

Digital Image Authentication by DCT and RPM Based Watermarking

Kuldeep Singh¹, Prof. Ashish Mishra²

¹*M.Tech. Scholar Department of CSE, SISTech., Bhopal, M.P., India*

²*Department of CSE, SISTech., Bhopal, M.P., India*

Abstract-- Digital watermarking has been proposed as a viable clarification to the necessity of copyright protection and authentication of multimedia system information in a networked environment, since it makes possible to identify the author, owner, distributor or approved client of a document. This paper elaborates quality of discrete cosine transform for image watermarking, DCT based image watermarking technique, classification and analysis of discrete cosine transform primarily based watermarking techniques. Discrete cosine transform and wavelet based mostly image watermarking ways that. It'll be useful for researchers to implement effective image watermarking methodology .the propose algorithmic program to supply information privacy and additional authentication. Watermark embedding into host image. Propose algorithmic program also have good performance in hardiness, reliable and computing complexity.

Keywords-Watermarking, Visibility, Security, Robustness, Discrete cosine transform, Reversible data hiding.

I. INTRODUCTION

Digital Image Watermarking is a newly and future reputable field in engineering. It is known as the process of fixing the uniqueness of a copyright holder within a digital image watermarking work that is very difficult and impossible to remove. Digital watermarking is the process of embedding information into a digital signal. The signal may be pictures, audio or video, for example. If the signal is unoriginal, then the material is also carried in the copy. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which classifies the owner of the media. When a television broadcaster adds its symbol to the corner of communicated video, this is also a visible watermark. In invisible watermarking [1], information is added as digital data to audio, picture or video, but it cannot be apparent as such. An important application of invisible watermarking is to copyright protection systems, which are intended to avoid or deter illegal copying of digital media.

A characteristic of the best watermark should be goal at maintaining the watermark very robust under wicked attacks in real and spectral domain. At the same time, the watermark should not transform the content of the work but slightly (it should be minute or almost negligible by human senses), and it should be practically impossible for illicit users to remove or alter it. By means of watermarking the work is still easy to get to, but everlasting marked.

For grey-level or color-image watermarking, watermark embedding techniques are planned to insert the watermark straight into the original image data, such as the luminance or color components or into some transformed version of the innovative data to take advantage of perceptual properties or robustness to particular signal manipulations. Requirements for image watermarking include imperceptibility, robustness to common signal processing operations, and capacity. Mutual signal processing operations which the watermark should survive include compression, filtering, rescaling, cropping, analog or Digital and Digital or Analog conversion, geometric distortions, and additive noise. Digital image processing goes through the process whose input and output, both are images [2]. For achieving the better quality of the watermark the PSNR is used. Watermark is used for authentication, identification and preservation of originality of an image. There are two concepts watermarking and fingerprinting. Watermarking is for adding or embedding some context to the base image which is used for its identification and authentication. While fingerprinting traces the source of copying the image. Fingerprinting, thus, provides necessary information to enable taking action against piracy of the image or context. On the other hand, watermarking is used for restricting the piracy. Digital watermarking is done in the image, audio, video or other multimedia files. It is also used in forensic department in various ways. In other words, we can also say that fingerprints are embedded in an image by using watermark algorithm. Once the authorized copy of digitized context is available, to identify the series guilty, which created those unauthorized copy can be identified. This is also called forensic watermarking. Another, concept is Visual Cryptography Scheme. In this process encoded secret image are distributed into n number of shared participants [3]. This is used for watermarking purpose. Reversible Watermarking is also called lossless or distortion free watermarking. It completely removes the watermarking and exactly recovers the original signal

image [4]. In this paper, we have used the concept of visual cryptography, reversible watermarking in small picture like logo or file containing signature of a person. If we can find robust methods for watermarking then in digital media we can authenticate signatures, logo and many important documents.

