www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 9 Sep 2015, Page No. 14409-14416

Digital Watermarking Algorithms: A Review

Achintya Singhal[1], Kamred Udham Singh[2]

[1] Department of Computer Science, Banaras Hindu University,
Varanasi U.P., India
Achintya.singhal@gmail.com
[2] DST-CIMS, Banaras Hindu University, Varanasi U.P., India
kamredudhamsingh@mail.com

Abstract: ***Due to the ease of network connectivity and the proliferation of digital capture devices, the access and sharing of images has become extremely feasible and convenient. However, some access and sharing may be unauthorized or illegal. Thus, digital watermarking has become an active research area focused on battling these types of activities. The paper compiles the various researches/advancements done in this field***.

Keywords: Digital media, DCT, spatial domain, transform domain.

1. Introduction

The availability of digital media has increased considerably due to the rapid expansion of the Internet and the overall development of digital technologies in the recent years. Not only without loss of quality duplication, but also easy modification that is unnoticeable at times can be done on digital contents. Detection of modified images, videos and audios are necessary in many contexts. So, security systems that can protect the content of digital data must be developed. Watermarking is suitable for such applications because it can insert invisible information in a host by modifying it unnoticeably. Due to which digital watermarking has received increasing attention since it has been observed as an effective mechanism for copyright protection of digital contents [2]. Anderson and Petitcolas (1998) [1] clarified the concept of steganography and explored its power and the domain. A number of approaches to hide encrypted copyright marks or serial numbers in digital image, audio, and video were also elaborated along with the prospective attacks on them.

Watermarking is not a new field and literatures trace that there been significant usage of steganography and cryptography since 14th century [3]. Though the word digital watermarking got phrased recently but there been significant development in 15th and 16th centuries [5]. Kahn (1996b) [4] described the history of steganography from its ancestry, through the development of invisible inks and microdots, to the spread spectrum communications. Finally, Pfitzmann (1996) [6] reported terminology agreed at the plenary session of the first international workshop on information hiding, whose aim was to help workers in copyright marking, steganography, covert channels and related fields to avoid confusion and ambiguity. Later, Zhao (1997) [8] provided a general introduction to watermarking techniques, the general protection goals and the ideas underlying in a number of implementations, particularly spread-sequence, frequency hopping and transform techniques. Voyatzis et. al., (1998) [10] summarized the main features of watermarking schemes for still images, reviewed the minimum steps for the implementation of their algorithm and briefly discussed the robustness issues.

The digital watermarking techniques have been studied and reviewed aggressively. The areas where significant contributions were made are in the area of digital image, digital audio and digital video. In this paper, the major contributions in the area of audio, video and image watermarking are compiled in the subsequent sections.

2. Digital Audio Watermarking

Digital audio watermarking involves the concealing of watermark data within a discrete audio file. Applications for this technology are numerous and intellectual property protection is currently the main driving force behind research in this area. To fight online music piracy, a digital watermark, could be added to all the recordings prior to its release, signifying the author of the work, along with the user who has purchased a legitimate copy.

Lacy et. al., (1998) [11] discussed music piracy, the availability of various technologies affecting it (like compression), different system-level vulnerabilities of copyright marking mechanisms, and their likely future role. Gruhl et. al., (1996) [12] described the use of cepstral transforms to embed data in an audio signal at typically 16 bits per second by manipulating the echo characteristics of the signal below the level of perceptibility. The technique proposed was much more robust against lossy compression techniques and D/A conversions than simple noise addition. But, the algorithm showed its limitation at gaps of silence, such as inter-word pauses in speech. In addition to copyright protection, this can be used for applications such as annotation, captioning and the automatic monitoring of radio advertisements. Chang and Moskowitz (1997) [13] considered four basic techniques for hiding data in a voice message: low-bit coding, phase coding, spread spectrum embedding and echo hiding. They analyzed the available bandwidth and how this is affected if an opponent perturbs the signal by adding noise, band-pass filtering or re-sampling. Some of the other major contributions in the area noted are Boney et. al., (1996) [14], Swanson et. al., (1998a) [15], Neubauer and Herre(1998) [18], Bassia and Pitas (1998) [19], Bassia et. al., (2001) [20], Tay et. al., (2003) [21] and Hafiz et. al., (2004) [22].

DOI: 10.18535/ijecs/v4i9.60

3. Digital Video Watermarking

Video watermarking involves embedding cryptographic information into the frames of digital video. Ideally, a user viewing the video cannot distinguish between the original video and the watermarked video, but a watermark extraction application can read and extract the. As the watermark is part of the video, this technology works independently of the video file format or codec. Hartung and Girod (1998) [24] presented a direct sequence spread spectrum technique which can embed watermarks both into compressed and uncompressed video sequences. They proposed two methods. The first technique regards the video signal as a one-dimensional signal acquired by line scanning. The embedded signal is amplified to exploit the temporal and spatial phenomena of the human visual system. The second technique generated a watermark signal per frame and adds it directly in the discrete cosine domain avoiding the need to uncompressed the video stream completely. The performance of the system was illustrated with various BER tables. Dittmann et. al., (1998) [25] proposed two marking methods for MPEG video. Both techniques were enhanced with smooth-block/edge detection and strong error correction codes. Contrary to other systems, the watermark was embedded in each frame of the video, to deter illicit copying of even a single image of a video. Swanson et. al., (1998b) [16] proposed a temporal wavelet transform domain video watermarking system based on a perceptual model which has dynamic strength controls mechanism. The system is also scene based to allow extraction of the watermark from a reduced number of frames. Chae and Manjunath (1999) [27] proposed the scheme based on texture masking and utilized a multi-dimensional lattice structure for encoding watermark data. Watermark data was embedded in video frames using the block DCT. The embedded scheme was blind. The proposed method enabled high rate of data embedding and was robust to motion compensated coding, such as MPEG-2. Besides the above noted contributions, majority of researchers treated the video watermarking same as image watermarking because the video is a collection of images in form of frames and execution of these frames at a specified speed gives the illusion of object motion. Hence, they proposed their algorithms suitable for videos too. But the videos have got very complicated and huge data structure in comparison to image data. Thus there exists an additional requirement i.e. the watermarking algorithm should be highly fast and efficient. Because of these limitations, very limited research is being conducted in this area.

