A Study on Watermarking Schemes for Image Authentication

S. Radharani
Lecturer,
Dept. of Comp. Science,
Sree Narayana Guru College, CBE

Dr. M.L. Valarmathi, Ph.D.
Asst. Professor,
Dept. of Comp. Science & Engg.,
Govt. College of Technology, CBE

Abstract

The digital revolution in digital image processing has made it possible to create, manipulate and transmit digital images in a simple and fast manner. The adverse affect of this is that the same image processing techniques can be used by hackers to tamper with any image and use it illegally. This has made digital image safety and integrity the top prioritized issue in today's information explosion. Watermarking is a popular technique that is used for copyright protection and authentication. This paper presents an overview of the various concepts and research works in the field of image watermark authentication. In particular, the concept of content-based image watermarking is reviewed in details.

Keywords- Watermark Lifecycle, Robust Watermarking Schemes, Fragile Watermarking Schemes, HVS, ICA.

1. Introduction

The rapid growth in the digital technology, image processing and Internet has made the reproduction of digitally created information simple and easy. The advancement in World Wide Web, MMS communication has made it possible to transmit and distribute this digitally created information in a fast and easy manner without any quality degradation. This new trend has several advantages which includes flexibility, cost effectiveness, etc., but at the same time, also possess some serious drawbacks. It allows hackers to manipulate / duplicate / access information illegally without the owners' knowledge. This has created a great concern on digital content security and is being studied seriously by several academicians and researchers [32]. In response to these challenges, digital watermarking schemes have been proposed in the last decade, where a small amount of imperceptible secret information is embedded into the digital content, which can be extracted at a later stage for copyright assertion, copy control, broadcasting, authentication, content integrity verification, etc [55].

Digital watermarking has been investigated deeply for its technical and commercial feasibility in all media types like, digital photographic image [31], audio [42], printed materials or compound document images [26], video [22], etc. It is a proven method for reducing content piracy and improving the ability to identify, tract and manage digital media [13]. It is widely used in applications of rights management, remote triggering, filtering/classification, e-commerce, etc. It is a technique that is used to balance the need for content security with best possible consumer experience to enable media and entertainment industries to adapt the advanced facilities of the modern digital revolution while reducing the threat of content theft.

In [45] watermarking is defined as a technique which embeds data into digital contents such as text, still images, video and audio data without degrading the overall quality of the digital media. A watermark is the information to be hidden and also indicates that the hidden information is transparent, while the term cover media indicates the media used for carrying the watermark. The watermarked data is the media which contains the watermark. In digital watermarking technology, the phrase embedding and extraction means the procedures used for inserting the watermark into the cover media and extracting the embedded watermark from the watermarked data respectively. Detection is an important process that is used for detecting whether the given media containing a particular watermark.

Several types of watermarking schemes have been proposed for handling different applications. Examples include

(1). copyright-related applications [3], [36], [43], [48] where the embedded watermark are robust

(2). medical, forensic, and intelligence or military applications [4], [27], [30], [51] [53] where the watermark are usually fragile or semi-fragile

(3). Content authentication applications [2], [47] where any tiny changes to the content are not acceptable, the embedding distortion has to be compensated for perfectly.

Digital watermarking techniques originally focused on copyright protection, but have been exploited in wide range of applications [49]. There are several categories of watermarking schemes that are designed for different applications. Among them, robust watermarks are generally used for copyright protection and ownership identification because they are designed to withstand attacks such as common image processing operations. In contrast, fragile or semi-fragile watermarks are mainly applied to content authentication and integrity attestation because they are fragile to attacks, i.e., it can detect any changes in an image as well as localizing the areas that have been changed. Both these techniques are to be treated separately and this paper deals with content based watermarking system for authentication.

The paper is organized as below. Section 1 provides an introduction to watermarking systems, Section 2 describes a general model of watermarking systems, Section 3 discusses the watermark classification and Section 4 presents a review on content based watermarking. A brief conclusion with future direction is presented in Section 5.

2. Generic Watermarking System

Digital watermarking algorithms are composed of three parts, namely, watermark embedding algorithm, watermark extraction algorithm and watermark detection algorithm [56]. A general watermark system phases is shown in Figure 1.