1.1 Classification of Digital Image Watermarking

Digital image watermarking has constituted into three classes consequently supported the various watermarks:

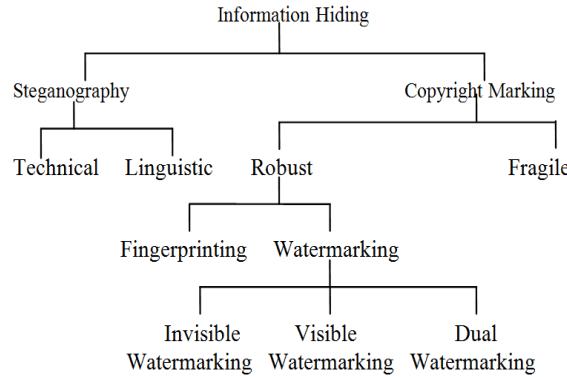


Fig1. Categories of Information Hiding

- Visible Watermarks-** These are the logos concept enlargement. These sorts of watermarks are solely applicable for the pictures. A transparency criterion evolves once these logos are embedded into the still pictures. The watermarks happiness to the current class is exhausting to get rid of or alter once cropping attack falls.
- Invisible Watermarks-** As the name clears its which means the watermark should be hidden from the surface world. The detection of those sorts of watermark will solely be done by the upper authority or agencies. The watermarks happiness to the current class is utilized by the author authentication or creator or possession and for locating the unauthorized person.
- Fragile Watermarks-** These are known as by the name of the tamper proof watermarks. The watermarks happiness to the current class is shattered by the info management. The image while not watermark indicates that a trial has been created on the initial image and forgery has evolved within the absence of watermark.

1.2 On The premise of Document

A digital watermarking is image, audio, video, text, software, databases and holographs digital documents for watermarking is widely divided into various categories like.

- Digital Image Watermarking-** An image available in the internet or in primary and secondary storage.
- Digital Video Watermarking-** A video sequence consists of still images. The watermarking is carried out in each image of video and thus whole video is watermarked.
- Digital Audio Watermarking-** Audio watermarking is based on embedding one or more key dependent watermark signals below the audibility threshold.
- Software Watermarking-** Software watermarking is a technique used to protect software from piracy. Software watermarking embeds a unique identifier watermarking S into program P. If S uniquely establishes the author of P then S is considered a copyright notice.
- Text Watermarking-** Text is available in digital media are also prone to be copied. Therefore, hidden text or key is inserted in between letters or words in text. When copied the hidden words are revealed and entire text will changed and become unreadable.
- Database Watermarking-** Databases are also watermarked in order to protect its unauthorized usage.
- Holographs-** Holographs are used for logos and copyright authentication. It is watermarked using 3D visualization.

1.3 On The premise of robustness

Robust method is for identification where semi fragile and fragile is for authentication [5]. In other words, we can say that robust watermarking is also visible. It is used for identification. Semi fragile and fragile is for covert watermarking. Generally, covert watermarking is used for authentication and forensic watermarking. Using covert watermarking unauthorized copying can be traced out from some hidden program embedded in the base image. Watermarking is a valid and useful method for preserving authenticity and

authorizing the use of digital image. There are various method of watermarking. Each method has its own pros and cons. Performance of watermarking system is based on three criteria i.e. Invisibility, Robustness and Capacity [6]. Invisibility means watermark should embedded in such a way that it is not identified by unauthorized uses. Robustness is concerned about tracing or tampering of watermark by attacker. A good watermark should be against filtering process, noise addition, lossy compression, geometry transformation such as rotation, scaling and translation. Capacity means maximum amount of information the embedded watermark can carry and those information can be detected reliably for the purpose of copyright protection and authentication.

An image authentication system should satisfy following criteria

1. **Sensitivity-** The system must be sensitive to malicious attacks, tampering, deletion or reduction of watermarking .Modification includes cropping or altering specific part of image.
2. **Tolerance-** The system must tolerate some loss of information and generally non-malicious manipulation.
3. **Reconstruction of altered region-** The system may need the ability to restore, even partially, altered or destroyed regions.
4. **Localization of altered region-** The system should be able to locate precisely any malicious alteration made to the image and verify other areas as authentication. [7]

1.4 On The premise of Applications

There are diverse applications of image watermarking. These are listed as follows

