International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

# A STUDY ON DIGITAL WATERMARKING AND APPLICATION FOR COPYRIGHT PROTECTION IN DIGITAL IMAGE

**Swati Mishra [1], G.R Mishra [2], Rajinder Tiwari [3]**

[1, 2, 3] *Department of Electrical and Electronics Engineering*

*Amity School of Engineering and Technology, Amity University, Lucknow, (India)*

## ABSTRACT

*With the advancement in the field of Information and Communication Technology, most of the information is kept in electronic form. The concept of keeping information electronically facilitate the user with easy access, contradictorily at the same point security of the information is fundamental issue nowadays. "Security" in the data transfer has been major area of concern in the past few decades and the threat of attack on the security haunt the both, receiver and sender. In today's scenario data security is the necessity. There are numerous encryption method available which can be employed to secure digital information over the network. In this paper we have given detailed study of digital watermarking and its application for copyright protection in digital image describing architecture, attributes and algorithms of digital watermarking.*

***Keywords: Copyright Protection, Digital watermarking, Information Security***

## I. INTRODUCTION

It has been witnessed that the recent growth in the segment of digital technologies accompanied by the growing inter-related high speed network and diminution in the cost of high performance digital devices have made distribution of the digital content ,an easy task and most common practice. Beside the enormous potential for business content suppliers, the threat of effortless illegitimate copying and distribution of the same has been brought as a result of the development in digital content distribution [7].

Among the solution of the issue concerning illegal copying and distribution of the digital content, promising solution is what we say it as Digital Rights Management abbreviated as DRM.DRM includes wide range of access control technologies which control the use, modification as well as distribution of the copyrighted works [3].DRM improves the hold of the right holder over their intellectual property assets. Due to widespread use of internet and advancement in the streaming media, the distribution of the digital content over the internet has effortless. Through DRM, the security and limited circulation of the digital information can be assisted[4].

There are two components in the DRM: 1.group of technologies like authentication, access control, key management, encryption, and digital watermarking 2.collection of technologies which ensures to convey copyright permission in 'right expression languages' [12].The primary purpose of the DRM systems are to protect the copyrights. With the DRM systems implementation of the copy restriction is possible[5].

Copyright protection which are meant to resolve the disputes over the ownership after buying and selling of the digital content, takes active part in the DRM. There is a need to authenticate the ownership document prior to the sale of the digital content to the buyer, and to authenticate the buyer as well is the necessary[9].

Illegal copying, modification and distribution of the digital image has become a concern due to development in the image processing tools. Protection of the digital image has become a prime concern in today's world of fast growing internet [10].But the DRM is not accepted universally as opponents of the DRM argues that it detain the typical use of digital data, which is conventionally legal. Thus DRM is a controversial policy [11].For the ownership identification of the digital image and copyright protection, the technique of digital watermarking has been evolved.

The rest of the paper is organized as follows. Section II describes attributes and classification of digital watermarking, followed by Section III in which architecture and algorithms of digital watermarking have been discussed. In Section IV various previous works in Digital watermarking and its application for copyright protection hasbeen briefed. Section V gives the conclusion of the study carried out.

## II. DIGITAL WATERMARKING TECHNIQUE

Digital watermarking is defined as a process of embedding the data into the multimedia element such as image, video and audio data. Protection against illegitimate replication and alteration of digital image is achieved by use the digital watermarking technique[8].In digital watermarking, the term "digital watermark" has its importance .and was coined by Andrew Tirkel and Charles Osborne. This is the marker which we embed in multimedia element like image, video and audio data. In future, for the various purpose like access control, broadcast monitoring and copyright protection, the digital watermark (embedded data) can be unearthed. Through certain algorithms we can embed copyright information into the multimedia data, the information may contain any text with special resemblance,and it can be either image or company logo and so on. The information embedded in the multimedia content is usually indiscernible, which can be only uncovered through number of distinct detectors [16].

In digital watermarking the user is allowed to view and access the multimedia content but it limit the user to make unauthorized use of digital information. This attribute of limiting unauthorized use of the digital content distinguish digital watermarking from the encryption [21].

