IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. I (Jul.-Aug. 2016), PP 37-42
www.iosrjournals.org

A Survey on Digital Image Authentication by DCT and RPM Based Watermarking

Kuldeep Singh[1], Prof. Ashish Mishra[2]
[1]*M. Tech. Scholar Department of CSE, SISTech., Bhopal, M.P., India*
[2]*Department of CSE, SISTech., Bhopal, M.P., India*

Abstract: *An image watermarking, data is embedded into cover media to prove ownership. Various Watermarking techniques are proposed by several authors within the last many years that embody spatial domain and transform domain watermarking. This paper elaborates quality of discrete cosine transform for image watermarking, DCT primarily based image watermarking method, classification and analysis of discrete cosine transform based mostly watermarking techniques. The aim of this paper is to produce a comprehensive review of the existing literature available on discrete cosine transform and wavelet based mostly image watermarking ways. It'll be helpful for researchers to implement effective image watermarking methodology.*

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 everlastingly 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:

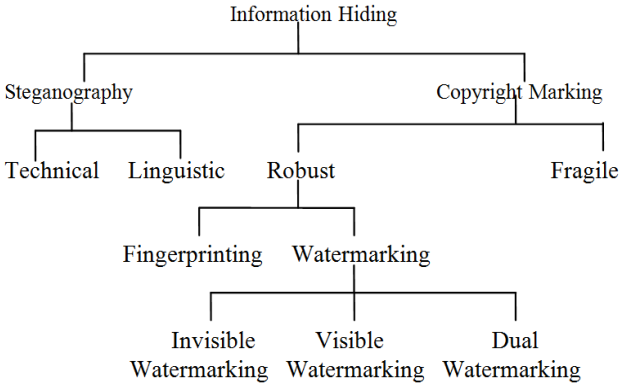

Fig1. Categories of Information Hiding

1. **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.
2. **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.
3. **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.

1. **Digital Image Watermarking**- A picture offered within the net or in primary and storage device.
2. **Digital Video Watermarking**- A video sequence consists of still pictures. The watermarking is applied in every image of video and therefore whole video is watermarked.
3. **Digital Audio Watermarking**- Audio watermarking is predicated on embedding one or a lot of key dependent watermark signals below the perceptibility threshold.
4. **Package Watermarking-** Package watermarking may be a technique accustomed shield package from piracy. Package watermarking embeds a novel symbol watermarking S into program P. If S uniquely establishes the author of P then S is taken into account a copyright notice.
5. **Text Watermarking**- Text is accessible in digital media are liable to be derived. Therefore, hidden text or key's inserted in between letters or words in text. Once derived the hidden words area unit disclosed and full text can modified and become unclear.
6. **Information Watermarking**- Databases are watermarked so as to shield its unauthorized usage.
7. **Holographs**- Holographs area unit used for logos and copyright authentication. It is watermarked exploitation 3D rational image.

1.3 On the premise of Robustness

Robust technique is for identification wherever semi fragile and fragile is for authentication [5]. In alternative words, we are able to say that sturdy watermarking is additionally visible. it's used for identification. Semi fragile and fragile is for covert watermarking. Generally, covert watermarking is employed for authentication and forensic watermarking. using covert watermarking unauthorized repeating may be copied out from some hidden program embedded within the base image. Watermarking may be a valid and helpful technique for protective believability and authorizing the employment of digital image. There are varied technique of watermarking. Every technique has its own professionals and cons. Performance of watermarking system is predicated on 3 criteria i.e. invisibleness, robustness and capability [6]. Invisibleness means that watermark ought to embedded in such how that it's not known by unauthorized uses. Robustness cares bothered about tracing or

change of state of watermark by attacker. A good watermark should be against filtering method, noise addition, lossy compression, geometry transformation like rotation, scaling and translation. Capability means that most quantity info| knowledge the embedded watermark will carry and people information may be detected dependably for the purpose of copyright protection and authentication.

