An Overview of Digital Watermarking Techniques

Barun K. Pandhwal, Devendra S. Chaudhari

Abstract*— One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Digital data can be stored efficiently with a very high quality and it can be manipulated very easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are better than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of information and a copy of a digital media is identical to the original. With digital multimedia distribution over World Wide Web, Intellectual Property Rights (IPRs) are more threatened than ever due to the possibility of unlimited copying. This problem can be handled by hiding some ownership data into the multimedia data, which can be extracted later to prove the ownership, a concept called watermarking. Continuous efforts are being made to device an efficient watermarking scheme and this paper conducts a literature survey of digital watermarking within an image. It describes the early work carried out on digital watermarks, including the brief analysis of various watermarking schemes and its potential applications.

***Index Terms*— Digital watermarking, Least significant bit, Discrete Cosine Transform, Discrete Wavelet Transform**

I. INTRODUCTION

Everyday tons of data is embedded on digital media or distributed over the internet. This data, which include still images, video, audio, or text are stored and transmitted in a digital format can be easily copied without loss of quality and efficiently distributed. Thus the protection of intellectual property rights has become increasingly important. Information stored in digital format because of ease of reproduction, retransmission and even manipulation allows a pirate either to remove a watermark and violate a copyright or to cast the same watermark after altering the data to forge the proof of authenticity. The design of techniques for preserving the ownership of digital information is in the basis of the development of future multimedia services.

In bank currency notes, a watermark is embedded which is used to check the originality of the note. The same concept of watermarking can be used in digital multimedia contents for checking the authenticity of the original content. Digital media has the capability to embed additional data into the original media data in a way which is perceptually, and sometimes also statistically undetectable.

Manuscript received on March, 2013.

Barun Pandhwal, Department of Electronics and Telecommunication Engineering, Government College of Engineering, Amravati, India.

Dr. Devendra S. Chaudhari, Head of Department, Electronics and Telecommunication Engineering, Government College of Engineering, Amravati, India.

This data-embedding potential can be exploited to build protection mechanisms against the threats mentioned before, or to provide additional functionalities. A watermarking algorithm embeds a data, an unperceivable digital code, namely the watermark, carrying information about the copyright status of the work to be protected [1].

This paper reviews some of the watermarking techniques carried out with their pros and cons. It firstly provides a general description of the desirable characteristics of digital watermarking system. Consecutively, various watermarking techniques are discussed in brief with the potential applications of the watermarking methodology. Finally, certain points are summarized based on the theory and experimental results obtained by various researchers.

II. ATTRIBUTES OF DIGITAL WATERMARKING SYSTEM

The significance of a watermarking property in any particular application depends upon the requirements of that specific application. Some of the watermarking system properties are highlighted in this section [2], [3].

A. Embedding Effectiveness

Effectiveness of watermarking system is the probability of detecting watermark(s), especially at the receiving point. The desired effectiveness is 100% but it is often not possible because of the requirement of perceptual similarity conflicts. Thus, it's application dependent to sacrifice effectiveness for better performance with respect to other characteristics.

B. Perceptual Similarity

Perceptual similarity is a measure that determines the similarity level between the original and watermarked image, especially at the receiving end. Sometimes the fidelity of the system can be sacrificed for the better performance with respect to other characteristics like higher robustness or low cost. The most commonly used image similarity index measure is PSNR (Peak Signal to Noise Ratio) for two X × Y images, O and W where one is original and the other is watermarked image that can be calculated as,

$$psnr = 20\log\left(\frac{\max^2}{MSE}\right)$$

Where MSE is defined as,

$$MSE = \frac{1}{XY}\sum_{i=0}^{1-X}\sum_{j=1}^{1-Y}[O(i,j) - W(i,j)]^2$$

Where max is the possible maximum value of the image i.e. max = 255 for 8-bit gray scale image.