4. Digital Image Watermarking

The digital image watermarking techniques can basically be grouped into three main classes:-

1. The spatial domain techniques whereby the watermark is embedded by directly modifying the pixel values of the original image.
2. The transform domain methods whereby the watermark is embedded by modulating the transform domain signal coefficients. The transform domain techniques have been found to have the greater robustness, when the watermarked signals are tested after having been subjected to common signal distortions.
3. The feature domain technique whereby the region, boundary and object characteristics etc. are taken into cognizance. Such watermarking methods may present additional advantages in terms of detection and recovery from geometric attacks, compared to previous approaches.

4.1 Spatial Domain Techniques

Many spatial techniques are based on adding/ subtracting fixed amplitude pseudo noise (PN) sequences to an image. PN sequences are also used as the "spreading key" when considering the host media as the noise in a spread spectrum system, where the watermark is the transmitted message. These approaches modify the least significant bits (LSB) of the host data on the assumption that the LSB data are visually insignificant. The watermark is generally recovered using knowledge of the PN sequence (and perhaps other secret keys, like watermark location) and the statistical properties of the embedding process. Two LSB techniques are described in Schyndel et. al., (1994) [52]. The first subtracts the LSB of the image with a PN sequence, while the second adds a PN sequence to the LSB of the image. In Bender et. al., (1996) [53] proposed a direct sequence spread spectrum technique to embed a watermark in host signals. It is a statistical technique that randomly chooses *n* pairs of points (a_i, b_i) in an image and increases the brightness of a_i, by one unit while simultaneously decreasing the brightness of b_i. Another PN sequence spread spectrum approach is proposed in Wolfgang and Delp (1996 September) [54], where the authors hide data by adding a fixed amplitude PN sequence to the image. They added fixed amplitude two dimensional PN sequence obtained from a long ID PN sequence to the image.

In Tanaka et. al., (1990) [38] the watermarking algorithms used a predictive coding scheme to embed the watermark into the image. Using the statistical properties of the image, the watermark was embedded into the image by dithering the image. In Schyndel et. al., (1994) [52] and Pitas and Kaskalis (1995) [56] an image is randomly split into two subsets of equal size. The mean value of one of the subsets is increased by a constant factor *k*. In effect, the scheme adds high frequency noise to the image. In Bruyndonckx et. al., (1995)[57] the watermark for an image is generated by modifying the luminance values inside 8x8 blocks of pixels and adding one extra bit of information to each block. The encoder secretly makes the choice of the modified block.

In general, the watermarking approaches that modify the LSB of the data are highly sensitive to signal processing operations and are easily corrupted.

4.2 Transform Domain Techniques

Many transform-based watermarking techniques have been proposed. To embed a watermark, a transformation is first applied to the host data, and then modifications are made to the transform coefficients. The works presented in Boland et. al., (1995) [58], Cox et. al., (1995 & 1996) [39] [40], Ruanaidh et. al., (1996 August & 1996 September) [45] [46], Bors and Pitas (1996 September)[47], Hartung and Girod (1996 October) [23], Nikolaidis and Pitas (1996 May), [49] and Tilki and Beex (1997) [50] can be considered to be the pioneer works that utilized the transform domain for the watermarking process. These papers were published at early stages of development of watermarking algorithms. Though these algorithms are not robust enough for watermarking copyright protection, they represented a basic framework for this research. The section has been divided into three main parts viz. wavelet decomposition techniques, discrete cosine transform techniques and fractal transform techniques.

4.3 Wavelet Decomposition Techniques

Many papers proposed to use the wavelet transformation for watermarking because of invisibility and the robustness of the digital watermark can be gained by using this approach. A perceptually based technique for watermarking images was proposed in Wei et. al., (1998 November) [51]. The watermark was inserted in the wavelet coefficients and its amplitudes were controlled by the wavelet coefficients so that watermark noise does not exceed the just-noticeable difference of each wavelet coefficient. Meanwhile, the order of inserting watermark noise in the wavelet coefficients was the same as the order of the visual significance of the wavelet coefficients. Zhu et. al., (1998 October) [59] proposed to implement a four-level wavelet decomposition using Gaussian sequence watermark of pseudo-random real numbers. The detail sub-band coefficients are watermarked. This algorithm can easily be built into video watermarking applications based on a three dimensional wavelet transform due to its simple structure. The algorithm was resilient against compression but robustness against rotation and other geometric attacks were not investigated. The major drawback of these algorithms was that the security was not guaranteed as one can extract the watermark statistically once the algorithm is known by the attackers.