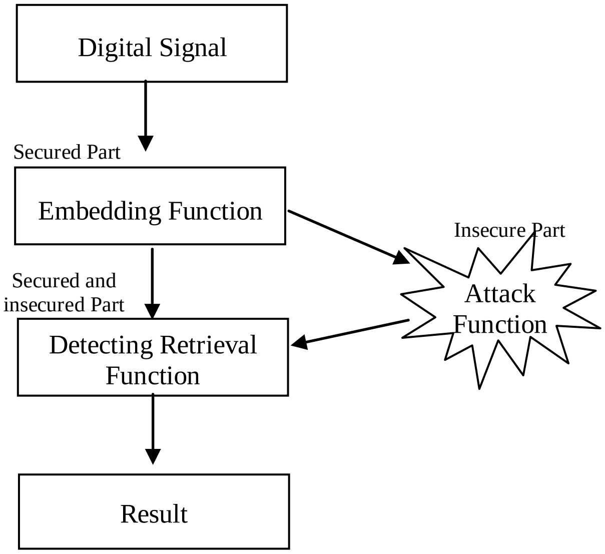

Figure 1: Watermark Lifecycle Phases

During embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored. If a person makes a modification, then the digital content is said to be attacked. A watermark attack is an attack on digital data where the presence of a specially crafted piece of data can be detected by an attacker without knowing the encryption key. Special attention has to be paid to the kind of attacks as they can help to develop better watermarking techniques and defined better benchmarks. According to [17], watermark attacks can be classified into four main groups:

(i) Simple attacks: These types of attacks attempt to damage the embedded watermark by modifications of the whole frame without any effort to identify and isolate the watermark. Examples include frequency based compression, addition of noise, cropping and correction.

(ii) Detection-disabling attacks: These attempts to break correlation and to make detection of the watermark impossible. Geometric distortion like zooming, shift in spatial or (in case of video) temporal direction, rotation, cropping or pixel permutation, removal or insertion are used.

(iii) Ambiguity attacks: These attacks the detector by producing fake watermarked data to discredit the authority of the watermark by embedding several additional watermarks so that it is not obvious which was the first, authoritative watermark.

(iv) Removal attacks: The removal attacks estimates the watermark, separate it out and discard only the watermark. Examples are collusion attack, denoising or exploiting conceptual cryptographic weakness of the watermark scheme (e.g. knowledge of positions of single watermark elements).

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted. In robust watermarking applications, the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal.

Any watermarking technique has to be evaluated to judge its performance. Three factors, as given below, must be considered while evaluating an image watermarking algorithm.

- Capacity, i.e. the amount of information that can be put into the watermark and recovered without errors;
- Robustness, i.e. the resistance of the watermark to alterations of the original content such as compression, filtering or cropping;
- Visibility, i.e. how easily the watermark can be discerned by the user.

The desired properties are high capacity, low distortion and high robustness to attacks or high security. These factors are inter-dependent; for example, increasing the capacity will decrease the robustness and/or increase the visibility. Therefore, it is essential to consider all three factors for a fair evaluation or comparison of watermarking algorithms.

3. Classification of Watermarking Schemes

Digital watermarking schemes can be broadly classified into four categories, namely, Robust, Fragile, Semi-fragile and Reversible. While, as mentioned previously, imperceptibility, low embedding distortion and security are the common requirements of all classes, each different category of scheme has different characteristics and, thus, is suitable for different applications. For example, while robustness is an essential requirement for copyright applications, it has no role in most authentication applications. This section provides a brief explanation of each of these schemes along with application areas where they can be applied.

3.1. Robust Watermarking Schemes

Robust watermarking algorithm aims at mixing a non-perceptible communication channel with image data, in such a way that the capacity of this extra channel degrades smoothly with the distortion the watermarked content undergoes. This class of schemes has found its applications in many areas, which includes the following.

- **Ownership proof and identification:** A watermark containing the identification information of the content owner can be embedded in the host media for proving or identifying copyright ownership. The working of such a scheme is dealt in several research works [16], [1]. Ambiguous ownership is one problem faced by these watermark applications. Some possible solutions to ambiguous ownership problems are reported by [34].
- **Transaction tracking/fingerprinting:** The copyright owner could inserts a unique watermark, which, for example, identifies the recipient, into each copy of the media and uses it to trace the source should illegal redistribution occur. The main challenge fingerprinting schemes face is the collusion attack in which several legal copies of the same media are obtained to produce an approximation of the original unwatermarked version for illegal redistribution. Some recent proposals for tackling collusion attack can be found in [48] and [44].
- **Copy control/copy prevention:** Illegal copying or recording is another common piracy scenario. One possible solution is to embed a never-copy watermark, that when detected by the detector installed in the recording device, disallows further recording. However, this mechanism requires every recording device to have a watermark detector. It is difficult to persuade the consumers to pay more for a device that restrict their "freedom" of making copies. This commercially undesirable requirement is unlikely to be met without the support of global legislation. This problem is dealt in detail by [5].
- **Broadcast monitoring:** In the advertisement applications, by embedding watermark that is to be broadcasted along with the host media, the advertisers can monitor whether or not the commercials they have paid for are aired by the broadcasters according to the contracts. A detailed explanation of the techniques and methods used for this purpose is given by De Strycker et al. [11].