C. Robustness

Robustness is the ability to detect the embedded watermark after common image processing operations like compression, filtering, geometric distortion etc. Sometimes watermarking systems are developed which have the ability to survive most of the intentional manipulations. Robustness is application dependent and it is not necessary that all the applications require robustness against all the operations. For example, in broadcast monitoring the robustness is required only against the communication related manipulations. In fragile watermarking, robustness is undesirable. However, there is another class of watermarking called semi-fragile watermarking, where robustness is required only against the unintentional manipulations.

D. Data Embedding Capacity

The number of bits, a watermarking scheme encodes within a cover work is referred to as data payload and is application dependent. For N bits watermark, the system can encode any of 2^N different messages. Increasing the watermark payload will affect the fidelity of the system and vice versa. Thus, it is very important for the researchers to make trade-off between contradicting properties of the watermarking while developing the watermarking systems. The three main contradicting parameters are robustness, imperceptibility, and payload. Increasing the watermark payload will affect the perceptual similarity (fidelity) of the image and robustness is affected by decreasing the watermark payload.

E. Blind and Informed Detection

In informed watermarking systems (i.e. transaction tracking), the detector requires the original or some information about the original unwatermarked image. However, in blind watermarking systems (i.e. copy control application), there is no need of original or any information about the original image. The terms *private* and *public* watermarking systems may be used alternatively for informed and blind watermarking approaches respectively. Blind detection is computationally complex having low PSNR value but offers very high security while informed detection is having high pay load and very high PSNR value having simple embedding and extracting algorithms.

F. Computational Complexity

Computational complexity indicates the amount of time watermarking algorithm takes to encode and decode. To ensure security and validity of watermark, more computational complexity is needed. Conversely, real-time applications necessitate both speed and efficiency.

III. WATERMARKING APPROACHES

Various watermarking system can be classified into two main domains i.e. Spatial domain techniques and Frequency domain techniques [4].

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression. On the other side, frequency domain techniques take the advantage of the human visual system's low sensitivity to high and middle frequency information. In these techniques, the image is first transformed to the frequency domain by the use of any transformation methods such as Fourier transform, discrete cosine transform (DCT) or discrete wavelet transform (DWT). Now the information is added to the values of its transform coefficients. After applying the inverse transform, the marked coefficients form the embedded image. Authors found that the transform techniques are having very high PSNR values for the composite image and various image processing tasks can be performed on it. Table I shows Watermarking domains and techniques.

Table I. Watermarking domains and techniques

Watermarking Domain	Technique
Spatial	Least Significant Bit Coding
	Patchwork Technique
	Predictive Coding
Frequency	Discrete Cosine Transform (DCT)
	Spread Spectrum
	Discrete Wavelet Transform and related techniques
	Combination of DWT and DCT

A. Least Significant Bit Coding (LSB)

LSB coding is one of the earliest methods of image watermarking. Van *et al.* proposed two LSB techniques. In the first method the LSB of the image was replaced with a pseudo-noise (PN) sequence while in the second a PN sequence was added to the LSB [5]. Though this method was simple, it lacks the basic robustness that may be expected in any data hiding application. It was able to survive simple operations such as cropping, any additive noise, however, it was not possible to process the composite image under operations such as intensity enhancement, resampling, requantization, image enhancement, etc. Furthermore, once the algorithm was discovered, it becomes an easy task for the intruder to alter or detect the hidden information.

B. Patchwork Technique

Bender *et al.* [6] proposed watermarking scheme based on statistical method called patchwork**.** In patchwork, n pairs of image points, (a, b) were randomly chosen. The image data in a were lightened while that in b were darkened. Patchwork was independent of the host image. Experimental results show that this algorithm was simple and easy showing reasonably high resistance to most nongeometric image modifications. However there were some limitations such as extremely low embedded data rate and hence this technique was useful to low bit-rate applications only. Also it was necessary to keep a register about where the pixels in the image lie. In the presence of severe affine transformations, it was still somewhat difficult to decode the image.