The approach used in Wolfgang et. al., (1998 October & 1999 July) [60] [61] was a four-level wavelet decomposition using 7/9-bi-orthogonal filters. The original image was needed for watermarking extraction. Also, Wolfgang et. al., (1998 October) [60]compared the robustness of watermarks embedded in the DCT and the DWT domains when subjected to lossy compression attack. They found that it is better to match the compression and watermarking domains. However, they incorporated watermark across the image, which may lead to loss of the watermarking coefficient inserted in the insignificant parts of the host image.

Dugad et. al., (1998 October) [62] used a Gaussian sequence of pseudo-random real numbers as a watermark and inserted them in a few selected significant coefficients. They exploited wavelet transformation with three-level decomposition using Daubechies-8 filters. For imperceptibility, the algorithm selected coefficients from detail sub-bands whose magnitude is above a given threshold. However, these locations are prone to modifications by compression or other common signal processing attacks, which reduces the robustness of the algorithm. Inoue et. al., (1998 October & 2000 October) [64] [63] suggested the use of a three-level decomposition using 5/3 symmetric short kernel filters or Daubechies- 16 filters. Experimental results showed that the proposed method gives the watermarked image of better quality compared to other algorithms existing at that time.

Xia et. al., (1997 September) [65] proposed an algorithm using two-level decomposition with Haar wavelet filters whereby most of the watermark was inserted in edges and textures. This enhanced invisibility of the watermarking process because the human eye is less sensitive to changes in edge and texture information. Further, only pseudo-random codes were added to the large coefficients at the high and middle frequency bands of the DWT of an image. Also, it was shown that this method was robust to some common image distortions. However, low pass and median filters will affect the robustness of the algorithm since most of the watermarking coefficients are in the high frequency coefficients of the host signal. Xie and Arce (1998 October) [66] developed a watermarking approach that decomposed the host image to get a low-frequency approximation representation. The watermark was a binary sequence and was embedded in the approximation image. This algorithm was designed for both image authentication applications and copyright protection. More number of decomposition increases algorithm’s robustness. Very good robustness can be achieved by deploying five-level wavelet decomposition, but is costly from the computational point of view.

Kundur and Hatzinakos (1997 September) [67] developed an algorithm for still image watermarking in which logo image, which was 2^m smaller than the host image, was used as watermark. The watermark embedding process employed multi-resolution fusion techniques and incorporated a model of the human visual system. Both the original image and the watermark were transformed into the DWT domain before embedding. Simulation results demonstrated robustness of the algorithm to common image distortions but were not robust to rotations. Kundur and Hatzinakos (1998) [68] proposed to apply the Daubechies family of orthogonal wavelet filters to decompose the original image to three-level multi-resolution representation. Also, Kundur and Hatzinakos (1998 October) [69] proposed a fragile watermark. They called the technique as telltale tamper-proofing method. Their design embedded the fragile watermark in the discrete wavelet domain of the signal by quantizing the corresponding coefficients with user-specified keys. The watermark was a binary signature, which was embedded into key-selected detail sub-band coefficients.

Podilchuk and Zeng (1998 May) [70] proposed two watermarking techniques for gray scale digital images that were based on utilizing visual models, which had been developed in the context of image compression. Their schemes were shown to provide very good results both in terms of image transparency and robustness.

Chae et. al., (1998) [71] and Chae and Manjunath (1998 January) [26] proposed a gray scale image watermarking technique, with a limitation that the watermark size can be as much as 25% of the host image size. They suggested using only one-level decomposition on both the host and the logo image. Their experimental results showed that the watermarked image was transparent to embedding and the quality of the extracted signature was high even when the watermarked image was subjected to wavelet impression and JPEG lossy compression. Geometric attacks were not studied in this work. The capacity issue with this scheme can be considered as trade-off between the quantity of hidden data and the quality of watermarked image.

Kim et. al., (1999 March) [30] proposed to insert a watermark into the large coefficients in each DWT band. Experimental results showed that the proposed three-level wavelet based watermarking method is robust against attacks like JPEG compression, smoothing, and cropping. Robustness against geometric distortions such as resizing and rotation was not discussed. The algorithm selected perceptually significant coefficients, for watermarking, by applying level-adaptive threshold scheme as given in Kim and Moon (1999 October)[28]. The proposed approach in Kim and Moon (1999 October) [28] decomposed the original image into three levels by applying bi-orthogonal filters. The experimental results showed that the embedding was invisible to human eyes and robust to various attacks but not geometric transformations.

The paper didn't address the possibilities of repetitive watermark embedding or watermark embedding weight to increase robustness.

A method for multi-index decision (maximizing deviation method) based watermarking was proposed in Zhihui and Liang (2000 July) [31]. This watermarking technique was designed and implemented in the DCT domain as well as the wavelet domain utilizing HVS (Human Visual System) models. Tsekeridou and Pitas (2000 May) [32] presented watermarks that were structured in such a way as to attain spatial self-similarity with respect to a Cartesian grid. Their scheme was implemented in the wavelet domain. Loo and Kingsbury (2000 April) [33] proposed a watermarking algorithm in the complex wavelet domain and modeled watermarking as a communication process. It was shown that the complex wavelet domain has relatively high capacity for embedding information in the host signal. They concluded that the complex wavelet domain is a good domain for watermarking. However, it is computationally very expensive.

Ejim and Miyazaki (2000 October) [34] suggested the technique using a wavelet packet of image and video watermarking. The energy for each sub-band was calculated. Then, certain sub-bands are pseudo-randomly selected according to their energy. These types of algorithms generate redundant information since the wavelet packet generates details and approximation sub-band for each resolution, which adds to the computation overhead.

