International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Adaptive Watermarking Based DCT with Set Partitioning in Hierarchical Trees

Simranjot Kaur[1], Er.Maninder Sharma[2]
[1]Computer Science & Engineering,
Doaba Group of College, PTU, Punjab, India
[2]Electronics & Communication Engineering,
Doaba Group of College, PTU, Punjab, India
[1]jotihira@gmail.com, [2]maninderecediet@gmail.com

Abstract: *In this paper, we propose a new adaptive watermarking scheme. One first contribution is a DCT modulation which adaptively takes care of the local specificities of the image content. The suggested scheme uses the embedded watermark to estimate the degradation of cover image under different distortions. The watermarking process is implemented in DCT domain of the cover image. The correlated DCT coefficients across the DCT sub-bands are categorized into Set Partitioning in Hierarchical Trees (SPIHT). Those SPHIT trees are further decomposed into a set of bit-planes. The watermark is embedded into the selected bit-planes of the selected DCT coefficients of the selected tree without causing powerful fidelity loss to the cover image. The experiments will be performed to estimate the image quality in terms of PSNR, MSE and SSIM. The results obtained will show that the proposed scheme has good computational capability for practical applications.*
Also we conclude from the experiments that it leads to optimal watermarking conduct. For the performance of this proposed work Image Processing Toolbox under the MATLAB software is used.

Keywords: *DCT, SPIHT, Watermarking, PSNR, MSE, SSIM.*

I. INTRODUCTION

1.1 Digital Watermarking

"Watermarking" is the development of masking digital figures in a hauler hint; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to demonstrate the authenticity or integrity of the carrier signal or to show the identity of its owners. Traditional Watermarks may be applied to visible media (resembling images or video), whereas in digital watermarking, the pointer may be audio, pictures, video, texts or 3D models.
DIGITAL watermarking is a process in which some information is embedded within a digital media so that the inserted fact becomes section of the media. This technique serves a number of purposes such as broadcast monitoring, data authentication, data indexing and so forth. Watermarks have two categories of roles: In the first category, the watermark is considered as a transmission code and the decoder must recover the whole transmitted information correctly. In the second type, the watermark serves as a authentication code. In the latter system, the watermark detector must simply determine the presence of a specific pattern. There is still required for reversible techniques that institute the buck distortion possible with high embedding capacity. Since the introduction of the concept of reversible watermarking in the Barton patent, numerous methods have been anticipated. Among these solutions, most update schemes use Expansion Embedding modulation, DWT modulation or, more recently, their combination. One of the foremost unease with these modulations is to avoid underflows and overflows. Basically, both image watermarking and image compression are concerned of the image redundancy, which is to be compact in the case of compression, whilst is employed to interleave the mark in the case of watermarking. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust" we mean the capability of the watermark to resist exploitation of the media, such as lossy compression (where squeezing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in various way), scaling, and cropping, just to specify some. In

some cases the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent.

