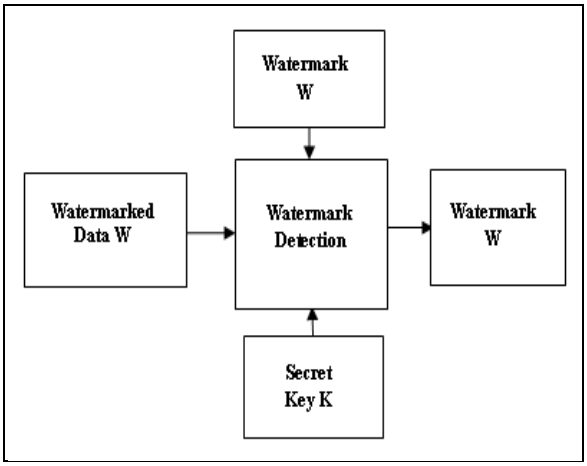


Fig.2. Digital Watermarking - Decoding

IV. Digital Watermarking Applications

Watermarking techniques can compliment encryption by embedding a secret imperceptible signal, a watermark, directly into the original data in such a way that it always remains present. Digital watermarking makes law enforcement and copyright protection for digital media possible and practical when it aims to automatically detect and possibly also prosecute copyright infringements.

The watermark stems from the ancient art of a Figurers or design incorporated into paper during its manufacture and appearing lighter than the rest of the sheet when viewed in transmitted light for the same purpose. A watermark can be used for the following purposes.

1. Image Data Authentication
2. Indexing and Image Labelling
3. Medical Safety
4. Data Hiding etc.
5. Copyright Protection
6. Fingerprinting
7. Copy Protection
8. Image Authentication and Data Integrity

V. Digital Watermarking with Adaptive DCT-DWT

The Adaptive Discrete Wavelet Transform – Discrete Cosine Transform, by this method I have taken the advantages of both DWT and DCT method for the watermarking purpose. In this technique we are first of all taking the DWT of the original image from which we will get 4 coefficients of image named approximate, horizontal, vertical and diagonal coefficients. Out of these four elements the approximate coefficients carry maximum information so we cannot change that coefficients and the diagonal coefficients are of high frequency so will be affected more by noise. So we can embed the message by changing the horizontal or/and vertical coefficients of the image.

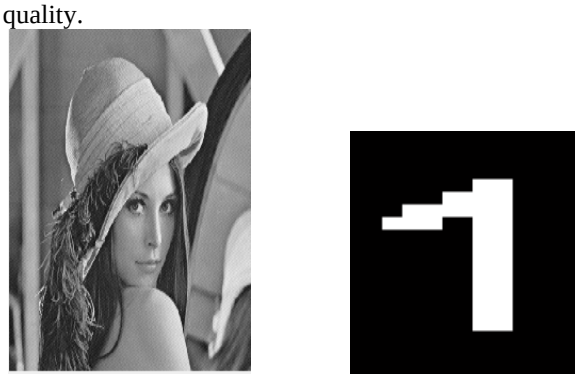
Here in this algorithm I am first of all taking the DWT of the original image and then taking the DCT of the horizontal coefficients of the DWT i.e. CH1. After wards embedding the watermark in the DCT and taking IDCT of the coefficients. Then taking the IDWT of the coefficients of the modified image which is our watermarked image using the combined DCT-DWT algorithm.

While recovering the watermark from the image we are supposed to follow the same steps in the almost inverse manner. I first take the DWT of image then taking the DCT of horizontal coefficients and retrieve the watermark from it.

(a) Original Image (b) Watermarked Image

Fig.3. Watermarking using Adaptive DCT-DWT

For detection, the image is broken up into those same 8x8 blocks, and a DCT-DWT performed. The same PN sequence is then compared to the middle frequency values of the transformed block. If the correlation between the sequences exceeds some threshold T, a “1” is detected for that block; otherwise a “0” is detected. Again k denotes the strength of the watermarking, where increasing k increases the robustness of the watermark at the expense of quality.



(a) Watermarked Image (b) Recovered Message

Fig.4. Watermark Detection using Adaptive DCT-DWT

VI. Implementation using Matlab

Watermarking has been used to measure the content of an image and text, with higher values indicating images which are richer in details.

Fig.5 shows the general block diagram of watermarking process. Original document can be image or text file. This document gives to the watermark embedder. The input of

the watermark embedder is watermark image which is generating by water marker generator with the help of secret key generator. Watermark embedder combines these two images or text and generate the watermarked image. It is transmit over channel and receive the transmitted document and given to the watermark extraction. Watermark extractor generates the original document as well as secrete message.