There are two major approaches to the designing of robust watermarking schemes namely spread spectrum (SS) watermarking [8] and quantization index modulation (QIM) [7] watermarking. The idea behind SS-based schemes [3], [36] is to treat the watermark as a narrow-band signal and embed each bit in multiple samples of the host media, which is treated as a wide-band signal. The common approach taken by QIM-based schemes [12], [35] is, first, to establish an association between a set of watermarks and another set of quantizers with their codebooks predefined according to the watermarks. Then to embed a watermark, a set of features are extracted from the host media and quantized to the nearest code of the quantizer corresponding to the watermark. For both types of schemes, a common practice for ensuring low distortion and reducing the interference between the watermark and the host media is the so-called informed embedding in which the information about the host media is exploited by the embedder [9].

3.2. Fragile Watermarking Schemes

In contrary to robust watermarking, fragile watermarks are sensitive to all kind of malicious and non-malicious manipulations, i.e. when manipulated the watermarks are expected to be completely destroyed. Therefore, they are useful for the following applications.

- **Authentication**: In the areas of military intelligence and news broadcasting, authenticity of the media sources is a key concern. By embedding a fragile watermark which identifies the source or producer in the media, the legitimate recipients of the marked media would be able to verify the authenticity of the received media by checking the presence of the source's or the producer's watermark. If the marked media is manipulated, the embedded watermark will become undetectable, the recipient will, thus, know that the media is not trustworthy.
- **Content-integrity verification.** In the areas of medical image archiving, media recording of criminal events, accident scene capturing for insurance and forensic purposes, content integrity may have decisive impact on court ruling. The very presence of a fragile watermark in the original media allows the relevant parties to verify the integrity of the content.

An effective fragile watermarking scheme must have the capability of thwarting the attacks, such as cut-and-paste (i.e. cutting one region of the media and pasting it somewhere else in the same or another media) and vector quantization (i.e. forging a new marked image by combining some regions of taken from different authenticated media while preserving their relative positions [21]. Some recent fragile schemes can be found in [56], [18]. However, fragile watermarks are sensitive not only to malicious manipulations but also to content-preserving operations such as lossy compression, transcoding, bit rate scaling, and frame rate conversion. Unfortunately, those content-preserving operations are sometimes necessary in many Internet and multimedia applications, making fragile watermarking feasible only in the applications, such as satellite imagery, military intelligence, and medical image archiving.

3.3. Semi-Fragile Watermarking Schemes

To facilitate the authentication and content-integrity verification for multimedia applications where content-preserving operations are a common practice, semi-fragile watermarking scheme have been proposed in the last few years [52], [20], [58]. This class of watermarks is intended to be fragile only when the manipulations on the watermarked media are deemed malicious by the schemes.

Usually, to achieve semi-fragility, the schemes exploit properties of, or relationships among, transformed coefficients of the media. Such properties and relationships are invariant to content-preserving operations while variant to malicious manipulations. The watermark is embedded by quantizing or adjusting the coefficients according to the watermark. The defined quantization step governs the fragility or sensitivity to manipulations and the degree of distortion. However, an immediate result of coefficient quantization is that a unique watermark may be extracted from many different media, which might have been subjected to some forms of content-preserving operations or malicious manipulations. Such a one-to-many correspondence can be problematic in terms false positives (i.e. a watermark, that was never embedded, is detected by the detector) and false negatives (i.e. the detector fails to detect an embedded watermark). Unfortunately, no optimal criteria for maintaining low false positive and false negative rates are currently in existence. Another challenge semi-fragile schemes faces is how to distinguish content-preserving operations from malicious attacks. For example, transcoding may be deemed acceptable for one application while it may be seen as malicious for another. Therefore, with these two issues, semi-fragile watermarking is usually not suitable for applications concerning legal and national security issues.

3.4. Reversible Watermarking Schemes

One limitation of the previously mentioned authentication schemes is that the distortion inflicted on the host media by the embedding process is permanent. Although the distortion is often insignificant, it may not be acceptable for some applications. For example, any tiny distortion of an image, even if it were a result of the watermark embedding process itself, in the legal cases of medical malpractice would cause serious debate on the integrity of the image. Therefore, it is desirable that watermarking schemes are capable of perfectly recovering the original media after passing the authentication process. Schemes with this capability are often referred to as reversible watermarking schemes [28], also known as invertible [14] or erasable watermarking [9].

The work of [2], [47], [14] search for two unequally represented sets of pixel groups such that changing the intensity of the elements belonging to one set changes their membership, making them belong to another set. A binary location map is then created, with each bit corresponds to one pixel group and the value (either 0 or 1) represents the membership of that pixel group. The location map subsequently undergoes some form of lossless compression so that its compressed version can be combined with the watermark, the actual payload, to form a bit stream for embedding. The embedding is carried out by changing the intensity of the pixel groups in order to make their membership consistent with the binary value of their corresponding bit in the bit stream. The extraction is simply a process of checking the membership of each pixel group of the watermarked image. If the image passes the authentication process, the original image can be recovered by uncompressing the location map and then changing the intensity of each pixel groups so that their intensity become compatible with their actual membership recorded in the location map.