1. **Copyright Protection-** When a new image is created, copyright information can be inserted as a watermark. In case of dispute of ownership, this watermark can provide evidence.
2. **Broadcast Monitoring-** This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.
3. **Tamper Detection-** Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted.
4. **Authentications and Integrity Verification-** Content authentication is able to detect any change in digital content. This can be achieved through the use of fragile or semi-fragile watermark which has low robustness to modification in an image.
5. **Fingerprinting-** Fingerprints are unique to the owner of digital content and used to identify when an illegal copy appeared where and which point of leakage.
6. **Content Descriptions-** This watermark can contain some detailed information of the host image such as labeling and captioning. For this kind of application, capacity of watermark should be relatively large and there is no strict requirement of robustness.
7. **Covert Communications-** It includes exchange of messages secretly embedded within images. In this case, the main requirement is that hidden data should not be identified.
8. **Digital Forensics-** It includes application in forensics science to assure that digital image is doctored or not.
9. **Device Control-** In this scenario, the media player is controlled by the digital watermark. If the desired copyright information cannot be detected from the host contents, the player refuses to play and record the unauthorized contents. If all device manufacturers abide to these device control policies, the piracy can be discouraged. However, in real scenarios, it is difficult to implement these policies due to the difficulty of global cooperation [8].

1.5 On The premise of Techniques

There are several transform domain watermarking schemes available in the literature

1. **Discrete Cosine Transform-** The popular block-based DCT transform segments image non-overlapping blocks and applies DCT to each block. These results in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub- band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low- frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression [9].
2. **Discrete Wavelet Transform-** Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image

watermarking and gives advantages of using DWT as against other transforms. For 2-D images, applying DWT corresponds

3. **Singular Value Decomposition-** SVD as a general linear algebra technique is used in a variety of applications. SVD is optimal matrix decomposition in a least square sense packing the maximum signal energy into a few coefficients as possible (Ganic *et al* 2003) and (Liu& Tan 2002). The SVD theorem decomposes a digital image A of size $M \times N$, as: $A = USV^T$, (1) where U and V are of size $M \times M$, and $N \times N$ respectively. S is a diagonal matrix containing the singular values. In watermarking trial, SVD is applied to the image matrix; then watermark resides by altering singular values (SVs)" [10].

1.6 Attacks on Watermarked Image

Attacks on watermarked image are distortions in watermarked image. These attacks may be intentional or unintentional. An image watermarking method can be judged against such relevant attacks. The attacks are broadly classified as signal processing attacks and geometric attacks

1. Signal Processing Attacks

Signal processing attacks are also called as image processing attacks or non geometric attacks. These common signal processing attacks may include compression of image, addition of noise like Gaussian or salt and pepper noise, gamma correction, filtering, brightness, sharpening, histogram equalization, averaging, collusion, printing, scanning etc.

2. Geometric Attacks

Geometric attacks include basic geometric transformations in an image. These include geometrical distortions like rotation, scaling, translation, cropping, row-column blanking, warping etc. Geometric attacks attempt to destroy synchronization of detection thus making the detection process difficult and even impossible

II. LITERATURE SURVEY

Jeng-Shyang Pan, Hao Luo, and Zhe-Ming Lu(2006), a lossless watermarking scheme for halftone image Authentication[11] . Authentication watermark is a hidden data inserted into an image that can be applied to detect any unauthorized change of the image. Here a block-based method is used.In this, 512×512 halftone images are selected to test the effectiveness of the method. The halftone image is divided into 4×4 blocks. The original watermark, i.e. the hash sequence of image, is computed by the MD5 hash function After translating the string into 0-1 sequence, 128-bit digest is obtained. In authentication, the watermark is extracted from the watermarked image, and the hash sequence is computed from the restored image. When the two sequences are equal, it is confirmed that the watermarked image has suffered no alteration. Both of them are equal to the original watermark.M. Barni *et al.* [12] have developed an improved wavelet-based watermarking through pixel-wise masking. It is based on masking watermark according to characteristics of HVS. The watermark is adaptively added to the largest detail bands. The watermark weighing function is calculated as a simple product of data extracted from HVS model. The watermark is detected by correlation.

M. Kim, D. Li, and S. Hong(2013),A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contents[13]. In this paper, algorithm for embedding watermarking is presented. Firstly, the original image is compressed into JPEG image and generates the watermark by using the 2D barcode and scrambling. Secondly, JPEG image is decayed into 3 subbands:H, V and D by using 2D DWT. Thirdly, the DFRNT(discrete fractional random transform) is performed on the sub-band coefficients. And then, watermark image is embedded into the sub-band coefficient value using quantization technique. Fourthly, the inverse DFRNT and inverse DWT is performed and lastly watermark JPEG image is obtained. The proposed algorithm has good invisibility and extraction performance, and ensures robustness

Victor *et al.* [14] have developed an algorithm that relies upon adaptive image watermarking in high resolution sub-bands of DWT. Weighting function is the product expression of data extracted from the HVS model.