1.2 Types of Water Marks

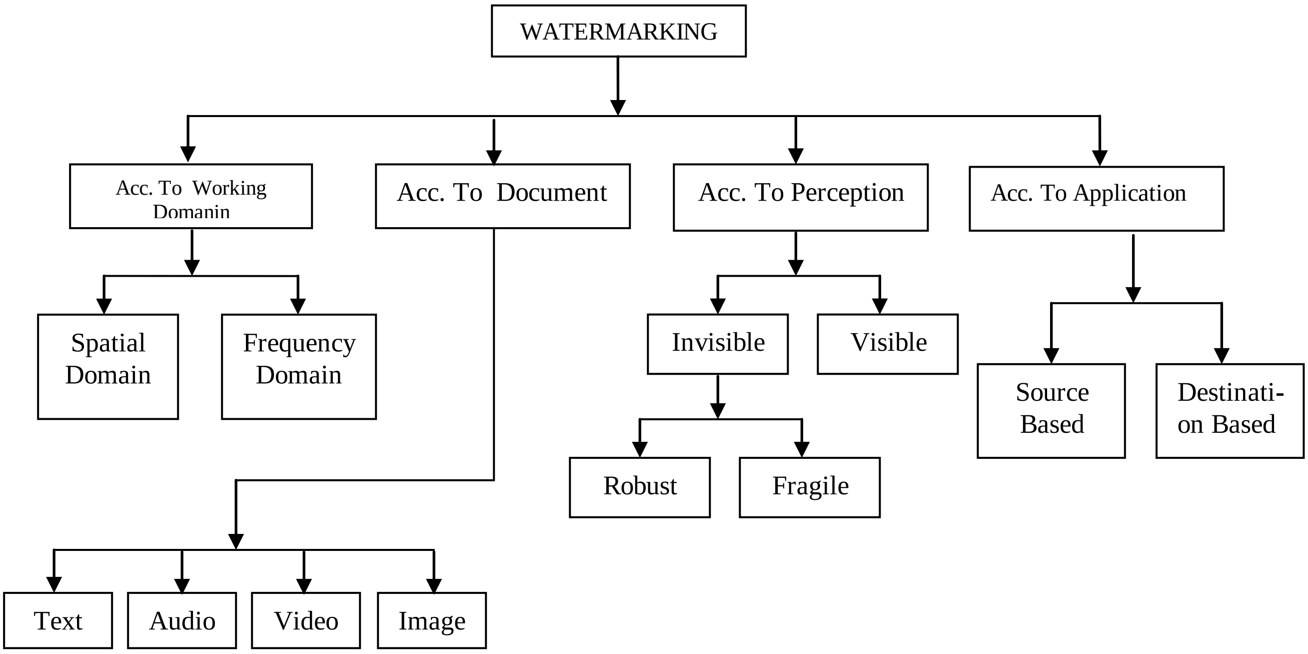


Figure 1.1: Hierarchy of Water marks

There are lots of techniques to overcome digital water marking .That all techniques are described below.

Visible watermarks: Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only.

Invisible watermark: Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for gratify and/or author substantiation and for detecting illicit copier.

Public watermark: Such a watermark can be read or retrieved by anyone using the specialized algorithm. In this sense, public watermarks are not sheltered. However, public watermarks are informative for carrying IPR information.

Private Watermark: Private watermarks are also known as secure watermarks. To study or reclaim such a watermark, it is vital to have the furtive key.

Fragile watermark: Fragile watermarks are also known as tamper-proof watermarks. Such watermarks are destroyed by data manipulation.

Bit-stream watermark: The term is sometimes used for watermarking of compressed data such as video.

Text document watermark: Text document is a discrete information source. In discrete sources, contents cannot be modified. The approaches for text watermarking are hiding watermark information in semantics and hiding watermark in text format.

In **semantic-based watermarking**, the text is deliberate just about the message to be buried. Thus, disingenuous information covers watermark information. Such techniques defy scientific approach.

1.3 Digital Watermarking Applications

- **Ownership Assertion**
  - ‘A’ uses a private key to engender a watermark and entrench it in the document
  - ‘A’ makes the watermarked image publicly available
  - ‘B’ claims that he owns the image derived from the public image

- **Fingerprinting**
  - Used to avoid unauthorized duplication and distribution.
  - A distinct watermark (a fingerprint) is embedded in each copy of the data.

- **Authentication & integrity verification**
  - A unique key associated with the source is used to create the watermark and then embed in the document.

- This key is then used to extract the watermark and the integrity of the document demonstrates on the cores of the veracity of the watermark.

- **Usage control & Copy protection**
  - Digital watermark inserted to indicate the number of copies tolerable.
  - Every time a copy is prepared the hardware transforms the watermark and at the same time it would not create any more copies of the data.

- **Content Protection**
  - Content owner strength wants to publicly and freely impart a preview of multimedia content being sold.

1.4 Characteristics of Digital Watermarks

- **Unobtrusive:** invisible adequate not to humiliate the data eminence and to thwart an attacker from finding and deleting it.
- **Readily Detectable:** the data owner or an independent control clout should effortlessly identify it.
- **Unambiguous:** retrieval of it should unambiguously identify the data owner.
- **Innumerable:** it should be possible to generate a large number of watermarks, all apparent.
- **Robust:** intricate to confiscate for an attacker, who would like to raze it in order to counterfeit the copyright of the data. Moreover, removal of it should cause a considerable degradation in the quality of the data.

1.5 Advantages/Disadvantages

- Embedding the checksum only changes (on average) half the number of pixel. So less visual distortion.
- Can cleave to multiple watermarks as long as they don't overlap.
- Extremely simple and fast.
- Extremely fragile. Any change to the checksum causes the failure of the verification procedure.
- Forger could reinstate a section with a further one of an identical size and checksum.
- Entire watermark can be removed by removing the LSB plane. Can't survive lossy compression.