One of the limitations of all three schemes is that the ratio of the number of members in the two sets is highly dependent on the host image. Usually images with more details or high-frequency components tend to have lower ratio, making the location map less compressible, thus, lowering the embedding capacity of the payload. An interesting scheme with media-independent embedding capacity is reported in [28] to alleviate this drawback.

4. Content Based Image Watermarking

Many digital watermarking schemes have been proposed in the literature for still images and videos and are mainly used in applications discussed in the previous chapters. In all these applications, apart from copyright protection, illegal copy protection, proof of ownership problems, identification of manipulations, there is a growing need for the authentication of the digital content. Recently, the searches for more secure watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and the robustness of a watermarking scheme [41], [54]. This section the various content based image watermarking methods.

4.1. Human Visual System (HVS)

The notion of using watermark as a masking phenomena with constrains of non-visibility is performed using the HVS properties. Much research has been done to increase the robustness and the data hiding capacity of watermarking techniques based on perceptual properties of the Human Visual System (HVS). Kay and Izquierdo in [24] used a content based estimation of Just Noticeable Distortion (JND) in frequency domain. To estimate the JND three image characteristics were considered, namely, texture, edgeness and smoothness. Their results proved that this technique was resilient to most common attacks like geometric image transformations.

Recently this work was improved by [40]. In this work, they considered the texture, luminance, corner and edge information of an image to create a mask that makes the watermark addition to the image less perceptible to the human eyes. The embedding and extraction are done in frequency domain, thereby gaining robustness again common attacks like compression and filtering. The results provided are encouraging.

Much research has been done to increase the robustness and the data hiding capacity of watermarking techniques based on perceptual properties of the Human Visual System (HVS) [46], [8], [50]. The development and improvement of accurate human vision models helps in the design and growth of perceptual masks that can be used to better hide the watermark information thereby increasing its security.

Similarly, in the work proposed by [23], the noise sensitivity of each pixel based on the local region image content such as texture, edge and luminance information was used to obtain the JND mask for the image to be watermarked. Then each bit of the watermark is spread spatially and shaped by pseudo-noise sequence such that its amplitude is kept below the noise sensitive of the pixel into which it is inserted. Experimental results proved that the technique was resistant to compression, cropping and noise attacks.

Parameswaran [38] proposed a content dependent image signature for authentication using wavelet domain. Most of the work in the literature uses DCT domain for content based watermarking. This work differed by using wavelet for image authentication. This work was followed by Parameswaran and Anbumani [29] proposed a robust image watermarking scheme to withstand geometric attacks using content based watermarking techniques. The watermarking was performed in four steps, namely, image normalization, content based watermark generation, watermark embedding and watermark extraction. Wavelet domain was used to construct the content dependent watermark and the watermark was embedded in the mid-frequency coefficients in the wavelet domain. The experimental results proved that the scheme proposed was very effective and was able to withstand attacks like copy attack, crop attack, protocol attacks and cryptographic attacks.

Later in 2007, [29] proposed a fragile watermarking scheme based on DWT domain which was able to resist all kinds of manipulations and had the ability to localize the tampered regions. To achieve high transparency while providing protection to all coefficients, the embedder algorithm involved all the coefficients within a hierarchical neighborhood of each sparsely selected watermarkable coefficient during the watermark embedding process. The way the nonwatermarkable coefficients are involved in the embedding process is content-dependent and nondeterministic, which allowed the proposed scheme to put up resistance to the so-called vector quantization attack, Holliman-Memon attack, collage attack, and transplantation attack.

In [54], Xie et al. proposed a novel content based watermarking technique in ridgelet domain. The blocks were classified using image texture characteristics and to improve the robustness middle frequencies of the RT subband was used. The watermarks were embedded in the most important energetic directions of the pieces with strong texture which are less sensitively to human’s vision. Experimental results showed that the watermarked scheme was robust to noise, cut and other intensive attacks.

Kim and Lee in [25] presented a content based fragile watermarking scheme for image authentication. This model was able to tolerate incidental distortions and indicated tampered regions in case of malicious manipulation. The watermark was extracted based on the image content and was inserted into the DCT block.

4.2. Independent Component Analysis (ICA)

DCT and DWT are the two transformation techniques that are widely used in the watermark embedding process. Recently, researchers have started using ICA for watermarking. In [15], ICA was applied to the blocks of the host image and that becomes the watermark. The least-energy independent components of the host were replaced by the high-energy independent components of the watermark image. The drawback of this scheme is that, for watermark extraction both the watermark and the host images are required.