N. Kaewkamnerd and K.R. Rao [15] developed a wavelet based image adaptive watermarking scheme. Embedding is performed in the higher level sub-bands of wavelet transform, even though this can clearly change the image fidelity. In order to avoid perceptual degradation of image, the watermark insertion is carefully performed while using HVS.Chih-Chin Lai and Ching-Chin Tsai[16], proposed Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. A hybrid image-watermarking technique based on DWT and SVD has been presented, where the watermark is embedded on the singular values of the cover image's DWT sub band. The main objective of developing this technique is to satisfy both imperceptibility and robustness.

Wang Hongjun, Li Na[17], have proposed a DWT based method in which watermark was embedded in middle frequency coefficient using α as flexing factor with $\alpha = \beta |m|$,where m is mean value of all coefficients watermarking embedded. But this method doesn't provide enough security.

Sasmita Mishra et.al. [18], described a survey on digital watermarking techniques, the idea behind this survey is to study different kind of watermarking techniques and present a robust watermark data using DWT and introduce fragile and semi-fragile watermarking techniques. Ali Al-Haj(2007), —Combined DWT-DCT Digital Image Watermarking[19] In this paper, Watermarking is done by embedding the watermark in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of the two transforms improves the watermarking performance considerably when it is compared to the DWT-Only watermarking approach.

Vinita Gupta, Atul Barve(2014), —Robust and Secured Image Watermarking using DWT and Encryption with QR Codes[20]. In this Paper, algorithm for embedding watermarking is presented by using DWT and encrypted with QR codes. Here cover image is selected and DWT is applied on it. A key K is selected to generate the QR code as secret key. QR code and watermark image is encrypted by using XOR operation. Then the encrypted watermark is embedded into the cover image and inverse DWT is applied on the embedded watermark image. For extraction, simply apply the DWT on the cover image. This algorithm is quite simple because of the use of simple X-OR operation for encryption. This algorithm is suitable on different kind of attacks on watermarked images like JPEG Compression, Poisson Noise Attack, Salt & Pepper Noise and Gaussian Noise.

To measure the quality of a watermarked image, the peak signal to noise ratio is typically used. The mentioned PSNR values are also given for a comparative analysis.

Purpose	Method	Performance
Verification of Military maps, great works of art, medical images etc. using Lossless Watermarking method for Halftone Images [11]	Digital Half toning on multi-toning images with hash chain of original image with MD5 hash function	Fragile watermarking low quality and Original image can be completely recovered by reverse process of watermarking application. Only secret key is to be saved.
Digital Image Watermarking for compacted image format (such as JPEG format) used on the web [13]	Robust and Invisible digital image watermarking algorithm through a 2D barcode and scrambling method based on DWT DFRNT transform. The Watermark extraction process is the inverse of watermark embedding process	PSNR ratio is approx. 40 DB for various images.
Combined DWT-DCT Digital Image Watermarking [19]	A combined DWT-DCT (Discrete Wavelet Transform and the Discrete Cosine Transform) digital image watermarking algorithm	Performance of the watermarking two transforms algorithms that were based solely on the DWT transform. Imperceptibility performance was better and the robustness got improved. PSNR for different sub-bands (HL2 HH2) is approx. 97 DB.
Colour Image Watermarking encrypted in QR code [20]	XOR operation for encryption of QR code and watermark, after applying DWT on the Cover image	This technique is robust and enhances the security. It does not change the quality of watermarked image. Simple XOR operation is used for encryption. PSNR ratio on various images is approx. 62 DB
M. Barni et al. [12] have developed an improved wavelet-based watermarking through pixel-wise masking	DWT & HVS	Wavelet-based watermarking through pixel-wise masking. It is based on masking watermark according to characteristics

		of HVS
Victor et al[14]	DWT & HVS	Developed an algorithm that relies upon adaptive image watermarking in high resolution sub-bands of DWT
N. Kaewkamnerd and K.R. Rao[15]	DWT & HVS	Wavelet based image adaptive watermarking scheme using HVS
Chih-Chin Lai and Ching-Chin Tsai[16]	DWT & SVT	A hybrid image-watermarking technique based on DWT and SVD has been presented, where the watermark is embedded on the singular values of the cover image's DWT sub band
Wang Hongjun, Li Na[17]	DWT	Proposed a DWT based method in which watermark was embedded in middle frequency coefficient
Sasmita Mishra et.al. [18],	DWT	Described a Survey on Digital Watermarking techniques

