ISSN:0975-9646

A Survey on Digital Watermarking Techniques

Sasmita Mishra, Amitav Mahapatra,Pranati Mishra

College of Engineering and Technology,
Biju Pattnaik University of Technology
Bhubaneswar, Odisha, India

***Abstract*—A digital watermark is a kind of marker covertly embedded in a noise tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal. Embedding a digital signal (audio, video or image) with information which cannot be removed easily is called digital watermarking. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. In this paper, we present a comprehensive survey on various digital watermarking techniques such as robust, fragile and semi fragile watermarking techniques. This paper provides evidence that digital watermarking techniques are of increasing interest and are of gaining popularity.**

***Keywords*— Digital Watermarking, Robust, Fragile, Semi-fragile Watermarking**

I. INTRODUCTION

In recent years, as digital media are gaining wider popularity, their security related issues are becoming greater concern. Digital watermarking is a technique which allows an individual to add copyright notices or other verification messages to digital media. Image authentication is one of the applications of digital watermarking, which is used for authenticating the digital images. The objective is not to protect the contents from being copied or stolen, but is to provide a method to authenticate the image and assure the integrity of the image. The way to realize this feature is to embed a layer of the authentication signature into the digital image using a digital watermark. In the case of the image being tampered, it can easily be detected as the pixel values of the embedded data would change and do not match with the original pixel values. There are many spatial and frequency domain techniques available for authentication of watermarking. Watermarking techniques are judged on the basis of their performance on a small set of properties. These properties include robustness, transparency, watermarking capacity, blind detection and security. Watermarking schemes are developed according to the requirements of the application and all applications do not require each of these properties in their entirety i.e. watermarking requirements are application dependent and some most desirable properties for these applications are conflicting in nature. A huge trade-off among them is often involved. Digital signature is also an authentication scheme that is used for verifying the integrity and authenticity of the image content. A digital signature can be either an encrypted or a signed hash value of image contents and/or image characteristics. The major drawback of digital signature is that it can detect if an image has been modified, but it cannot locate the regions where the image has been modified. To solve this problem, many researchers have proposed watermarking based schemes for image authentication.

II. WATERMARKING PRINCIPLE

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself. Figure 1 shows the basic block diagram of watermarking process.

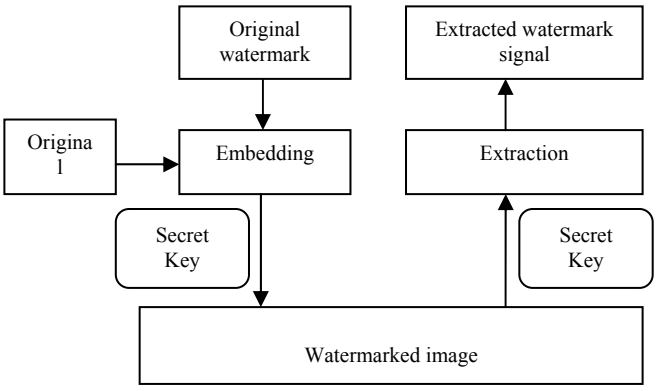

Fig. 1 Block diagram of Watermarking Process

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark.

III. BASIC REQUIRMENTS

The major requirements for digital watermarking are:

A. Transparency

The embedded watermark should not degrade the original image. If visible distortions are introduced in the image, it creates suspicion and makes life ease for the attacker.It also degrades the commercial value of the image.

B. Robustness

This is by far the most important requirement of a watermark. There are various attacks, unintentional (cropping, compression, scaling) and intentional attacks which are aimed at destroying the watermark. So, the embedded watermark should be such that it is invariant to various such attacks.

C. Capacity or Data Load

This quantity describes the maximum amount of data that can be embedded into the image to ensure proper retrieval of the watermark during extraction.

IV. CLASSIFICATION

A. Visible

The watermark is visible which can be a text or a logo used to identify the owner.

Any text or logo to verify or hide content

Fw= (1-α) F+ α*W

Fw = Watermarked Image

α =constant; 0<=α<=1, IF α=0 No watermark, if α=1 watermark present

F =original image

W =watermark

B. Invisible

The watermark is embedded into the image in such a way that it cannot be perceived by human eye. It is used to protect the image authentication and prevent it from being copied.

Invisible watermark can be further divided into three types:

1) *Robust Watermark*: It aims to embed information in a file that cannot be easily destroyed. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks.

2) Fragile Watermark: They are designed with very low robustness. They are used to check the integrity of objects.

3) *Public and Private Watermark:* They are differentiated in accordance with the secrecy requirements for the key used to embed and retrieve watermarks. If the original image is not known during the detection process then it is called a public or a blind watermark and if the original image is known it is called a non blind watermark or a private watermark.