II. LITERATURE SURVEY

(Kim & Suthaharan 2004)He proposed An Entropy Masking Model for Multimedia Content Watermarking. Inserting maximal allowable transparent watermark, which in turn is extremely hard to attack with common image processing operations, is important aspect of watermark design. We present a new watermark design tool for digital images and digital videos that are based on human visual system (HVS) characteristics. In this tool, basic mechanisms of inhibitory and excitatory behavior of HVS cells are used to determine image dependent upper bound values on watermark insertion. This allows us to insert maximal allowable transparent watermark, which in turn is extremely hard to attack with common image processing, Motion Picture Experts Group (MPEG) compression. As the number of image details (e.g. edges) increases in an image, the HVS decreases its sensitivity to the image details. Similarly, the HVS decreases its sensitivity to the object motions as the number of motion increases in a video signal. We model this decreased sensitivity to the image details and object motions as an entropy masking. Entropy masking model can be efficiently used to increase the robustness of image and video watermarks. We have shown that our entropy-masking model provides watermark scheme with increased transparency and henceforth increased robustness.

Sha Wang, Dong Zheng, Jiying Zhao, *Member, IEEE*, Wa James Tam, and Filippo Speranza in 2014. Image quality evaluation is very important. In applications involving signal transmission, the Reduced- or No-Reference quality metrics are generally more practical than the Full- Reference metrics. In this study, we propose a quality estimation method based on a novel semi-fragile and adaptive watermarking scheme. The proposed scheme uses the embedded watermark to estimate the degradation of cover image under different distortions. The watermarking process is implemented in DWT domain of the cover image. The correlated DWT coefficients across the DWT sub bands are categorized into Set Partitioning in Hierarchical Trees (SPIHT). Those SPHIT trees are further decomposed into a set of bitplanes. The watermark is embedded into the selected bitplanes of the selected DWT coefficients of the selected tree without causing significant fidelity loss to the cover image. The accuracy of the quality estimation is made to approach that of Full-Reference metrics by referring to an "Ideal Mapping Curve" computed *a priori*. The experimental results show that the proposed scheme can estimate image quality in terms of PSNR, wPSNR, JND and SSIM with high accuracy under JPEG compression, JPEG2000 compression, Gaussian low-pass filtering and Gaussian noise distortion. The results also show that the proposed scheme has good computational efficiency for practical applications.

(Abhilash & Shamseerdaula 2013). He proposed A Novel Lossless Robust Adaptive Watermarking Method for Copyright Protection of Images. Robust adaptive watermarking (RRW) methods are popular in multimedia for protecting copyright, while preserving intactness of host images and providing robustness against unintentional attacks. However, conventional RRW methods are not readily applicable in practice. That is mainly because: 1) they fail to offer satisfactory reversibility on large-scale image datasets; 2) they have limited robustness in extracting watermarks from the watermarked images destroyed by different unintentional attacks; and 3) some of them suffer from extremely poor invisibility for watermarked images. There-fore, it is necessary to have a framework to address these three problems, and further improve its performance. This paper presents a novel pragmatic framework, wavelet-domain statistical quantity DWT and clustering (WSQH-SC). Compared with conventional methods, WSQH-SC ingeniously constructs new watermark embedding and extraction procedures DWT and clustering, which are important for improving robustness and reducing run-time complexity. Additionally, WSQH-SC includes the property-inspired pixel adjustment to effectively handle overflow and underflow of pixels. This results in satisfactory reversibility and invisibility. Furthermore, to increase its practical applicability, WSQH-SC designs an enhanced pixel-wise masking to balance robustness and invisibility. We perform extensive experiments over natural, medical, and synthetic aperture radar images to show the effectiveness of WSQH-SC by comparing with the histogram rotation-based and histogram distribution constrained methods. Index Terms— Integer wavelet transform, k-means clustering, masking, robust adaptive watermarking (RRW).

III. PROBLEM FORMULATION

- Different algorithm on watermarking technique has been proposed previously but there have been always need for better and more secure results.
- The previous watermarking uses dwt algorithm alone which is poor in quality.
- The techniques are more prone to noise and less accurate.
- The performance of watermarking system was poor on the basis of MSE and PSNR.