III. IMPLEMENTATION ENVIRONMENT AND RESULT DISCUSSION

MATLAB is a high-level technical compute language and interactive environment for algorithm development, data visualization, records analysis, and numeric computation Matlab is a software program that allows you to do data manipulation and visualization, calculations, math and programming. It can be used to do very simple as well as very sophisticated tasks. Image Processing Toolbox provides a comprehensive set of reference-standard algorithms and graphical tools for image processing, analysis, visualization, and algorithm development. You can perform image enhancement, image declaring, feature detection, noise decrease, image segmentation, spatial transformations, and image registration. Many functions in the toolbox are multithreaded to take benefit of multicore and multiprocessor computers.

A) PERFORMANCE MATRICES

1. Recover time: The time which is taken to recover the watermark image $W M(i, j)$ into original image $O(i, j)$ then that time is called recover time .

2. PSNR: The term peak signal-to-noise ratio is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.

PSNR =10log10 (MAX^2 /MSE)

MAX is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. MSE is the Mean Square Error between the original $O(i, j)$ and the watermarked image $W M(i, j)$

B) RESULT ANALYSIS

The following steps are used in this algorithm: Load an original image and host image in MATLAB. Divide the host image into small blocks and convert into 8x8 matrixes. Embed the watermark data into the divided small blocks in host image and row wise revs bits replace into the host image. Get watermark image Apply attack on watermark image Recover original image Calculate parameter and End. The following experimental

1. Coefficient Replacement using DCT Technique

Experimental results of the proposed data embedding and Watermark Image attack Using Superposition attack, Noise attack, smoothing attack, JPEG attack extraction are presented and discussed in this section. Two 8-bit images with a size of 64×64 were simulated. Undetectable or transparency can be obtained from the PSNR of embedded image. The original image “Nature (512×512)” with a size of, it cannot be found

any difference by human vision. The watermarked images attacked by Superposition attack, Noise attack, smoothing attack, JPEG attack method with quality less and cropping and painting. Most approaches embedded the hidden data into the middle band of the DCT block. In the proposed method, the bit stream is hidden in the lower band.

2. Row Bits replace using RPM

In this section, we use the classical gray-level image, Nature image (512×512 , 8 bits per pixel) as host image and embed a watermark (64×64 , 8 bits per pixel) into the host image. We can get an error image $D(i, j)$ by calculating the difference of the original host image $I(i, j)$ and the recovered image $I'(i, j)$. We know that pixels are changed in the embedding and extraction process. By calculating the PSNR ratio of changed pixels to the original image size and recover image size, surely, the watermark cannot be completely extracted from the host image. The performance evaluation of DCT and RPM is summarized in the given below table.

Table 1. Performance Evaluation of DCT and RPM

Attack	Experimental Image	Recover Time (in sec)		PSNR (in db)	
		DCT	RPM	DCT	RPM
Superposition	 512 x 512 JPG	1.0452	0.8218	135.0499	143.7961
Noise		1.248	0.9466	473.2204	869.4743
JPEG Attack		3.6036	3.3646	2.9277	8.3798
Smoothing		0.9828	0.8374	2.9202	8.343

1. Recover Time

Watermark as a SISTech college logo image 64×64 sizes as an original image extract in Nature image 512×512 as a host image. In this process recover time in RPM is less compare to DCT.