C. Predictive Coding Scheme

Predictive coding scheme was proposed by Matsui and Tanaka for gray scale images [7]. In this method the correlation between adjacent pixels was exploited.

A set of pixels where the watermark had to be embedded was chosen and alternate pixels were replaced by the difference between the adjacent pixels. This was further improved by adding a constant to all the differences. A cipher key was created which enabled the retrieval of the embedded watermark at the receiver. This was much more robust when compared to LSB coding.

D. DCT

A DCT based information hiding system was proposed in which the image was first segmented into non-overlapping blocks of 8x8 and forward DCT was applied to each of the block [8]. After that a selection criteria was applied followed by applying coefficient selection criteria. The watermark was embedded by modifying the selected coefficients and the final watermarked image was obtained by applying inverse DCT. Fig.1 shows a typical structure of DCT based watermarking.

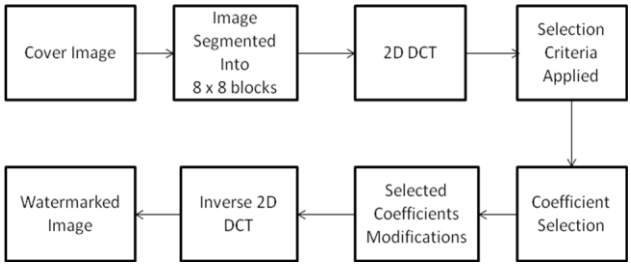

Fig.1 Typical structure of DCT based watermarking

Most of the energy in the DCT domain is concentrated in the low frequencies. As is known low frequencies are perceived very well by human eye, hence the chances of the watermark being perceptible was high where as high frequencies are prone to attacks such as compression and scaling. Thus the middle frequency bands were chosen such that they avoid the most visual important parts of the image without over-exposing themselves to removal through compression and noise attacks. The main advantage of DCT which makes it attractive for watermarking is its energy compaction property. This property divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. Experimentally, this technique proved to be highly resistant to JPEG compression as well as to significant amount of noise. However, it suffered from visual artifacts as DCT was done on the blocks.

E. Spread Spectrum

In 1997, Cox *et al.* presented their non-blind spread spectrum watermarking scheme operating in a block-DCT domain [9]. The authors pointed out that despite the risk of potential fidelity distortions the watermark needs to be embedded in an image's perceptually relevant components in order to be robust against image processing attacks. The proposed watermarking scheme therefore aimed to embed the watermark into the image's perceptually significant frequency components without introducing visible distortions to achieve robustness against simple image processing and geometrical image manipulation. To determine the optimal locations for the watermark, a perceptual mask of a DCT was used to highlight locations with good properties for robustness and image quality which normally results in picking low frequency coefficients. This approach was inspired by the concept of spread spectrum communications, in which a narrow-band signal is transmitted over a much larger bandwidth, so that the energy added to any single frequency is imperceptible. For marking a Gaussian sequence of real numbers was embedded into the most significant coefficients found in the image's 8x8 DCT blocks. To verify the presence of the watermark, the cross correlation value between the extracted watermark and the original watermark was computed. Experimental results showed that this method resists JPEG compression with a quality factor down to 5%, scaling, dithering, cropping and collusion attacks.

F. Discrete Wavelet Transform and related techniques

DWT based techniques are very similar to theoretical model of Human Visual System (HVS). It is more frequently used due to its time/frequency characteristics. Here an image is passed through series of low pass and high pass filters which decompose the image into sub bands of different resolutions. As most of the energy is concentrated in the approximate (LL) sub band having low frequency sub bands, any change in these low frequency sub bands would cause a severe degradation of image. As the human eyes are not sensitive to high frequency sub bands, the secret information is embedded in either vertical, horizontal or diagonal (LH, HL or HH respectively) sub bands. Fig. 2 shows a generalized DWT based watermarking scheme.