4.4 Discrete Cosine Transform Techniques

In the very early days, Discrete Cosine Transformation was widely studied by the source coding community in the context of JPEG and MPEG compression Wallace (1992) [35], Pennebaker and Mitchell (1992) [36] and Rao and Yip (1990) [37]. Later, it was also considered to embed a message inside images (Koch and Zhao 1995 [7] , Zhao 1996 [9]) and videos (Matsui and Tanaka, 1994 [55]). The main arguments for using DCT in watermarking are the following:

- Embedding rules operating in the DCT domain is often more robust to JPEG and MPEG compression; thus the watermark designer can prevent JPEG/MPEG attacks more easily.
- The studies on visibility (i.e., visual distortions) can be reused; these studies help to predict the visible impact of the watermark on the cover-image.
- Watermarking in the DCT domain offers the possibility of directly realizing the embedding operator in the compressed domain (i.e., inside a JPEG or MPEG encoder) in order to minimize the computation time.

Several watermarking algorithms have been proposed to utilize the discrete cosine transformation. However, Cox et. al., (1995 & 1997 December) [39] [42] and Koch and Zhao (1995) [7] algorithms are the most well-known DCT-based algorithms. Cox et. al., (1995) [39] proposed the well-known spread spectrum watermarking schemes. The image was first subjected to a global discrete cosine transformation. Then, the 1,000 largest coefficients in the DCT domain were selected for watermarking. They used a Gaussian sequence of pseudo-random real numbers of length 1,000 as a watermark. This approach achieves good robustness against compression and other common signal processing attacks. This was the result of selection of perceptually significant transform domain coefficients. However, the algorithm was weak against the invariability attack proposed by Craver (1997 October) [43]. Also, the global DCT employed on the image is computationally expensive. Cox et. al., (1996 September) [41] described the technique for applying digital watermarks to both video and audio signals. The mark was inserted using discrete cosine transform technique into the perceptually most significant spectral coefficients of the signal using the concept of spread spectrum communications. They showed that marks can still be recovered after various common processing operations including scaling, JPEG compression, dithering and clipping. Hsu and Wu (1999 January) [44] also proposed gray scale image watermarking using DCT transformation. They incorporated binary image as the watermark into the middle frequency parts of the original image. The results reflected sustainability to JPEG compression.

Koch and Zhao (1995) [7] proposed to use a sequence of binary values, as a watermark. This approach modified the difference between randomly selected mid-frequency components in random image blocks. They picked pseudo-randomly 8x8 DCT coefficient blocks. From each block, two coefficients in the mid-frequency range were pseudo-randomly selected. Each block was quantized using the JPEG quantization matrix and a quantization factor. This was not a robust algorithm because only two coefficients were watermarked from each block. The algorithm was not robust against scaling or rotation because the image dimensions were used to generate an appropriate pseudo-random sequence. Also, visible artifacts may be produced because the watermark was inserted in 8x8 DCT domain coefficient blocks. These artifacts may be seen more in smooth regions than in edge regions.

Swanson et. al., (1996 September) [17] proposed a DCT based watermarking scheme for images that used the properties of human visual system. The watermark was a PN-sequence that is shaped using frequency masking. Ruanaidh et. al., (1996 August) [46] presented a DCT based private invisible watermarking technique for still images. The watermark was embedded by modulating the DCT coefficients with a bi-directional coding. A technique to determine the number of bits to be placed at a given location was also presented. Barni et. al., (1998) [76] proposed a digital watermarking algorithm similar to Cox's method. However, the mark was inserted in the same set of DCT coefficients after the usual zigzag ordering, instead of using the 1000 largest DCT coefficients as Cox does. To achieve perceptual invisibility, only middle frequencies were modified. The method survived JPEG compression, low-pass filtering, cropping and rescaling. Bors and Pitas (1998) [48] proposed watermarking algorithm based on imposing constraints in the DCT domain. Random image blocks were selected via a Gaussian network classifier and DCT coefficients in these blocked were modified to satisfy some predefined constraints. The original image was not required for watermark detection and simulations showed this method is resistant to JPEG compression and filtering.

Some of the other major contributions in the area noted are Bors and Pitas (1996 September) [47], Piva et. al., (1997 September) [72], Tang and Aoki (1997) [74], Barni et. al., (1997) [75], Tao and Dickinson (1997)[77] , Goutte and Baskurt (1998) [78], Duan et. al., (1998) [79], Huang and Shi

(1998 April) [80] Kankanhalli and Ramakrishnan (1999) [81], Kang and Aoki (1999) [82] and Kim et. al., (1999) [29].

4.5 Fractal Transform Techniques

Though a lot of work has been done in the area of invisible watermarks using the DCT and the wavelet -based methods, a relatively few references exist for invisible watermarks based on the fractal transform. The reason for this might be the computational expense of the fractal transform. Discussions of fractal watermarking methods were presented in Puate and Jordan (1996 November) [83], Roche and Dugelay (1998) [84] and Bas et. al., (1998 October) [85]. Puate and Jordan (1996 November) [83] used fractal compression analysis to embed a signature in an image. In fractal analysis, similar pattern were identified in an image and only a limited amount of binary code can be embedded using this method. Since fractal analysis is computationally expensive and some images do not have many large self-similar patterns, the technique may not be suitable for general use.