IV. OBJECTIVES

- Enhanced watermarking algorithm is proposed which is based on tree structure using SPIHT and 3 level DCT and DWT.
- Proposed algorithm is more secure and provides two tier securities.
- It doesn't degrade the quality of image.
- It has better Accuracy, PSNR, SSIM and MSE results.

V. METHODOLOGY

Phase1: Firstly we develop a code for the loading the image in the database of the MATLAB. This is done for the loading the image value in the workspace of the MATLAB.

Phase2: After that we develop a code for the loading the message image or text for the embedded purpose. And we also develop a code for the watermark embedding using adaptive watermark embedding strength.

Phase3: We develop a code for the applying the DWT, DCT and SPIHT techniques to the image.

Phase4: After that we decode for the extraction purpose of the embedded message from the watermarked image IDWT and IDCT. And finally we compare the result on the basis of PSNR, SSIM, Accuracy and MSE.

VI. RESULTS

Comparision Table

	PSNR	MSE	SSIM
DCT	90.0765	1.6955e+04	0.1366
DWT	64.3420	3.2263e+04	0.2366
Histogram	91.9581	1.6176e+04	0.4366
Histogram+Entropy	96.7755	1.5869e+04	0.4459
DCT+DWT+SPIHT	99.9581	1.5175e+04	0.5732

Fig. 6.1: Comparison between the techniques DCT, DWT, Histogram, Histogram with Entropy and DCT ,DWT with SPHIT on the basis of PSNR, MSE & SSIM.

Comparison of PSNR between Previous and our algorithm

	Previous Work	Proposed Work
PSNR	96.7755	99.9581

Fig 6.2: Comparison on the basis of PSNR values between previous work and proposed algorithm