This was followed by the work of [56], where the host image, the key image, and the watermark image as the independent sources. Embedding was done by weighted addition of the key and the watermark to the host. For watermark extraction, two more mixtures were obtained by adding the key and the watermark using different weights. ICA was then applied to these mixtures to separate the host, the key, and the watermark. The host and the key both are required for watermark extraction. In the next decade, Shen *et al.*, (2003) extended this work to use ICA.

Liu et al. [33] used ICA for detection of the watermark which is a random sequence embedded in low-frequency DCT coefficients. Original DCT coefficients are required for watermark detection and for creating a second mixture needed for ICA. Bounkong et al. [6] applied ICA to each block of the host image and obtained its independent components, where the watermark was embedded. In the extraction phase, ICA was applied to each block to obtain the independent components, which was dequantized to extract the watermark.

Recently, ICA was also used employed by [37] for upsizing and downsizing. [19] Combined ICA and Redundant DWT (RDWT) for successful multilogo watermarking.

The different watermarking schemes are compared and given in Appendix.

5. Conclusion

The literature review reveals the fact that there are numerous innovative and inventive watermarking approaches. Now research is oriented towards content-based watermarking schemes. Most of the proposed watermarking schemes are based on Human Visual System (HVS) using Just Noticeable Distortion (JND) for the selection of watermark positions. ICA a more recent technique is being mainly used for copyright protection. The drawback here is that to have a successful copyright protection scheme a lot of information about the host image is needed for watermark extraction, which are artificially created. To avoid this, the future research direction is planned in using ICA to determine the content of the image, thus totally eliminating the need of host image information during extraction process. Further, the review reveals the fact that even though abundant information on content based watermarking schemes are published, a performance evaluation of various schemes is absent. Future work is also planned to perform a performance evaluation of existing content based watermarking schemes.

References

[1] Ahmad, S. and Lu, Z. (2007) A Joint Biometrics and Watermarking Based Framework for Fingerprinting, Copyright Protection, Proof of Ownership, and Security Applications, International Conference on Computational Intelligence and Security Workshops (CISW 2007), Pp.676-679.

[2] Alattar, A.M. (2004). Reversible watermark using the difference expansion of a generalized integer transform, IEEE Transactions on Image Processing, Vol.13, No.8, Pp.1147-1156.

[3] Barni, M., Bartolini, F. and Piva, A. (2002) Multichannel watermarking of color images, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 12, No.3, Pp. 142 – 156.

[4] Barreto, P.S.L.M., Kim, H.Y. and Rijmen, V. (2002) Toward secure public-key blockwise fragile authentication watermarking, IEE Proceedings - Vision, Image and Signal Processing, Vol. 148, No.2, Pp.57-62.

[5] Bloom, J.A., Cox, I.J., Kalker, T., Linnartz, J.P.M.G., Miller, M.L. and Traw, C.B.S. (1999) Copy protection for DVD video, Proceedings of the IEEE, Vol.87, No.7, Pp.1267-1276.

[6] Bounkong, S., Toch, B., Saad, D. and Lowe, D. (2003) ICA for watermarking digital images, Journal of Machine Learning Research, Pp. 1471-1498.

[7] Chen, B. and G.W. Wornell (2001) Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, IEEE Transactions on Information Theory, Vol.47, No.4, Pp.1423-1443.

[8] Cox, I. and Miller, M. (1997) A review of watermarking and the importance of perceptual modeling, Proceedings of the SPIE/IST& T Conference on Human Vision and Electronic Imaging II, SPIE, San Jose, CA, vol. 3016, pp. 92–99.

[9] Cox, I., Miller, M. and Jeffrey, B. (2002) Digital watermarking: principles and practice, Morgan Kaufmann.

[10] Cox, I.J., Kilian, J., Leighton, F.T. and Shamoon, T. (1997) Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing, Vol.6, No.12, 1673–1687.

[11] De Strycker, L., Termont, P., Vandewege, J., Haitsma, J., Kalker, A., Maes, M. and Depovere, G. (2000) Implementation of a real-time digital watermarking process for broadcast monitoring on a TriMedia VLIW processor, IEE Proceedings - Vision, Image and Signal Processing, Vol. 147, No.4, Pp.371-376.

[12] Eggers, J.J., Bauml, R., Tzschoppe, R. and Girod, B. (2003) Scalar Costa scheme for information embedding, IEEE Transactions on Signal Processing, Vol.51, No.4, Pp.1003-1019.

[13] Eskicioglu, A. and Delp, E.(2001) An overview of multimedia content protection in consumer electronics devices, Proceedings Signal Processing Image Communication, Vol. 16 Pppp. 681-699.