4.6 Feature Domain Techniques

These techniques focused on image region, boundary and characteristics, like flat regions, textures, and edges etc., for watermarking. This gives an additional advantage in terms of detection and recovery from geometric attacks compared to other methods. Also, these algorithms may be designed so that selective robustness to different classes of attacks is obtained. As a result, watermark flexibility will be improved considerably. Kutter et. al., (1999 October) [86] used feature point extraction and the Voronoi diagram as an example to define region of interest (ROI) to be watermarked. The feature extraction process is based on a decomposition of the image using Mexican-Hat wavelet. The stability of the method proposed in Kutter's work depends on the features points. These extracted features have the drawback that their location may change by some pixels because of attack or during the watermarking process which will cause problems during the detecting process. Kutter classified this technique as second generation watermarking.

Later in 2000, ICIP organized a special session on second-generation digital watermarking algorithms Baudry et. al., (2000 October) [87], Eggers et. al., (2000 October) [88], Furon and Duhamel (2000 October) [89] , Loo and Kingsbury(2000 April) [33], Lu and Liao (2000 October)[91], Miller et. al., (2000 October)[92], Piva et. al., (2000 October) [73] and Solachidis et. al., 2000 October) [93]. Eight papers were presented in this session. This special session was intended to provide researchers with the opportunity of presenting the latest research results on second-generation digital watermarking.

In Solachidis (2000 October)[93] the properties of the-Fourier descriptors were utilized in order to devise a blind watermarking scheme for vector graphics images. With this approach, the watermarking method will be robust to a multitude of geometric manipulations and smoothing. But the results showed weak robustness and required improvement more in this direction.

A new modulation scheme was proposed by Lu et. al., (2000 July)[90] and Lu and Liao (2000 October)[91]. Half of the watermark was positively embedded and the other half was negatively embedded. This approach can be applied to all spread spectrum watermarking algorithms. It performed better than random insertion. Security issues and geometric attacks were not considered in the design of this algorithm. Also, Lu and Liao (2000 October) [91] used the same approach to propose a semi-blind watermark extraction. The original image was not required at the detection side; only a set of image-dependent parameters was needed. These parameters described the wavelet coefficient probability distribution that originally has been embedded.

5. Summary

It is apparent that the digital watermarking can be achieved by using either transform techniques i.e. embedding the watermark data into the frequency domain representation of the host image or by directly embedding the watermark into the spatial domain data of the image. The discussion shows that creating robust watermarking methods is still a challenging research problem. The algorithms developed are robust against some attacks but not against others. Also, some of the current methods are designed to suit only specific application, which limits their widespread use. Moreover, there are drawbacks in the existing algorithms associated with the watermark-embedding domain. These drawbacks vary from system to system. Watermarking schemes that modify the LSB of the data using a fixed magnitude PN sequence are highly sensitive to signal processing operations and are easily corrupted. Some transform domain watermarking algorithms cannot survive most image processing operations and geometric manipulations. Using fractal transforms, only a limited amount of binary code can be embedded. Since fractal analysis is computationally expensive, and some images do not have many large, self-similar patterns, fractal-based algorithms may not be suitable or practical for general use. Feature domain algorithms suffer from problems of stability of feature points if they are exposed to an attack. Security is an issue facing most of the algorithms reviewed.

Digital watermarking is claimed to be the ultimate solution for copyright protection over Internet. However, some problems related to robustness and security of watermarking algorithms to intentional or unintentional attacks still remain unsolved and needs to be addressed.

6. References

[1] Anderson, R. J., and Petitcolas, F. A. P. (1998). On the limits of steganography. IEEE Journal of Selected Areas in Communications (Special issue on copyright & privacy protection.), vol. 16(4) pp. 474–481

[2] Petitcolas, F.A.P., Anderson, R.J., and Kuhn, M.G. (1999). Information hiding – a survey. *Proceedings of the IEEE (USA)*, vol. 87(7), pp. 1062–1078.

[3] Kahn, D. (1996a). The Codebreakers – The story of secret writing. Scribner, New York, U.S.A., 1996. ISBN 0-684-83130-9.

[4] Kahn, D. (1996b). The history of steganography. *Proceedings of the 1st international workshop on Information Hiding*, pp 1–5.

[5] Leary, T. (1996). Cryptology in the 15th and 16th century. Cryptologia, vol. 20(3), pp. 223–242.

[6] Pfitzmann, B. (1996). Information Hiding Terminology - Results of an Informal Plenary Meeting and Additional Proposals. Information Hiding, pp 347–350.

[7] Zhao, J., and Koch, E. (1995, August). Embedding robust labels into images for copyright protection. *Proceeding of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna*, pp. 1–10.

[8] Zhao, J. (1997). Look, it's Not There – Digital watermarking is the best way to protect intellectual property from illicit copying. BYTE.COM. http://www.byte.com/art/9701/sec18/art1.htm

[9] Zhao, J. (1996). A WWW Service to Embed and Prove Digital Copyright Watermarks. *Proceedings of the European Conference on Multimedia Applications, Services and Techniques*, pp. 695–709.

[10] Voyatzis, G., Nikolaidis, N., and Pitas, I. (1998). Digital watermarking: an overview. *9th European Signal Processing Conference (EUSIPCO'98), Island of Rhodes, Greece, 8–11 Sept. 1998*, pp. 9–12. ISBN: 960-7620-05-4.

[11] Lacy, J., Quackenbush, S. R., Reibman, A., and Snyder, J. H. (1998). Intellectual property protection systems and digital watermarking. *Optics Express*, vol. 3(12). pp. 478–484.

[12] Gruhl, D., Lu, A., and Bender, W. (1996). Echo hiding. *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 295–315.