### 2.1 Attributes of digital watermarking

In accordance with the type of application for which we are using digital watermarking the requirement of the system varies. Robustness, security, verifiability and non-perceptibility are primary characteristics of digital watermarking. The watermark embedded in the digital data should be **robust** enough so that it survive even after many attacks and processing. It should not be recognizable in the multimedia contents or in other words they should be **non-perceptible**. Watermarks must achieve the task of providing evident of ownership of copyright protected content. Watermark information can be extracted and even modified by the authorized user and thus fulfills the requirement **(security and verifiability)** of digital watermarking techniques [16].

International Journal of Electrical and Electronics Engineers
Vol. No.8 Issue 01, January-June 2016
www.arresearchpublication.com
IJEEE
ISSN 2321 - 2055

### 2.2 Classification of Digital Watermarking

Digital watermarking can be classified into many aspects depending upon the factor of classification. According to its attributes it is categorized into fragile watermarking and robust watermarking. Robust watermarking is used to sign copyright information in digital data and after many attacks it survives to provide the certification. Unlike robust watermarking, fragile watermarking is sensitive to the change in the signal and state of fragile watermarking is the indication of number of times data suspects tampering. Another class of digital watermarking is categorized on the basis of type of media being embedded in the digital data. Thus is divided into audio watermarking, graphic watermarking, image watermarking, and video watermarking. On the basis of detection process digital watermarking can be divided into visual watermarking and blind watermarking. Both visual and blind digital watermarking contradict each other, as original data is desirable during testing sequence in visual digital watermarking but not in blind digital watermarking. Application field of the visual watermarking is narrow but that of blind watermarking is widespread. Other class of digital watermarking is based on its purpose and dispersed into tampering tip watermarking, copyright protection, anti-counterfeiting watermarking and anonymous mark [16].

## III. ARCHITECTURE OF DIGITAL WATERMARKING SYSTEM

*A. Conceptual model of Digital watermarking*

Digital watermarking is a technique in by which operating algorithms on the original multimedia content, we embed special information which indicated the identity of the copyright owner. The process of digital watermarking can be achieved by practicing two subdivision methods: watermark embedding and watermark detection and extraction. By watermark embedding we mean to embed watermark, which can be any form of image, text and so on, to the original digital content. For security purpose and to prevent illegitimate replication and alteration in the digital content, key can be used. After watermark embedding the process of Watermark detection and extraction is done to determine either the digital data embeds stated watermark or the same can be obtained.

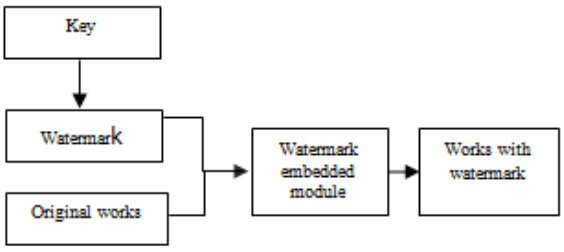


Figure1 Watermark embedding module [16]

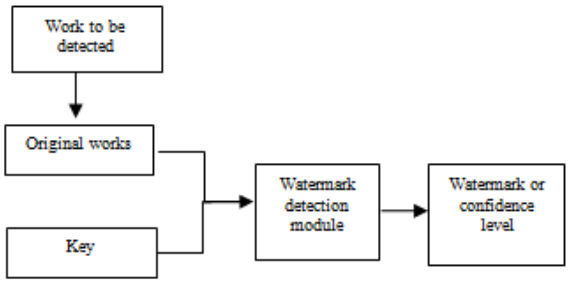


Figure2 Watermark detection and extracting module

*1. Different algorithms in Digital Watermarking*

Algorithms of digital watermarking can be categorized in two domain: 1.Spatial domain algorithms 2. Transform domain algorithms. Fig. 3 gives the hierarchical representation of digital watermarking algorithms.