[14] Fridrich, J., Goljan, M. and Du, R. (2001) Lossless data embedding – new paradigm in digital watermarking, EURASIP Journal of Applied Signal Processing, Vol.2, Pp. 185-196.

[15] Gonzalez-Serrano, F.J., Molina-Bulla, H.Y. and Murillo-Fuentes, J.J. (2001) Independent component analysis applied to digital image watermarking, International Conference on Acoustic, Speech and Signal Processing (ICASSP), Vol. 3, Pp. 1997-2000.

[16] Habib, M., Sarhan, S. and Rajab, L. (2005) A Robust-Fragile Dual Watermarking System in the DCT Domain, Lecture Notes in Computer Science, Knowledge-Based Intelligent Information and Engineering Systems, Springer Berlin / Heidelberg, Vol. 3682/2005, Pp. 548-553.

[17] Hartung, F. and Kutter, M.(1999) Multimedia Watermarking Techniques, Proc. of IEEE, Tutorial, Survey, and Special Issue on Data Hiding & Security, pp.1079-1107.

[18] Hasan, M.H. and Gilani, S.A.M. (2006) A Fragile Watermarking Scheme for Color Image Authentication, World Academy of Science, Engineering and Technology, Vol. 19, Pp.39-43.

[19] Hien, T.D., Nakao, Z. and Chen, Y. (2006) Robust multi-logo watermarking by RDWT and ICA, Signal Processing, Elsevier, Vol. 86, Pp.2981-2993.

[20] Ho, C.K. and Li, C.T. (2004) Semi-fragile watermarking scheme for authentication of JPEG images. Proceeding of the IEEE international Conference on Information Technology: Coding and Computing, I, Pp. 7 – 11.

[21] Holliman, M. and Memon, N. (2000) Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes, IEEE Transactions on Image Processing, Vol.9, No.3, Pp.432-441.

[22] Hussein, J. and Mohammed, A. (2009) Robust Video Watermarking using Multi-Band Wavelet Transform, IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1,Pp. 44-49.

[23] Kankanhalli, M.S., Ramakrishnan, K.R. and Rajmohan (1998) Content based watermarking of images, International Multimedia Conference, Proceedings of the sixth ACM international conference on Multimedia, Pp. 61-70.

[24] Kay, S. and Izquierdo, E. (2001) Robust content based image watermarking, Proc. Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS' 2001, Tampere, Finland.

[25] Kim, M. and Lee, W. (2004) A Content-Based Fragile Watermarking Scheme for Image Authentication, Lecture Notes in Computer Science, Content Computing, Springer Berlin / Heidelberg, Vol. 0302/2004, Pp. 258-265.

[26] Kim, Y., Moon, K. and Oh, I. (2003) A text watermarking algorithm based on word classification and inter-word space statistics, Proceedings Seventh International Conference on Document Analysis and Recognition, Pp. 775 -779.

[27] Li C.T. (2004a) Digital fragile watermarking scheme for authentication of JPEG images. IEE proceedings - Vision, Image, and Signal Processing.

[28] Li C.T. (2004b) Reversible watermarking scheme with image-independent embeddingcapacity, Research Report CS-RR-401, Department of Computer Science, University of Warwick, Coventry, UK.

[29] Li, C.T. and Si, H. (2007) Wavelet-based fragile watermarking scheme for image authentication, J. Electron. Imaging, Vol. 16, Issue 1, Pp. 17-22.

[30] Li, C.T. and Yang, F.M. (2003) One-dimensional neighbourhood forming strategy for fragile watermarking, Journal of Electronic Imaging, Vol.12, No.2, Pp.284-291.

[31] Lim, Y., Xu, C. and Feng, D.D. (2001) Web based image authentication using invisible Fragile watermark, ACM International Conference Proceeding Series; Vol. 147, Proceedings of the Pan-Sydney area workshop on Visual information processing, Vol. 11,Pp. 31-34.

[32] Lin, S.D., Kuo, Y. and Huang, Y. (2006) An Image Watermarking Scheme with Tamper Detection and Recovery, First International Conference on Innovative

Computing, Information and Control (ICICIC'06), Vol. 3, Pp.74-77.

[33] Liu , J., Zhang, X., Sun, J. and Lagunas, M.A. (2003) A digital watermarking scheme based on ICA detection, 4th International Symposium on Independent Component Analysis and Blind Signal Separation, (ICA 2003), Nara, Japan, Pp. 215-220.

[34] Liu, R. and Tan, T. (2002) An SVD-based watermarking scheme for protecting rightful ownership, IEEE Transactions on Multimedia, Vol.4, No.1, Pp. 121-128.

[35] Liu, Y. and Smith, J.O. (2004) Watermarking sinusoidal audio representations by quantization index modulation in multiple frequencies, Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing.