[13] Chang, L.W., and Moskowitz, I. S. (1997). Critical Analysis of Security in Voice Hiding Techniques. *Information and Communications Security – First International Conference, Beijing, China, ICICS'97*, pp. 203-216.

[14] Boney, L., Tewfik, A. H., and Hamdy, K. N. (1996). Digital watermarks for audio signals. *IEEE- International Conference on Multimedia Computing and Systems, Hiroshima, Japan*, pp. 473–480.

[15] Swanson, M.D., Zhu, B., Tewfik, A.H., and Boney, L. (1998a). Robust audio watermarking using perceptual masking. *Signal Processing. European Association for Signal Processing (EURASIP)*, vol. 66(3), pp.337–355.

[16] Swanson, M. D., Zhu, B. and Tewfik, A.H. (1998b). Multiresolution scene based video watermarking using perceptual models. IEEE Journal on Special Areas in Communications, vol. 16(4), pp. 540–550.

[17] Swanson, M.D., Zhu, B., and Tewfik, A.H. (1996, September). Transparent robust image watermarking. *International Conference on Image Processing Proceedings*, ICIP 96, pp. 211–214.

[18] Neubauer, C., and Herre, J. (1998). Digital Watermarking and its Influence on Audio Quality. *105th Convention of the Audio Engineering Society, San Francisco, California, U.S.A*, pp.1–16.

[19] Bassia, P., and Pitas, I. (1998). Robust audio watermarking in the time domain. *9th European Signal Processing Conference (EUSIPCO'98)*, pp. 25–28.

[20] Bassia, P., Pitas, I., and Nikolaidis, N. (2001). Robust audio watermarking in the time domain. *IEEE Transactions on Multimedia*. vol 3(2) pp. 232–241.

[21] Tay, D.B.H., Abeysekera, S.S. and Balasuriya, A.P. (2003). Audio Signal Processing via Harmonic Separation using Variable Laguerre Filters. *IEEE*, pp. III-558–III-561

[22] Hafiz, M., Khokhar, A. and Ansari, R. (2004). Robust audio watermarking using frequency selective spread spectrum theory. *IEEE ICASSP*, pp 385–388.

[23] Hartung, F., and Girod,B. (1996, October). Digital watermarking of raw and compressed video. *Proceeding of the SPIE Digital Computing Techniques and Systems for Video Communication*, vol. 2952, pp. 205–213.

[24] Hartung, F., and Girod, B. (1998). Watermarking of uncompressed and compressed video. Signal Processing – European Association for Signal Processing (EURASIP), vol. 66(3), pp. 283–301.

[25] Dittmann, J., Stabenau, M., and Steinmetz, R. (1998). Robust MPEG video watermarking technologies. *Proceedings of the sixth ACM international conference on Multimedia Bristol, United Kingdom*, pp 71–80. ISBN:0-201-30990-4.

[26] Chae, J. J., and Manjunath, B.S. (1998, January). A robust embedded data from wavelet coefficients. *Proceeding of SPIE, Electronic Imaging, Storage and Retrieval for Image and Video Database*, vol. 3312, pp. 308–317.

[27] Chae, J.J., and Manjunath, B.S. (1999). Data hiding in video. IEEE, pp. 311–315.

[28] Kim, J.R., and Moon, Y.S. (1999, October). A robust wavelet-based digital watermarking using level-adaptive thresholding. *International Conference on Image Processing Proceedings*, ICIP 99, vol. 2, 226–230.

[29] Kim, S.W., Suthaharan, S., Lee, H.K., and Rao, K.R. (1999). Image watermarking scheme using visual model and BN distribution. *Electronics Letters*, vol. 35(3), 212–214.

[30] Kim, Y.S., Kwon, O.H., and Park, R.H. (1999, March). Wavelet based watermarking method for digital images using the human visual system. *Electronics Letters*, vol. 35(6), 466–468.

[31] Zhihui, W., and Liang, X. (2000, July). An evaluation method for watermarking techniques. *IEEE International Conference on Multimedia and Expo*, ICME 2000, vol. 1, pp. 373–376.

[32] Tsekeridou, S., and Pitas, I. (2000, May). Wavelet-based self-similar watermarking for still images. *The IEEE International Symposium on Circuits and Systems*, ISCAS 2000, vol. 1, pp. 220–223.

[33] Loo, P., and Kingsbury, N. (2000, April). Digital watermarking with complex wavelets. *IEE Seminar on Secure Images and Image Authentication*, pp. 10/1–10/7.

[34] Ejim, M., and Miyazaki, A. (2000, October). A wavelet-based watermarking for digital images and video. *International Conference on Image Processing*, ICIP 2000, vol. 3, pp. 678–681.

[35] Wallace, G.K. (1992). The JPEG Still Picture Compression Standard. *IEEE Transaction on Consumer Electronics*, vol. 38(1), pp. 18–34.

[36] Pennebaker, W. B., and J. L. Mitchell (1992), *JPEG Still Image Data Compression Standard*, New York: Van Nostrand Reinhold Company.

[37] Rao, K. R., and P. Yip (1990), *Discrete Cosine Transform: Algorithms, Advantages, Applications*, New York: Academic Press.

[38] Tanaka, K., Nakamura, Y., and Matsui, K. (1990). Embedding secret information into a dithered multi-level image. *Proceeding of IEEE Military Communications Conference*, pp. 216–220.

[39] Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1995). Secure spread spectrum watermarking for multimedia. *Technical Report 95-10, NEC Research Institute*, pp. 1–33.