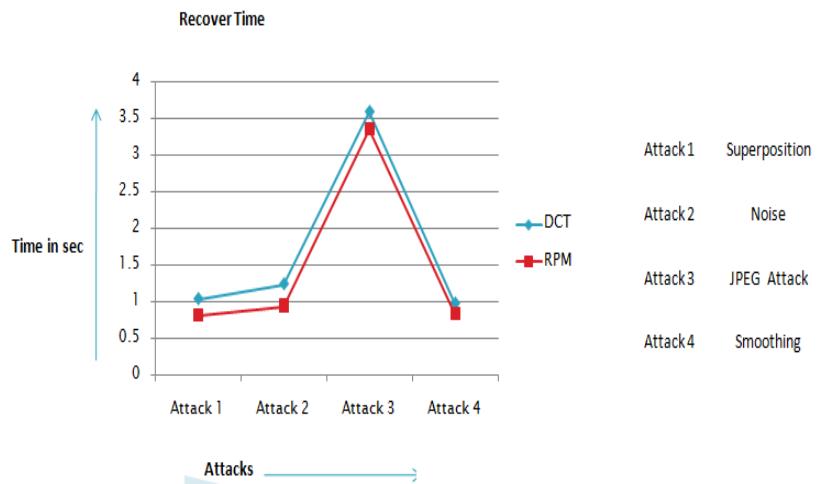


Fig2. Recover time analysis between DCT and RPM

2. Average Recover Time

Watermark as a SISTech college logo image 64×64 sizes as an original image extract in Nature image 512×512 as a host image. In this process average recover time in RPM is less compare to DCT.

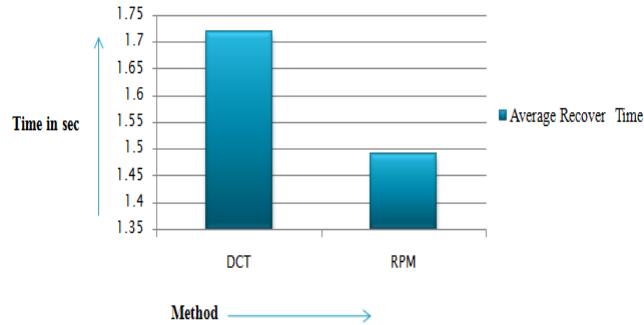


Fig3. Average Recover time analysis between DCT and RPM

3. PSNR

SISTech college logo image 64x64 sizes as an original image and Nature image 512x512 as a host image embedding and generated watermark image. In this process embedding time in RPM is less compare to DCT. Watermark as a SISTech college logo image 64x64 sizes as an original image extract in Nature image 512x512 as a host image .In this process recover time in RPM is less compare to DCT. In this process PSNR value is high in RPM as compare to DCT.

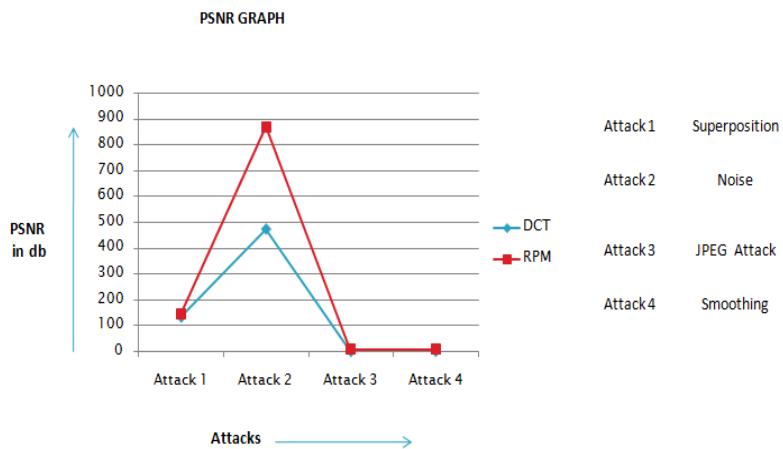


Fig4. PSNR analysis between RPM and DCT

4. Average PSNR

SISTech college logo image 64x64 sizes as an original image and Nature image 512x512 as a host image embedding and generated watermark image. In this process embedding time in RPM is less compare to DCT. Watermark as a SISTech college logo image 64x64 sizes as an original image extract in Nature image 512x512 as a host image .In this process recover time in RPM is less compare to DCT. In this process average PSNR value is high in RPM as compare to DCT.

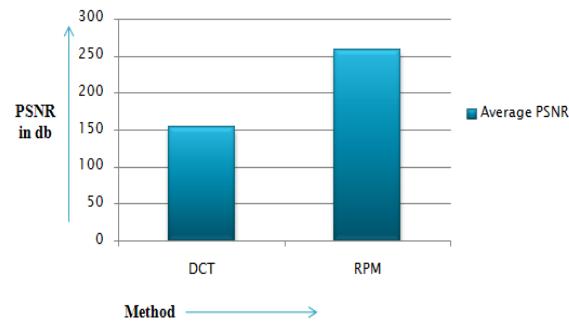


Fig5. Average PSNR analysis between RPM and DCT

IV. CONCLUSION

In this thesis, a RPM and the DCT algorithms was taken up with an objective of developing watermarking algorithms for images. Implementation results prove that this algorithm provide data privacy and more authentication .The original host image and data image in which PSNR of RPM is greater than DCT. RPM also have good performance in robustness, reliable and computing complexity. Fast and Suitable for robustness against DCT. The developed watermarking method is resistant against various attacks.