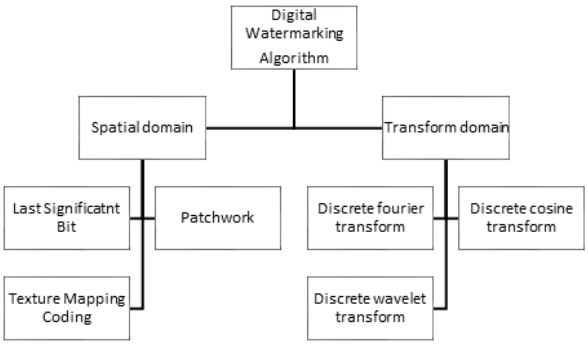


**Figure1 Hierarchical representation of digital watermarking algorithms**

*2. Spatial domain algorithms*

In the algorithms which comes under the spatial domain, direct manipulation in the pixel of the original image itself is done, contradicting the steps in the transform domain. Spatial domain algorithms are prone to malicious attacks, but are easy to implement, encrypt and decrypt.

a) *Least Significant Bit algorithm*: Least significant bit (LSB) algorithm is simplest approach in which information is embedded into the randomly selected bit of the digital image, which ensures that watermark embedded is invisible. Limitation of the LSB is that it is non robust.

b) *Patchwork algorithm:* Statistical method which uses redundant pattern encoding to embed message in the digital image. It survive after numerous malicious attacks and resist lossy compression coding.

c) *Texture mapping coding algorithm:* For the area with the large number of arbitrary texture image, this algorithm is considered beneficiary. In this algorithm texture part of the image embed watermark. We can say that this is most resistive towards the attacks.

1. *Transform domain algorithms*

In transform domain algorithms the input image is equivalent to the image in the spatial domain and then the image is decomposed into sine and cosine components. The output obtained after transformation represents image in the frequency domain. The algorithms of Transform domain are found to be more robust than spatial domain. After the orthogonal transformation on image, the next step is to embed watermark information in the image obtained in the transform domain. For the retrieval of the image in the spatial domain, inverse transform is used. Transform domain methods like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) are some of the most famous transform domain methods.

## IV. APPLICATIONS OF DIGITAL WATERMARKING IN COPYRIGHT PROTECTION OF DIGITAL IMAGE

There has been an immense area in application of digital watermarking and one of the application of digital watermarking is copyright protection of digital image. In this paper we have presented brief description of the work done in the area of application of digital watermarking for copyright protection in digital image.

Jiang Xuehua [16] has discussed application of digital watermarking technology along with the application for protecting copyright by using DCT algorithm and concluded that DCT based watermark can endure wide range of image processing and resist malicious attacks and compression.

DragosN and Radu O.Preda proposed a scheme of digital watermarking based on wavelet packets for copyright protection of digital image.[1] In this approach they have worked on different details of scale in which they have decomposed the original digital image. And different level of detail embed the binary image taken as watermark. As a result of computation using this approach on the digital image, they witnessed that there is a minimal degradation to the original image and provide robustness.

Jen-Sheng Tsai et al. [2] have discussed feature based algorithm of the digital watermarking for digital content authentication and copyright protection. They have extracted the characteristic region of the original obtained from the grayscale watermark image in which watermark has to be embedded, by using Hessian-Affine feature detector. Then after the extraction of the characteristic region in the original image, copyright watermark is embedded into the characteristic regions detected by the Hessian Affine feature detector. By using block wise fragile watermarking technique in the remaining portion of the original image authentication can be obtained. The result of method discussed above showed that proposed watermarking algorithm can resist most attacks. Beside this, since the fragile watermark was not the part of the characteristic region, accuracy of location for content authentication is affected.

N. Nagamalleswara Rao et al. [3] have proposed copyrights protection of digital images with the help of biometrics and digital watermarking. In this approach minor points from the fingerprints of the first owner of the digital image has been extracted and then these minutiae points are shuffled and group together as vector. The single values obtained after the computation of SVD of the vector, is embedded into the original image. In DCT-SVD domain watermark embedding and extraction process is done. They uncovered that in the case of ownership dispute, the particular value of coordinates of minutiae act as proof.