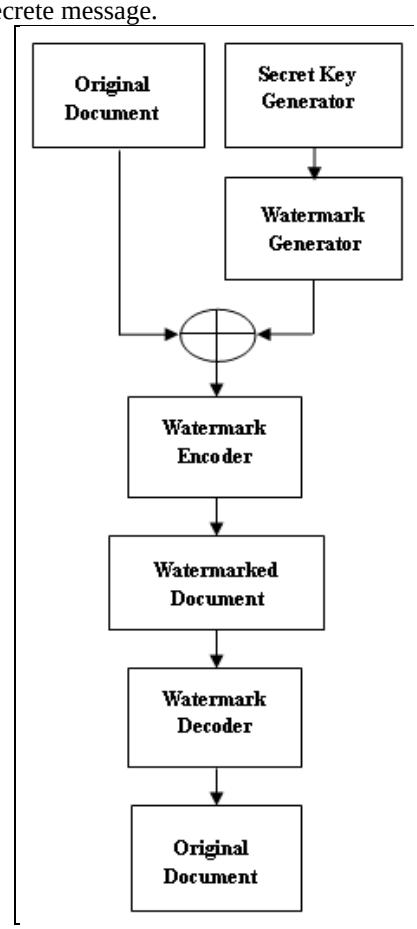


Fig.5. General Block Diagram of Watermarking

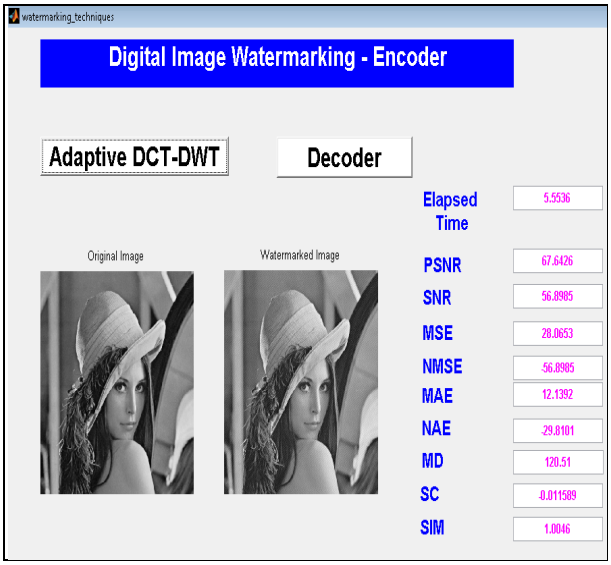


Fig.6. GUI window for Encoding for Digital Image Watermarking

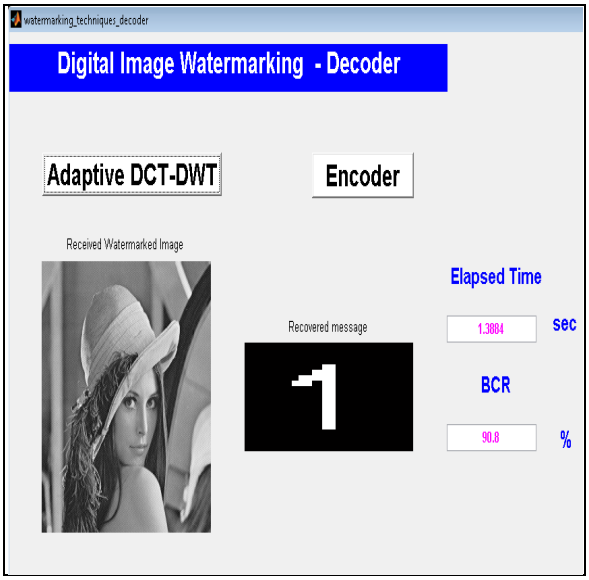


Fig.7. GUI window for Decoding for Digital Image Watermarking

The steps behind the MATLAB-GUI interface process are shown in fig.6. and fig.7. So the proposed program can be interpreted as a function to carry out image and text using adaptive DCT-DWT. A Leena image and text nine are displayed in the experimental figures.