REFERENCE

- [1] A.B. Watson, G.Y. Yang, J.A. Solomon, and J. Villasenor, "Visibility of wavelet quantization noise" IEEE Trans. Image Processing, vol. 6, pp. 1164-1175, Aug. 1997
- [2] Rafael C. Gonzalez, Richard E. Woods, Steven, L. Eddins, "Digital Image Processing Using MATLAB" Pearson Education, 2007.
- [3] IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, June 2011 307 Embedded Extended Visual Cryptography Schemes Feng Liu and Chuankun Wu.
- [4] IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, September 2011 873 Improved Embedding for Prediction- Base Reversible Watermarking Dinu Coltuc, Member, IEEE.
- [5] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.Mohammad Ali Akhaee,
- [6] A Survey of RST Invariant Image Watermarking Algorithms, Dong Zheng, Yan Liu, Jiyang Zhao, and Abdulmotelab El Sadikk ,University of Ottawa ACM Computing Surveys, Vol. 39, No. 2, Article 5, Publication date: June 2007.
- [7] A Survey Watermarking Algorithm for image Auhentication, EURASIP Journal on Applied Signal Processing 2002: Hindawi Publishing Corporation by Christian Ley & Jean Luc Dugeley.
- [8] Jidong Zhong, (2006) "Watermark Embedding and Detection" , PhD Thesis.
- [9] Navnidhi Chaturvedi1, Dr.S.J.Basha2, "Comparison of Digital Image watermarking Methods DWT & DWT -DCT on the Basis of PSNR",International Journal of Innovative Research in Science, Engineering and Technology Vol. 1, Issue 2, December 2012 IJIRSET www.ijirset.com Page no 147.
- [10] A Mansouri, A Mahmoudi Aznaveh And F Torkamani Azar , "SVD-based digital image watermarking using complex wavelet transform"Vol. 34, Part 3, June 2009, pp. 393–406.
- [11] Jeng-Shyang Pan, Hao Luo, and Zhe-Ming Lu, —A Lossless Watermarking Scheme for Halftone Image Authentication, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006
- [12] Barni M, Bartolini F, Piva, "An Improved Wavelet Based Watermarking Through Pixelwise Masking", IEEE transactions on image processing, Vol. 10, 2001 pp.783-791.
- [13] M. Kim, D. Li, and S. Hong, —A Robust and Invisible Digital Watermarking Algorithm based on Multiple Transform Method for Image Contentsl :Proceedings of the World Congress on Engineering and Computer Science 2013 Vol I WCECS 2013, 23-25 October, 2013, San Francisco, USA
- [14] Victor V., Guzman, Meana, "Analysis of a Wavelet-based Watermarking Algorithm", IEEE Proceedings of the International Conference on Electronics, Communications and Computer, 2004, pp. 283-287.
- [15] N. Kaewkamnerd and K.R. Rao, "Wavelet Based Image Adaptive Watermarking Scheme", IEEE Electronic Letters, Vol. 36, Feb. 2000, pp.312-313.

- [16] Chih-Chin Lai, Cheng-Chih Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Transaction on Instrumentation and Measurement", vol. 59, no. 11, November 2010.
- [17] Wang Hongjun, Li Na," An algorithm of digital image watermark based on multiresolution wavelet analysis", International Workshop on VLSI Design and Video Technology, Proceedings, pp: 272- 275, 28-30 May 2005.
- [18] Sasmita Mishra, Amitav Mahapatra, Pranati Mishra, "A Survey on Digital Watermarking Techniques", International Journal of Computer Science and Information Technologies, Vol. 4(3), 2013, 451-456.
- [19] Ali Al-Haj, Combined DWT-DCT Digital Image Watermarking, Journal of Computer Science 3 (9): 740-746, 2007.
- [20] Vinita Gupta, Atul Barve, —Robust and Secured Image Watermarking using DWT and Encryption with QR Codes, International Journal of Computer Applications (0975 – 8887)Volume 100 – No.14, August 2014.