Neha Bansal et al [21] have compared various watermarking techniques and concluded that DCT transform is best suited algorithm for digital watermarking among the rest algorithms namely LSB.

Kaushik Deb et al. [19] have proposed the combined DWT and DCT based digital watermarking for copyright protection of digital image. Scalability and compression is achieved by using DWT and DCT respectively. This algorithm preserves the higher quality of original image and robustness under several attacks which includes image processing, JPEG compression and so on.

Ming-Chiang Hu et al. [13] have proposed two phase digital watermarking methodology for securing copyright of the digital image. By this we are able to extract both gray scale as well as binary watermark image from the protected image. In the first step pixel values of the initial input image is operated upon to construct grayscale watermark. In this approach binary watermark can be obtained from the grayscale watermark permuted in the prior stage. They concluded that their approach is best among the present proposed methods, as it satisfies all the attributes like robustness and security.

Lu et al. [14] proposed algorithm based on mean-removed vector quantization to tackle prevailing issues such as in the field of copyright protection and authentication of digital image using digital watermarking.

M.A. Dorairangaswamy and B. Padhmavathi [6] presented blind watermarking scheme to secure copyright of digital image. In this approach they have embedded binary watermark image in the original input digital image.

In watermark extraction they don't need the original image, and thus they named their proposed scheme as a 'blind' approach.

## V.CONCLUSION

The fast growing networks of computers and specifically, the whole new era of internet has revolutionized the means of communication. The tremendous growth in the field of Information and Communication Technology has resulted in the change in the pattern in which data used to be stored earlier. Beside the advantage it provides over analog data, it has the threat of being altered and easily manipulated. In this paper concept of digital watermarking along with the attributes and algorithm of digital watermarking has been discussed. The paper gives the description of the application of digital watermarking for copyright protection of digital images. Spatial domain algorithms for data hiding are simple but are prone to attacks and unauthorized access. Whereas transform domain algorithms overcome the limitation of spatial domain and offer robustness. DCT is the algorithm which is mostly preferred over the rest of the algorithms like LSB and provide compression without much degradation in the original content. The scalability corresponds to the DWT. And when the characteristics of both DWT and DCT combines, it sustain robustness and high quality image even after several attacks. The motivation for the future work is to propose a new algorithm to protect copyright of medical images and look forward in a future where medical images can be protected against alterations and attacks.

## VI. ACKNOWLEDGEMENTS

The authors are thankful to Hon'able C – VI, Mr. Aseem Chauhan (Additional President, RBEF and Chancellor AUR, Jaipur), Maj. General K. K. Ohri (AVSM, Retd.) Pro-VC Amity University, Uttar Pradesh Lucknow Campus, Wg. Cdr. (Dr.) Anil Kumar, Retd. (Director, ASET), Prof. S. T. H. Abidi (Professor Emeritus), Brig. U. K. Chopra, Retd. (Director AIIT), and Prof O. P. Singh (HOD, Electrical & Electronics Engg.) for their motivation, kind cooperation, and suggestive guidance.

## REFERRENCES

[1] Claudine Conrado,MilanPetkovic,MichielvanderVeenand Wytsevan der Velde"ControlledSharing of Personal ContentUsing Digital Rights Management",Journal of Researchand Practice inInformation Technology,Vol. 38,No.1,February2006.

[2] N. Nagamalleswara Rao, P. Thrimurthy and B. RaveendraBabu, "An efficient copyright protection scheme for digital images using biometrics and watermarking",2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT ,pp 69 – 74, August 2009.

[3] C.Johnson, P. Montague and C. Steketee, "Digital Rights Managementfor Content Distribution", In proceedings o f AustralasianInformationSecurityWorkshop2003(AISW2003), Vol.21,2003.

[4] Authors Emir Ganic,AhmetM. Eskicioglu,"RobustDWT-SVD domain image watermarking: embedding datainall frequencies",International MultimediaConference, Magdeburg, Germany, pp. 166-174, 2004.