[36] Moulin, P. and Ivanovic, A. (2003) The zero-rate spread-spectrum watermarking game, IEEE Transactions on Signal Processing, Vol. 51, No.4, Pp.1098 – 1117.

[37] Nguyen, V.T. and Patra, J.C. (2004) Digital image watermarking using independent component analysis, PCM 2004, Lecture Notes in Computer Science 3333, Springer-Verlag, Pp. 364-371.

[38] Parameswaran, L. (2005) Content Dependent Image Signature for Authentication Using Wavelets, Proceedings of NCIS, Karunya Deemed University, Coimbatore, Nov.2005.

[39] Parameswaran, L. and Anbumani, K. (2006) A Content Based Image Watermarking Scheme Resilient to Geometric Attacks, International Journal of Computer Science, Vol. 2, No. 2, Pp. 118-123.

[40] Parthasarathy, A.K. and Kak. S. (2007) An Improved Method of Content Based Image Watermarking, IEEE Transactions On Broadcasting, Vol. 53, No. 2, Pp.468-479.

[41] Qi, X. and Qi, J. (2007) A robust content-based digital image watermarking scheme, Signal Processing, Elsevier, Vol. 87, Issue 6, Pp. 1264-1280.

[42] Sachs, D., Anand, R. and Ramchandran, K. (2000) Wireless image transmission using multiple-description based concatenated codes,Proceedings Data Compression Conference DCC 2000, P. 569.

[43] Sebe, F. and Domingo-Ferrer, J. (2003) Collusion-secure and cost-effective detection of unlawful multimedia redistribution, IEEE Transactions on Systems, Man and Cybernetics, Part C, Vol. 33, No.3, Pp.382 – 389.

[44] Shen, M., Zhang, X. and Sun, L., Beadle, P. J. and Chan, F.H.Y. (2003) A method for digital image watermarking using ICA, 4th International Symposium on Independent Component Analysis and Blind Signal Separation (ICA 2003), Nara, Japan, Pp. 209-214.

[45] Steineback, M., Dittann, J. and Neuhold, E. (2009) Digital Watermarking - Common watermarking techniques, Important Parameters, Applied mechanisms, Applications, Invertible watermarking, Content-fragile watermarking, Online Encyclopedia, Contributed Article, http://encyclopedia.jrank.org/articles/ pages/6725/Digital-Watermarking.html#ixzz0Zoj226VL

[46] Swanson, M., Kobayashi, M. and Tewfik, A. (1998) Multimedia data embedding and watermarking technologies, Proceedings of the IEEE, vol. 86, no. 6, pp. 1064–1087.

[47] Tian, J. (2003) Reversible data embedding using a difference expansion, IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No.8, Pp.890-896.

[48] Trappe, W., Wu, M., Wang, Z.J. and Liu, K.J.R. (2003) Anti-collusion fingerprinting for multimedia, IEEE Transactions on Signal Processing, Vol. 51, No.4, Pp.1069–1087.

[49] Wang, F., Pan, J. and Jain, L.C. (2009) Digital watermarking techniques, Studies in Computational Intelligence, Springer Berlin / Heidelberg, Vol. 232/2009, Pp. 11-26.

[50] Wolfgang, R.B. and Delp, E.J. (1996) A watermark for digital images, Proc. 1996 Int. Conference on Image Processing, Lausanne, Switzerland, vol. 3, pp. 219–222.

[51] Wong, P.W. and Memom, N. (2000) Secret and public key authentication watermarking schemes that resist vector quantization attack, Proceeding of the SPIE conference on Security and Watermarking of Multimedia Contents II.

[52] Wu, X., Hu, J., Gu, Z. and Huang, J, (2005) A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters, Conferences in Research and Practice in Information Technology Series; Vol. 108, Proceedings of the 2005 Australasian workshop on Grid computing and e-research, Vol. 44, Pp. 75-80.

[53] Xie, L. and Arce, G.R. (2001) A class of authentication digital watermarks for secure multimedia communication IEEE Transactions on Image Processing, Vol.10, No.11, Pp.1754-1764.

[54] Xie, Z., Wang, S., Gan, L., Zhang, L. and Shu, Z. (2008) Content Based Image Watermarking in the Ridgelet Domain, International Symposium on Electronic Commerce and Security, Pp.877-881.

[55] Ye, J. and Tan, G. (2008) An Improved Digital Watermarking Algorithm for Meaningful Image, International Conference on Computer Science and Software Engineering, vol. 2, Pp.822-825.

[56] Zhang, X. and Wang, S. (2009) Fragile watermarking scheme using a hierarchical mechanism, Signal Processing, Vol. 89, Issue 4, Pp. 675-679.

[57] Zhou, X., Duan, X. and Wang, D. (2004) A Semi-Fragile Watermark Scheme For Image Authentication, 10th International Multimedia Modelling Conference, pp.374.