[40] Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1996). A secure, robust watermark for multimedia. *Information Hiding, Springer Lecture Notes in Computer Science*, vol. 1174, pp. 183–206.

[41] Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1996, September). Secure spread spectrum watermarking for images, audio and *video. International Conference on Image Processing Proceedings*, ICIP 96, vol. 3, pp. 243–246.

[42] Cox, I.J., Kilian, J., Leighton, F.T., and Shamoon, T. (1997, December). Secure spread spectrum watermarking for multimedia. *IEEE Transaction Image Processing*, vol. 6(12), pp. 1673–1687.

[43] Craver, S., Memon, N., Yeo, B., and Yeung, M. (1997, October). On the invertibility of invisible watermarking techniques. *International Conference on Image Processing Proceedings*, ICIP 97, pp. 540–543.

[44] Hsu, C., and Wu, J. (1999 January). Hidden digital watermarks in images. IEEE transactions on image processing, vol. 8(1), pp. 58–68.

[45] Ruanaidh, J.J.K.Ó., Boland, F., and Dowling, W. (1996, September). Phase watermarking of digital images. *International Conference on Image Processing Proceedings,* ICIP 96, pp. 239–242.

[46] Ruanaidh, J.J.K.Ó., Dowling, W.J., and Boland, F.M. (1996, August). Watermarking digital images for copyright protection. *IEE Proceedings on Vision, Signal and Image Processing,* vol. 143(4), pp. 250–256.

[47] Bors, A., and Pitas, I. (1996, September). Image watermarking using DCT domain constraints. *International Conference on Image Processing Proceedings,* ICIP 96, pp. 231–234.

[48] Bors, A., and Pitas, I. (1998). Image watermarking using block site selection and D.C.T. domain constraints. *Optics Express.* vol. 3(12) pp. 512–523.

[49] Nikolaidis, N., and Pitas, I. (1996, May). Copyright protection of images using robust digital signatures. *Proceeding of IEEE Conference Acoustics,* Speech *& Signal Processing,* pp. 2168–2171.

[50] Tilki, J.F., and Beex, A.A. (1997). Encoding a hidden digital signature onto an audio signal using psychoacoustic masking. *IEEE Southeastcon 97, Blacksburg, VA,* pp. 331–333.

[51] Wei, Z.H.. Qin, P., and Fu, Y.Q. (1998, November). Perceptual digital watermark of images using wavelet transform. *IEEE Transactions on Consumer Electronics,* vol. 44(4), pp. 1267 –1272.

[52] Schyndel, R.G., Tirkel, A.Z., and Osborne, C.F. (1994). A digital watermark. *Proceeding of IEEE International Conference on Image,* vol. 2, pp. 86–90.

[53] Bender, W., Gruhl, D., Morimoto, N., and Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal,* vol. 35(3 & 4), pp. 1–24.

[54] Wolfgang, R.B., and Delp, E.J. (1996, September). A watermark for digital images. *International Conference on Image Processing Proceedings,* ICIP 96, pp. 219–222.

[55] Matsui, K., and K. Tanaka (1994). Video-steganography: How to Secretly Embed a Signature in a Picture. *Journal of the Interactive Multimedia Association Intellectual Property Project,* vol. 1(1), pp. 187–206

[56] Pitas, L, and Kaskalis, T. (1995). Applying signatures on digital images. *Proceeding of IEEE Nonlinear Signal Processing Workshop,* pp. 460–463.

[57] Bruyndonckx, O., Quisquater, J.J., and Macq, B. (1995). Spatial -method for copyright labeling of digital images. *Proceeding of IEEE Nonlinear Signal Processing Workshop,* pp. 456-459.

[58] Boland, F., Ruanaidh, J.O., and Dautzenberg, C. (1995). Watermarking digital images for copyright protection. *Proceeding of IEE International Conference on Image Processing and Its Applications,* pp. 321–326.

[59] Zhu, W., Xiong, Z., and Zhang, Y. (1998, October). Multiresolution watermarking for images and video: A unified approach. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 1, pp. 465–468.

[60] Wolfgang, R.B., Podilchuk, C.I., and Delp, E.J. (1998, October). The effect of matching watermark and compression transforms in compressed color images. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 1, pp. 440–444.

[61] Wolfgang, R.B., Podlchuk, C.I., and Delp, E.J. (1999, July). Perceptual watermarks for digital images and video. *Proceedings of IEEE Special Issue on Identification and Protection of Multimedia Information,* vol. 7, pp. 1108–1126.

[62] Dugad, R., Ratakonda, K., and Ahuja, N. (1998, October). A new wavelet-based scheme for watermarking images. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 2, pp. 419–423

[63] Inoue, H., Miyazaki, A., and Katsura, T. (2000, October). Wavelet-based watermarking for tamper proofing of still images. *International Conference on Image Processing Proceedings,* ICIP 2000, pp. 88–91.

[64] Inoue, H., Miyazaki, A., Yamamoto, A., and Katsura, T. (1998, October). A digital watermark based on the wavelet transform and its robustness on image compression. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 2, pp. 391–395.

[65] Xia, X., Boncelet, C.G., and Arce, G.R. (1997, September). A multiresolution watermark for digital images. *International Conference on Image Processing Proceedings,* ICIP 97, vol. 1, pp. 548–551.

[66] Xie, L., and Arce, G.R. (1998, October). Joint wavelet compression and authentication watermarking. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 2, pp. 427–431.