Measurement Parameters are:

1. Similarity (A): It gives idea of how much similar the watermarked image and original image is.
2. Correlation Quality (CQ): It is an inbuilt function of MATLAB which finds correlation between the images.
3. Image Fidelity (IF): It is found from NMSE.
4. Mean Absolute Error (MAE): It calculates the mean of all the absolute errors between pixels of original and watermarked image.
5. Mean Difference (MD): It calculates the mean of the difference between original and watermarked image pixels.
6. Mean Square Error (MSE): It gives amount of error introduced by embedding a watermark in the image.
7. Normalized Absolute Error (NAE): It calculates the normalized values of absolute error by the factor of 1/MN.
8. Normalized Cross Correlation (NCC): It calculates the correlation factor between pixels of the original image and watermarked image.
9. Normalized Mean Square Error (NMSE): It calculates the normalized values of the mean square error by factor 1/MN.
10. Peak Signal to Noise Ratio (PSNR): It gives amount of degradation between peak values of original and watermarked image pixels.
11. Structural Content (SC): This is inbuilt function of MATLAB which finds the quality of embedding.
12. Signal to Noise Ration (SNR): It gives amount of degradation between all the pixels of original and watermarked image.

VII. CONCLUSION

This paper implemented Adaptive DCT-DWT with watermarking technique and the domain of watermarking technique are better in context to the perceptibility of watermarked image to the human eye as they are affecting very less to the image quality. So this paper, finally come to the conclusion that there is a trade off between perceptibility and robustness of the watermarking technique. From this the user should decide the preference of quality and apply the watermarking technique suitable to the requirements. In future this technique can be implemented for the video, audio and text. Also the technique is implemented in the MATLAB simulator which can be implemented for the real time applications on the Digital Signal Processor (DSP) system or ARM Processor system. The real time implementation of this technique can be useful to the applications like live telecasting of video and audio signals to secure them from the tempering in between the channel.

REFERENCES

[1] Gonzalez RC, Woods RE: Digital Image Processing Prentice Hall, Upper Saddle River, NJ; 2002.
[2] R. Wolfgang and E.J. Delp "A Watermark for Digital Image," IEEE int. Conf on Image Processing, Vol. 111, pp2 19-222 Lausanne, Switzerland, September 1996.
[3] Chiou-Ting Hsu and Ja-Ling Wu, "Multiresolution Watermarking for Digital Images," IEEE Trans. Circuits and System II, Vol. 45, No. 8, pp. 1097-1101, August 1998.
[4] Athanasios Nikolaidis and Ioannis Pitas, "Asymptotically Optimal Detection for Additive Watermarking in the DCT and DWT Domains," IEEE Transaction on Image Processing, Vol. 12, No. 5, May 2003.
[5] Wai C. Chu, "DCT-Based Image Watermarking Using Sub sampling," IEEE Transaction on Multimedia, Vol. 5, No. 1, March 2003.
[6] Shinfeng D. Lin and Chin-Feng Chen, "A Robust DCT-Based Watermarking for Copyright Protection," IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, AUGUST 2000.
[7] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking," Journal of Computer Science 3 (9): 740-746, 2007.
[8] Shital Gupta, Dr Sanjeev Jain, "A Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform," Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010.
[9] Beghdadi A, Negrate AL: Contrast enhancement technique based on local detection of edges. Comput Visual Graph Image Process 1989, 46:162-274.
[10] Amina Saleem, Azeddine Beghdadi and Boualem Boashash "Image fusion-based contrast enhancement", EURASIP Journal on Image and Video Processing 2012, 2012:10.
[11] Tang J, Peli E, Acton S: Image enhancement using a contrast measure in the compressed domain. IEEE Signal Process Lett 2003, 10(10):289-292
[12] Tang J, Kim J, Peli E: Image enhancement in the JPEG domain for people with vision impairment. IEEE Trans Biomed Eng 2004, 51(11).
[13] Mauro Barni and Franco Bartolini, Watermarking Systems Engineering Enabling Digital Assets Security and Other Applications, Marcel Dekker Inc., New York, 2004.
[14] Chang-Tsun Li, Multimedia Forensics and Security, Information Science Reference, New York, 2008.
[15] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Tony Kalker, Digital Watermarking and Steganography, Morgan Kaufmann Publications, USA, 2008.
[16] Michael Arnold, Martin Schmucker and Stephen D. Wolthusen, Techniques and Applications of Digital Watermarking and Content Protection, Artech House, Boston, London, 2003.
[17] Yoseph Abate, Digital Image Watermarking, ECE Department, Addis Ababa University, 2005.
[18] Alper Koz, Digital Watermarking based on Human Visual System, Electrical and Electronics Department, Middle East Technical University, 2002.
[19] Navneetkumar Mandhani, Watermarking using Decimal Sequences, Electrical and Computer Engineering Department, Louisiana State University, 2004.
[20] Ali Al-Haj, Combined DCT-DWT Digital Image Watermarking, Journal of Computer Science, 3 (9): 740-746, 2007