Appendix: Comparison Table for various Watermarking Schemes.

S.No.	Reference	Method	Result
Robust Watermarking Schemes			
1	3	Multichannel watermarking of color images, Space – time coding	Low visible distortion in the host image & robust to various attacks.
2	36	The zero-rate spread-spectrum watermarking game, game – theoretic method, karhunen-Loeve transform	Additive watermarks are suboptimal
3	7	Quantization index modulation & distortion – compensated (QIM)	QIM methods are provably better than additive spread spectrum and generalized LBM against bounded perturbation
Fragile Watermarking Schemes			
4	18	Cryptography (SHA160) and Digital Watermarking Payload is computed by the variance factor α by deploying all the 12 neighboring pixels.	Blind, Computationally fast and exactly locates the tampered regions. Average PSNR value is 43.1639 dB
5	56	Hierarchical mechanism. LSB bits are used for pixel derived and block derived watermark data.	This scheme is capable of recovering the original watermarked version without any error
Semi-Fragile Watermarking Schemes			
6	52	Image authentication based on Integer wavelet Transform with parameters. Lifting scheme is used to improve the processing speed of DWT.	This scheme gives guarantee for the safety of the watermark and locate the tamper area accurately and sensitive to the change of parameter. The embedding parameter α is −1.5 Average PSNR value = 42.185 dB
7	20	Here, a new digital watermark based scheme for verifying the authenticity of JPEG images are proposed, based on a unique concept referred to as the lowest authenticable JPEG quality. Security of this system is based on scramble key. The invariant feature is generated from DCT coefficients in the low / middle frequency domain and embedded into the image by modifying the DCT coefficient in the high frequency domain.	The image quality was preserved by the proposed scheme because the feature is embedded in high band of the DCT frequency domain. Average PSNR value = 37.65 dB. The result shows that this scheme has good visual quality of the watermarked image.
Reversible Watermarking Schemes			
8	47	Data embedding is done using a Difference Expansion. Redundancy in the digital content is used to achieve reversibility.	Average payload size = 191201 bits. Average bit rate = 0.7294 bpp. Average PSNR value = 34.52 dB. In this scheme both the payload capacity limit and the visual quality of embedded images are among the best in the literature.
Content Based Image Watermarking			
9	41	This scheme combines the advantage of important feature extraction, Delaunay – tessellation – based triangle matching,	The overall average PSNR value for 105 watermarked images is 42.87 dB.

		perceptual analysis, one way – hash functions, error correcting codes and spread – spectrum based blind watermark embedding and retrieval to reduce the watermark synchronization problem and resist geometric distortions and common image processing attacks.	The average detection rates using ECC for all simulated geometric attacks are 92.34%, 87.25% and 76.57% for medium, low and high textured images respectively. This scheme does not perform well for the extremely low textured images due to the insufficient important feature points. It also fails the JPEG compression with a quality factor of lower than 20%.
Human Visual System (HVS)			
10	40	This scheme utilizes the perceptual information of the image content, by taking advantage of frequency selectivity and assigns weights to provide some perceptual criteria in the watermarking process. Instead of PSNR, weighted peak signal to Noise ratio (WPSNR) is used to measure the perceptual quality and an additional parameter called the noise visibility function (NVF) is introduced.	Better method of detecting edges. Detects corners using curvature scale space instead of a Moravec operator. This scheme introduces a content based watermarking scheme using decimal sequences and the results are found to be highly satisfactory in terms of watermark detection. A very good balance between robustness and imperceptibility has been achieved. WPSNR is found to be 38.99 dB. WPSNR value remains constant for all the prime numbers.
11	29	Wavelet – based fragile watermarking scheme for Image authentication. This scheme can be incorporated into JPEG 2000 pipeline to facilitate authentication.	Average PSNR value = 56.36 dB. Average Watermarkable ratio = 22.08 % Average Watermarked ratio = 18.63 % High security is achieved by establishing contextual dependence among coefficients by involving the unwtermarkable coefficients in the creation of watermark and the embedding process.
Independent Component Analysis (ICA)			
12	15	Here image is used as the watermark. Matrix B^W is used to restore the watermark. In this sense this matrix is the key of a cryptographic problem.	This method is successful in extracting the watermark even when the image has been attacked.
13	6	The embedding process uses Quantization Index modulation. Decoding to the nearest grid point is the simplest decoding for a quantization embedding scheme. Maximum a posteriori (MAP) decoding using noise and source models derived from experiments.	PSNR value = 43 dB. For a given image, attack type and attack strength the test was repeated 100 times with a different embedded message m of length 1024. Based on local information and a linear transform, this method is computationally efficient. The use of Bayesian decoding method has the potential to provide an optimal decoding scheme.