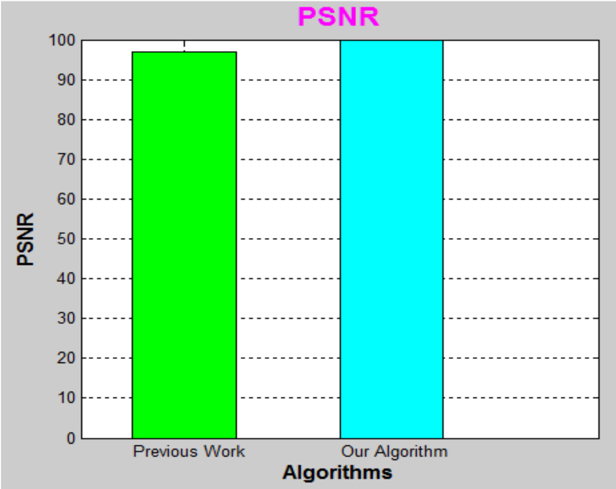


Fig 6.3: Graph of PSNR values between previous work & our algorithm

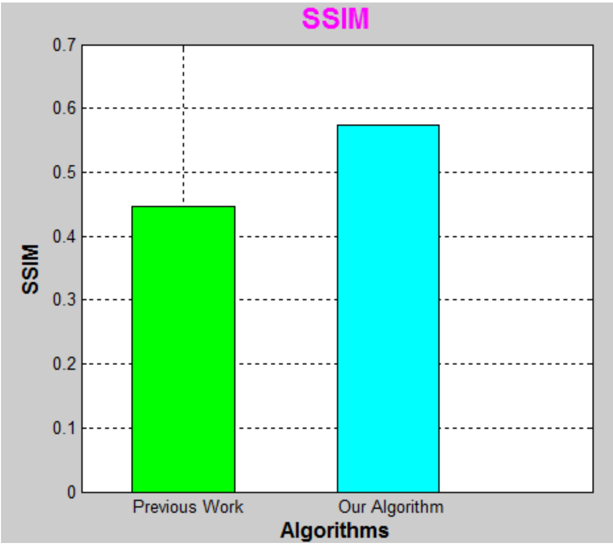


Fig 6.4: Graph of SSIM values between previous work & our algorithm

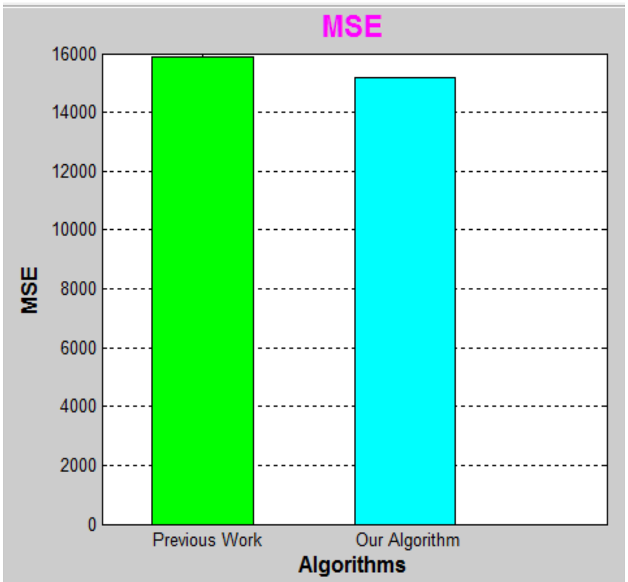
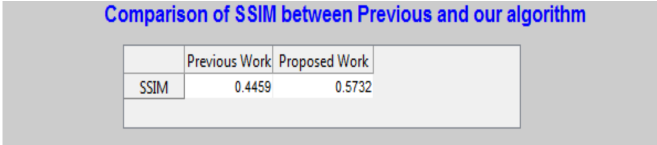


Fig 6.5: Graph of MSE values between previous work & our algorithm



Comparison of SSIM between Previous and our algorithm

	Previous Work	Proposed Work
SSIM	0.4459	0.5732

Fig 6.6: Comparison of SSIM values between previous and proposed work

VII. CONCLUSION

From the above detailed discussion, it will be beneficial impending into assorted concepts involved, and boost further advances in the area. The accurate watermarking is directly depending on the nature of the image to be watermarked and by its quality. Current research is directly concern to the digital images. From various studies, we have seen that the originality stands in identifying parts of the image that are watermarked using distinct techniques like DWT .This scheme can still be improved however; this method is fragile as any modifications will impact the watermark. Then we propose a SPIHT, DWT and DCT with increase in level i.e., 3 level DWT and DCT for watermarking embedding algorithm to keep the balance between watermarks' imperceptibility and its robustness. For the extraction of watermark we propose IDCT and IDWT. The proposed scheme is designed to estimate image quality in terms of the quality metrics, such as Accuracy, PSNR, MSE, SSIM. Thus we have proved that hybrid technique is far better in comparison to DCT or DWT. In future we can further use combination of other algorithm as well as watermarking can be combined with stegnography.

REFERENCES

[1]. Kim, S.-W.K.S.-W. & Suthaharan, S., 2004. An entropy masking model for multimedia content watermarking. 37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the, 0(2002), pp.1–6.

[2]. Sha Wang, Dong Zheng, Jiying Zhao, Wa James Tam, and Filippo Speranza "Adaptive Watermarking and Tree Structure Based Image Quality Estimation" *IEEE TRANSACTIONS ON MULTIMEDIA*, VOL. 16, NO. 2, FEBRUARY 2014

[3]. Abhilash, S. & Shamseerdaula, S.M., 2013. OPEN ACCESS A Novel Lossless Robust Reversible Watermarking Method for Copyright Protection of Images. , 3(6), pp.317–323.

[4]. D. Coltuc, "Improved embedding for prediction-based adaptive watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 873–882, Sep. 2011.

[5]. H. J. Hwang, H. J. Kim, V. Sachnev, and S. H. Joo, "Adaptive watermarking method using optimal histogram pair shifting based on prediction and sorting," KSII, Trans. Internet Inform. Syst., vol. 4, no. 4, pp. 655–670, Aug. 2010.

[6]. W. Pan, G. Coatrieux, N. Cuppens, F. Cuppens, and C. Roux, “An additive and lossless watermarking method based on invariant image approximation and Haar wavelet transform,” in Proc. IEEE EMBC Conf., Buenos Aires, Argentina, 2010, pp. 4740–4743.

[7]. V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Adaptive watermarking algorithm using sorting and prediction,” IEEE Trans. Circuit Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

[8]. G. Coatrieux, C. Le Guillou, J.-M. Cauvin, and C. Roux, “Adaptive watermarking for knowledge digest embedding and reliability control in medical images,” IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2, pp. 158–165, Mar. 2009.