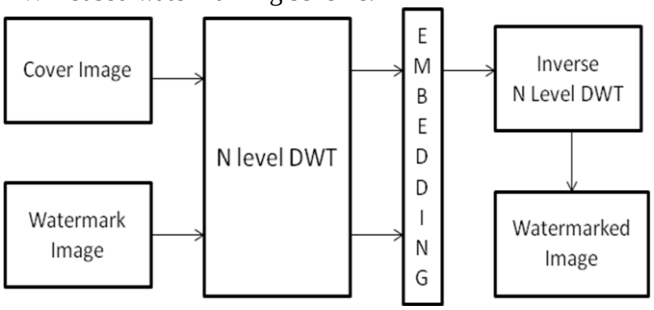

Fig.2 Generalized DWT based watermarking Scheme

Xia *et al.* added a Gaussian random noise to the large coefficients in the DWT domain [10]. Here the watermark was inserted in the middle and high frequency bands of the image. In the decoding process, the DWT of the marked image was performed and the sections of the watermark were extracted and correlated with sections of the original watermark. A watermark was detected if the cross-correlation was above a threshold. Experimental results showed that the DWT based watermark approach was robust to several kinds of distortion such as additive noise, resolution reduction and compression.

A new approach of watermarking in wavelet domain where human visual system (HVS) characteristics are exploited to hide the watermark was developed by Barni *et al.* [11]. The watermark to be embedded was a pseudo- random sequence which was adaptively added to the DWT coefficients of three largest detail sub-bands. The detection was achieved by measuring the correlation between the watermarked coefficients and the watermarking code. The most important feature of this technique was that the watermark embedding was performed pixel by pixel considering the texture and the luminance content of all the image sub-bands. Experimental results showed that this method performed exceptionally well in case of lossy compression.
Also,

the watermarking energy can be kept so high that even a small portion of the image is sufficient to correctly guess the embedded code.

Kundur *et al.* proposed the use of gray scale logos as watermark [12]. They addressed a multi-resolution fusion based watermarking method for embedding gray scale logos into wavelet transformed images. The logo undergoes 1-level decomposition for watermarking. Each sub-band of the host image was divided into blocks of size equal to the size of sub-band of the logo. Four sub-bands of the logo corresponding to different orientations were added to the blocks of the same orientation. For fusion, the watermark was scaled by salience factor computed on a block by block basis. Simulation results showed that the proposed technique was highly robust to compression and additive noise. In fact, if the images were almost completely destroyed yet the watermark can be extracted fairly accurately.

Authors had developed a new semi-blind reference watermarking scheme using a combination of DWT and singular value decomposition (SVD) [13]. In this method instead of using a PN sequence, a gray scale logo image was used as watermark. For embedding process the original image was first transformed into wavelet domain and then using directive contrast and wavelet coefficients a reference sub-image was formed. By amending the singular values of the reference image using the singular values of the watermark, the watermark was embedded into the reference image. This technique proved to be very robust and was able to withstand a variety of attacks including ambiguity attack. Also, it was found that after undergoing operations such as filtering, addition of noise, JPEG compression, cropping, resizing, rotation and pixilation, the extracted logo was still recognizable.

A blind image watermarking scheme based on wavelet tree quantization was proposed [14]. In this approach a super tree was formed by grouping the wavelet coefficients of the host image. This super tree was quantized in such a way that it exhibits a large enough statistical difference which can be used for embedding and extracting watermark. This technique proved to be robust for both time and frequency domain attacks.

An algorithm was proposed by Ramani *et al*. which was having very high data hiding capacity [15]. It was based on Integer to Integer Wavelet Transform (IWT) with Bit Plane Complexity segmentation (BPCS). IWT was used to decompose the cover image whereas BPCS takes the advantage of HVS which cannot recognize changes in complex positions of the image. The drawback with this method was that it needed separate processing for R, G and B components of the color image.