[67] Kundur, D., and Hatzinakos, D. (1997, September). A robust digital image watermarking method using wavelet-based fusion. *International Conference on Image Processing Proceedings,* ICIP 97, vol. 1, pp. 544–547.

[68] Kundur, D., and Hatzinakos, D. (1998). Digital watermarking using multiresolution wavelet decomposition. *International Conference on Acoustics, Speech and Signal Processing Proceedings,* vol. 5, pp. 2969–2972.

[69] Kundur, D., and Hatzinakos, D. (1998, October). Towards a telltale watermarking technique for tamper-proofing. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 2, pp. 409–413.

[70] Podilchuk, C.I., and Zeng, C.W. (1998, May). Image-adaptive watermarking, using visual models. *IEEE Journal on Selected Areas in Communications,* vol. 16(4), pp. 525–539.

[71] Chae, J.J., Mukherjee, D., and Manjunath, B.S. (1998). A robust data hiding technique using multidimensional lattices. *Proceedings IEEE International Forum on Research and Technology Advances in Digital Libraries,* ADL 98, pp.319–326.

[72] Piva, A., Barni, M., Bartolini, F., and Cappellini, V. (1997, September). DCT based watermark recovering without resorting to the uncorrupted original image. *International Conference on Image Processing Proceedings,* ICIP 97, pp. 520–523.

[73] Piva, A., Caldelli, R., and De Rosa, A. (2000, October). A DWT-based object watermarking system for MPEG-4 video streams. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 5–8.

[74] Tang, W., and Aoki, Y. (1997). A DCT-based coding of images in watermarking. *Proceedings of International Conference on Information, Communications and Signal Processing,* ICICS97, vol. 1, pp. 510–512.

[75] Barni, M., Bartolini, F., Cappellini, V., and Piva, A. (1997). Robust watermarking of still images for copyright protection. *13th International Conference on Digital Signal Processing Proceedings,* DSP 97, vol. 1, pp. 499–502.

[76] Barni, M., Bartolini, F., Cappellini, V., and Piva, A. (1998). A D.C.T.-domain system for robust image watermarking. *Signal Processing*. European Association for Signal Processing (EURASIP), vol. 66(3) pp. 357–372

DOI: 10.18535/ijecs/v4i9.60

[77] Tao, B., and Dickinson, B. (1997). Adaptive watermarking in the DCT domain. *IEEE International Conference on Acoustics, Speech, and Signal Processing,* ICASSP 97, vol. 4, pp. 2985–2988.

[78] Goutte, R., and Baskurt, A. (1998). On a new approach of insertion of confidential digital signature into images. *Proceedings of Fourth International Conference on Signal Processing,* ICSP 98, vol. 2, pp. 1170–1173.

[79] Duan, F.Y., King, I., Chan, L.W., and Xu, L. (1998). Intra-block min-max algorithm for embedding robust digital watermark into images. *Multimedia Information Analysis and Retrieval,* pp. 255–264.

[80] Huang, J., and Shi, Y.Q. (1998, April). Adaptive image watermarking scheme based on visual masking. *Electronics Letters,* vol. *34(8), pp.* 748–750.

[81] Kankanhalli, M., and Ramakrishnan, K. (1999). Adaptive visible watermarking of images. *IEEE International Conference on Multimedia Computing and Systems,* vol. 1, pp. 568–573.

[82] Kang, S., and Aoki, Y. (1999). Image data embedding system for watermarking using Fresnel transform. *IEEE International Conference on Multimedia Computing and Systems,* vol. 1, pp 885–889.

[83] Puate, J., and Jordan, F. (1996, November). Using fractal compression scheme to embed a digital signature into an image. *Proceedings of SPIE Photonics East'96 Symposium*, pp.1–12.

[84] Roche, S., and Dugelay, J. (1998). Image watermarking based on the fractal transform: A draft demonstration. *IEEE Second Workshop on Multimedia Signal Processing,* pp. 358–363.

[85] Bas, P., Chassery, J., and Davoine, F. (1998, October). Using the fractal code to watermark images. *International Conference on Image Processing Proceedings,* ICIP 98, vol. 1, pp. 469–473.

[86] Kutter, M., Bhattacharjee, S.K., and Ebrahimi, T. (1999, October). Towards second generation watermarking schemes. *International Conference on Image Processing Proceedings,* ICIP 99, vol. 1, pp. 320–323.

[87] Baudry, S., Nguyen, P., and Maitre, H. (2000, October). Channel coding in video watermarking: Use of soft decoding to improve the watermark retrieval. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 25–28.

[88] Eggers, J.J., Su, J.K., and Girod, B. (2000, October). Robustness of a blind image watermarking scheme. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 17–20.

[89] Furon, T., and Duhamel, P. (2000, October). Robustness of asymmetric watermarking technique. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 21–24.

[90] Lu, C.S., Liao, H.Y., and Sze, C.J. (2000, July). Combined watermarking for image authentication and protection. *IEEE International Conference on Multimedia and Expo,* ICME 2000, vol. 3, pp. 1415–1418.

[91] Lu, C.S., and Liao, H.Y. (2000, October). Oblivious cocktail watermarking by, sparse code shrinkage: A regional and global-based scheme. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 13–16.

[92] Miller, M., Cox, L, and Bloom, J. (2000, October). Informed embedding exploiting image and detector information during watermark insertion. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 1–4.

[93] Solachidis, V., Nikolaidis, N., and Pitas, I. (2000, October). Fourier descriptors watermarking of vector graphics images. *International Conference on Image Processing Proceedings,* ICIP 2000, vol. 3, pp. 9–12.