[5] E. T. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp., "Advances in digital video content protection", IEEE: Special Issue on Advances in Video Coding and Delivery, pp171-183, 2005.

[6] A.Piva ,F.Bartolini, and M. Barni, "Managing copyright in open networks, "IEEE Trans. Internet Computing, vol.6, no.3, pp.18–26, May–June. 2002.

[7] Shang-LinHsieh,Lung-YaoHsu,andI-JuTsai,"A CopyrightProtection Scheme for ColorImages using SecretSharing andWaveletTransform", proceedings of WorldAcademy of Science,Engineering And Technology,Vol. 10,December 2005.

[8] Hans Georg Schaathun,"Onwatermarking/fingerprinting for copyright protection",First InternationalConference on InnovativeComputing, InformationandControl,ICICIC'06,Beijing,Vol. 3,pp. 50-53,August. 30.-September1, 2006.

[9] IanKerr,Hacking@privacy:"Why WeNeedProtectionfromthe Technologies That Protect Copyright", Inproc. Of Conference onprivacyand identity,2007.

[10] Jiang Xuehua, "Digital Watermarking and its Application in Image Copyright Protection", International Conference on Intelligent Computation Technology and Automation (ICICTA), Vol. 2, pp 114-117, May 2010.

[11] Neha Bansal, Vinay Kumar Deolia,Atul Bansal and PoojaPathak,"Comparative analysis of LSB, DCT and DWT for Digital Watermarking", 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp 40-45,March 2015

[12] DragosN and RaduO.Preda, "A new digital watermarking scheme for image copyright protection using wavelet packets" 7th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, pp 518-521,September 2005.

[13] Jen-Sheng Tsai, Win-Bin Huang, Chao-Lieh Chen and Yau-Hwang Kuo, "A Feature-Based Digital Image Watermarking For Copyright Protection and Content Authentication", IEEE International Conference on Image Processing, ICIP, Vol.

[14] Kaushik Deb, Md. Sajib Al-Seraj, Md. MoshiulHoque and Md. Iqbal Hasan Sarkar "Combined DWT-DCT based digital image watermarking technique for copyright protection", 7th International Conference on Electrical & Computer Engineering (ICECE), pp 458-461,December 2012.

[15] Gil-Je Lee, Eun-Jun Yoon and Kee-Young Yoo, "A Novel Multiple Digital Watermarking Scheme for the Copyright Protection of Image", Fourth International Conference on Innovative Computing, Information and Control (ICICIC), pp 756-759, December 2009.

[16] Zhe-Ming Lu, Wei-Min Zheng, Jeng-Shyang Pan and Zhen Sun, "Multipurpose Image Watermarking Method Based on Mean-removed Vector Quantization", Journal of Information Assurance and Security, Vol. 1, pp. 33-42, 2006

[17] ManjunathaPrasad.R and ShivaprakashKoliwad "A robust wavelet-based watermarking scheme for copyright protection of digital images", International Conference on Computing Communication and Networking Technologies (ICCCNT), pp 1-9, July 2010.

[18] M.A.Dorairangaswamy and B.Padhmavathi, "An effective blind watermarking scheme for protecting rightful ownership of digital images", TENCON 2009-IEEE Region 10 Conference, pp 1-6, January 2009.

[19] Ming-Chiang Hu, Der-Chyuan Lou and Ming-Chang Chang, "Dual- wrapped digital watermarking scheme for image copyright protection," Computers & Security, Vol. 26, No. 4, pp. 319-330,2007.

[20] Wie Song, Xiang-chun Liu, Ren-wei Ding and Peng-yuNa,"Digital watermarking technique for digital medical images", International Symposium on Information Technology in Medicine and Education (ITME),Vol.2,pp 928-931, August 2012.

[21] KetaRaval and Sameena Zafar, "Digital Watermarking with copyright authentication for image communication", International Conference on Intelligent Systems and Signal Processing (ISSP), pp 111-116, March 2013.