A method based on combination of DWT and a Generic algorithm which can be used to find the best sub band for watermark embedding was introduced [16]. This technique provided imperceptibility and robustness simultaneously but the process was too lengthy and time consuming.

1-level DWT alpha blending technique was proposed which embeds the invisible watermark into the salient features of the original image using Daubecheis wavelets [17]. In this approach the decomposed components of both the images were multiplied by a scaling factor and then added. Result shows that the quality of the watermarked image, recovered image and extraction of watermark were dependent only on the values of the scaling factors k and q. Also the process of embedding and extracting was simpler when compared to DCT method. There was a limitation that the size of the watermark must be smaller than the host image and the frame size of both the images should be made equal.

G. Combination of DWT and DCT

A technique based on joint DWT – DCT transformation was proposed [18]. A binary watermarked logo is scrambled by Arnold cat map and embedded in certain coefficient sets of a 3-level DWT transformed of a host image. Then, DCT transform of each selected DWT sub-band is computed and the PN-sequences of the watermark bits are embedded in the middle frequencies coefficients of the corresponding DCT block. In extraction procedure, the same procedures as the embedding process is used to extract the DCT middle frequencies of each sub-band. Finally, correlation between mid-band coefficients and PN-sequences is calculated to determine watermarked bits.This technique proved to be more robust and imperceptible as the visual artifact drawback of the block based DCT method is reduced giving comparatively higher PSNR value.

IV. APPLICATIONS

There are diverse applications of watermarking for which suitable watermarking systems are designed. Watermark can be used in copyright protection which prevents redistribution of copyrighted images. Authentication for ownership verification in case of ATM, credit cards, etc. can also be achieved. Content labelling and content protection are the most common examples of visible watermarks. Nowadays digital watermarking is also being used in biomedical and satellite imaging to highlight some peculiar regions and parts of an image. Covert communication which includes transmitting hidden data which is almost imperceptible to the intruder is being achieved using watermarking schemes having high data embedding capacity.

V.CONCLUSION

Significant number of watermarking techniques can be found in the literature used in the variety of applications because of their advantages over the alternative methods. The overall study in this paper shows that the spatial methods are relatively fast and requires low resources and even they can provide comparable performance over scaling and additive noise attacks. On the other hand, frequency domain methods are computationally complex but performs exceptionally well in terms of robustness, pay load capacity, image operations and imperceptibility. DCT based watermarking systems are highly resistant to JPEG compression and shows high energy compaction property while DWT based watermarking systems are more preferred choice because of the advantages listed out by several authors in their respective research over the years.

REFERENCES

1. Y. Wang, J. Doherty and R.Van Dyck, "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images," *IEEE Trans. Image processing*, vol. 11, no. 2, 2002, pp.77-88.
2. M. Hsieh, D. Tseng and Y. Huang, "Hiding Digital Watermarks Using Multiresolution Wavelet Transform," *IEEE Trans. Industrial*