An image authentication system should satisfy following criteria

1. **Sensitivity**- The system should be sensitive to malicious attacks, tampering, deletion or reduction of watermarking. Modification includes cropping or neutering specific a part of image.
2. **Tolerance**- The system should tolerate some loss of knowledge and usually non-malicious manipulation.
3. **Reconstruction of altered region**- The system might have the power to restore, even part, altered or destroyed regions.
4. **Localization of altered region**- The system ought to be ready to find exactly any malicious alteration created to the image and verifies different areas as authentication. [7]

1.4 On the premise of Applications

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

1. **Copyright Protection**- When a replacement image is made, copyright info may be inserted as a watermark. Just in case of dispute of possession, this watermark will give evidence.
2. **Broadcast monitoring**- This application is employed to monitor unauthorized broadcast station. It can verify whether the content is actually 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 sure.
4. **Authentications and Integrity Verification**- Content authentication is able to detect any modification in digital content. This may be achieved through the employment of fragile or semi-fragile watermark that has low robustness to modification in an image.
5. **Fingerprinting**- Fingerprints are unique to the owner of digital content and used to establish when an illegal copy appeared wherever and that purpose of leakage.
6. **Content Descriptions**- This watermark will contain some elaborated info of the host image like labeling and captioning. For this kind of application, capability of watermark should be comparatively giant and there is no strict demand of robustness.
7. **Covert Communications**- It includes exchange of messages secretly embedded at intervals pictures. in this case, the most demand is that hidden information shouldn't be known.
8. **Digital Forensics**- It includes application in forensics science to assure that digital image is doctored or not.
9. **Device Control**- In this situation, the media player is controlled by the digital watermark. If the specified copyright info can't be detected from the host contents, the player refuses to play and record the unauthorized contents. If all device manufacturers abide to those device control policies, the piracy may be discouraged. However, in real situations, it's tough to implement these policies due to the problem of worldwide cooperation [8].

1.5 On the premise of Techniques

There are many transform domain watermarking schemes accessible within the literature

1. **Distinct circular function transform**- The well-liked block-based DCT transform segments image non-overlapping blocks and applies DCT to every block. These results in giving 3 frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub- band. DCT-based watermarking is predicated on 2 facts. the primary fact is that a lot of of the signal energy lies at low-frequencies sub-band that contains the foremost necessary visual components of the image. The second fact is that top frequency elements of the image are sometimes removed through compression and noise attacks. The watermark is thus embedded by modifying the coefficients of the center frequency sub-band so that the visibility of the image won't be affected and the watermark will not be removed by compression [9].
2. **Distinct wave transform**- Distinct wave Transform (DWT) is a mathematical tool for hierarchically moldering a picture. it's helpful for process of non-stationary signals. The transform is predicated on tiny waves, known as wavelets, of variable frequency and restricted length. wave transform provides each frequency and spatial description of a picture. in contrast to standard Fourier transform, temporal info is maintained during this transformation method. Wavelets are created by translations and dilations of a fixed operate known as mother wave. This section analyses quality of DWT for image watermarking and provides blessings of using DWT as against alternative transforms. For 2-D pictures, applying DWT corresponds

3. **Singular worth Decomposition**- SVD as a general algebra technique is employed in a very form of applications. SVD is perfect matrix decomposition in a very least square sense packing the utmost signal energy into many coefficients as attainable (Ganic et al 2003) and (Liu& Tan 2002). The SVD theorem decomposes a digital image A of size M × N, as: A = USVT , (1) wherever U and V are of size M×M, and N ×N severally. S may be a square 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 could also be intentional or un-intentional. an image watermarking technique may be judged against such relevant attacks. The attacks are generally classified as signal processing attacks and geometric attacks

1. Signal processing Attacks

Signal processing attacks are known as image processing attacks or non geometric attacks. These common signal processing attacks might embody compression of image, addition of noise like mathematician or salt and pepper noise, gamma correction, filtering, brightness, sharpening, bar chart leveling, averaging, collusion, printing, scanning etc.

2. Geometric Attacks

Geometric attacks include basic geometric transformations in a picture. These include geometrical distortions like rotation, scaling, translation, cropping, row-column blanking, distortion etc. Geometric attacks attempt to destroy synchronization of detection therefore creating the detection process difficult and even not possible

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. Expected Outcome

1. It is reliable digital image.
2. It is provide good authentication.
3. It is good robustness and ownership.
4. It is providing secures in data hiding.

IV. Conclusion

This paper focuses on data hiding and this paper focuses on digital image in frequency domain and digital watermarking techniques like DCT, DWT SVD their advantages, disadvantages and applications. Both embedding and extraction of watermark is being done using the techniques. For checking the robustness of these methods various attacks on watermarked images are performed Noise, Rotation, Gaussian noise and unsharping. DCT-DWT, SVD shows better results among these methods compared in terms of PSNR after attack on watermarked image.

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 Aurhentication, 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 Contents‖ :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 Transcation 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.