Electronics, vol. 48, no. 5, 2001, pp.875-882.
3. B. Gunjal and R. Manthalkar, " An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms," Journal of Emerging Trends in Computing and Information Sciences vol. 2, no. 1, 2011, pp.37-42.
4. C. Lin and Y. Ching, "A Robust Image Hiding Method Using Wavelet Technique," Journal of Information Science and Engineering, vol. 22, 2006, pp.163-174.
5. R. van Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," *Proc. IEEE Int. Conf. Image Processing*, vol. 2, 1994, pp. 86–90.
6. W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding," IBM Systems Journal, vol. 35, nos. 3,4, 1996, pp.313-336.
7. F. Hartung and M.Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, 1999, pp. 1079–1107.
8. B. Kaur, A. Kaur, J. Singh, "Steganographic Approach For Hiding Image In Dct Domain," International Journal Of Advances In Engineering & Technology, Vol. 1,Issue 3, 2011, pp.72-78.
9. I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking For Multimedia," *IEEE Trans. Image Processing*, vol. 6, 1997, pp. 1673–1687.
10. X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark For Digital Images," in *Proc. IEEE Int. Conf. Image Processing*, vol. 1, 1997, pp. 548–551.
11. M. Barni, F. Bartolini, and A. Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking," *IEEE Trans. Image processing*, vol. 10, no. 5, 2002, pp.783-791.
12. D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," *Proc. IEEE Int. Conf. Image Processing*, vol. 1, 1997, pp. 544–547.
13. G. Bhatnagar and B. Raman, "A New Robust Reference Watermarking Scheme Based on DWT-SVD," Computer Standards and Interfaces, vol.31, no.5, 2009, pp. 1002-1013.
14. S. Wang and Y. Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking," *IEEE Trans. Image processing*, vol. 13, no. 2, 2004, pp.154-165.
15. K. Ramani, E. V. Prasad, Dr. S. Varadarajan, "Steganography Using Bpcs To The Integer Wavelet Transformed Image," International Journal of Computer Science and Network Security, vol.7 no.7, 2007, pp. 293-302.
16. A. Haj and A. Errub, "Performance Optimization of Discrete Wavelets Transform Based Image Watermarking Using Genetic Algorithms," Journal of Computer Science, vol.4, no.10, 2008, pp.834-841.
17. A. Singh and A. Mishra, "Wavelet Based Watermarking On Digital Image," Indian Journal of Computer Science and Engineering Vol 1 No 2, 2011, pp. 86-91.
18. L. Feng, L. Zheng and P. Cao, "A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection," *Proc. IEEE Int. Conf. Computer Science and information tech.*, vol.7, 2010, pp.455-458.

AUTHORS PROFILE

Barun Pandhwal is presently pursuing his M.Tech in Electronic System and Communication (ESC) from Government College of Engineering, Amravati. He received his B.E. in Electronics and Telecommunication from Sant Gadge Baba Amravati University in 2010. He was placed 9th in order of merit of Sant Gadge Baba Amravati University, Amravati in year 2010. His area of research includes Image Processing, Wavelet Analysis and Digital Watermarking.

Dr. Devendra S. Chaudhari is presently working as Head, Department of Electronics and Telecommunication Engineering at Government College of Engineering, Amravati. He obtained his BE, ME, from Marathwada University, Aurangabad and PhD from Indian Institute of Technology Bombay, Powai, Mumbai. He has been engaged in teaching, research for period of about 25 years and worked on DST-SERC sponsored Fast Track Project for Young Scientists. He has worked as Head Electronics and Telecommunication, Instrumentation, Electrical, Research and in-charge Principal at Government Engineering Colleges.Dr. Chaudhari published research papers and presented papers in international conferences abroad at Seattle, USA and Austria, Europe. He worked as Chairman / Expert Member on different committees of All India Council for Technical Education, Directorate of Technical Education for Approval, Graduation, Inspection, Variation of Intake of diploma and degree Engineering Institutions. As a university recognized PhD research supervisor in Electronics and Computer Science Engineering he has been supervising research work since 2001. One research scholar received PhD under his supervision.

He has worked as Chairman / Member on different university and college level committees like Examination, Academic, Senate, Board of Studies, etc. He chaired one of the Technical sessions of International Conference held at Nagpur. He is fellow of IE, IETE and life member of ISTE, BMESI and member of IEEE (2007). He is recipient of Best Engineering College Teacher Award of ISTE, New Delhi, Gold Medal Award of IETE, New Delhi, Engineering Achievement Award of IE (I), Nashik. He has organized various Continuing Education Programmes and delivered Expert Lectures on research at different places. He has also worked as ISTE Visiting Professor and visiting faculty member at Asian Institute of Technology, Bangkok, Thailand. His present research and teaching interests are in the field of Biomedical Engineering, Digital Signal Processing and Analogue Integrated Circuits.