V. WATERMARKING TECHNIQUES

The various watermarking techniques are:

A. Spatial Domain Techniques

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression. Various spatial domain techniques are as follows:-

- *Least Significant Bit Coding (LSB)*

LSB coding is one of the earliest methods. It can be applied to any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

- *Predictive Coding Schemes*

Predictive coding scheme was proposed by Matsui and Tanaka in [18] for gray scale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust as compared to LSB coding.

- *Correlation-Based Techniques*

In this method a pseudo random noise (PN) with a pattern W(x, y) is added to an image. At the decoder the correlation between the random noise and the image is found out and if the value exceeds a certain threshold value the watermark is detected else it is not.

- *Patchwork Techniques*

In patchwork watermarking, the image is divided into two subsets. One feature or an operation is chosen and it is applied to these two subsets in the opposite direction. For instance if one subset is increased by a factor k, the other subset will be decreased by the same amount. If a[i] is the value of the sample at I in subset 'A' which is increased and b[i] is the value of the sample in the subset 'B' whose value is decreased, then the difference between the two subsets would intuitively result in

$\Sigma(a[i]-b[i]) = 2N$ for watermarked images $1<=N<=\infty$

$= 0$ otherwise

B. Frequency Domain techniques

In Frequency domain the secret data are hidden in the lower or middle frequency portions of the protected image, because the higher frequency portion is more likely to be

suppressed by compression. But how to select the best frequency portions of the image for watermark is another important and difficult topic. Various frequency domain techniques are as follows:-

- *Discrete cosine transform (DCT) based technique*

Discrete cosine transform (DCT): It is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to a set of n coefficients. It is very robust to JPEG compression, since JPEG compression itself uses DCT. However, DCT methods lack resistance to strong geometric distortions.

- *Discrete Fourier Transformation (DFT) based technique*

It is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks.DFT uses complex numbers, while DCT uses just real numbers.

- *Discrete wavelet transform (DWT) based technique*

DWT-based methods enable good spatial localization and have multi resolution characteristics, which are similar to the human visual system. Also this approach shows robustness to low-pass and median filtering. However, it is not robust to geometric transformations.

C. Wavelet Transform based Watermarking

The wavelet transform based watermarking technique divides the image into four sidebands – a low resolution approximation of the tile component and the component's horizontal, vertical and diagonal frequency characteristics. The process can then be repeated iteratively to produce N scale transform. The Figure 2 below shows the wavelet based transforms:

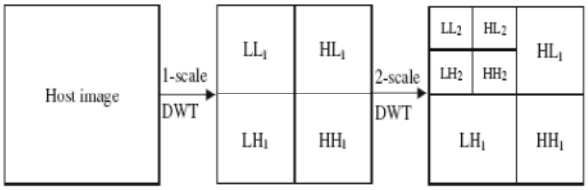

Fig. 2 Wavelet based transforms

-Digital watermarking techniques [15] are classified according to various criteria like robustness, perceptibility, embedding and retrieval methods. Robustness is an important criterion which means the ability of watermark to resist common image processing operations. Watermarking techniques based on robustness can be further divided into three main categories:

(1) Robust (2) Fragile (3) Semi-fragile

Robust watermarking schemes are applied for proving ownership claims whereas fragile watermarking is applied to multimedia content authentication. These watermarking schemes have their own requirements in terms of robustness. Robust watermarks should be able to survive a wide range of friendly operations and malicious attacks, whereas fragile watermarks are intolerable to both malicious and content preserving operations. Fragile watermarking techniques are designed with a goal to identify and report every possible tampered region in the watermarked digital media. Semi-fragile watermarks are intermediate in robustness between the two and are also used for image authentication. Some critical applications like medical imagining and forensic image archiving also requires the fragile watermarks to be reversible. The different quantitative parameters such as PSNR, True and false positive may be used for the evaluation of the method of watermarking schemes.

A. Literature Survey on Robust Watermarking Techniques

A well-known frequency-domain watermark scheme was introduced by Cox et al. [1] in 1997, which is a spread-spectrum watermark scheme. They used a spread-spectrum-like method to insert watermark into the perceptually most significant spectral components of the signal. The watermark is a sequence of real numbers X = x1,…,xn with a normal distribution N(0,1) that has zero mean and a variance of one. The watermark is inserted into the original image V to produce the watermarked image V'. By this scheme, Cox et al. spread the watermark over broadband so it is imperceptible in any frequency beam. However, how to select the best strength value α of the watermark for hiding is an important and difficult topic.

In 1998, Huang and Shi [2] proposed an adaptive spread-spectrum watermark scheme based on human visual system. It was adaptive in the strength of watermarks by accounting the human visual mask: brightness sensitivity and texture sensitivity. The brightness sensitivity is estimated by the DC components in the DCT domain. The texture sensitivity is estimated by quantizing the DCT coefficients using the JPEG quantization table and calculating the numbers of non-zero coefficients. All blocks are clustered into three classes: (1)dark and weak texture, (2) bright and strong texture, and (3) remaining situation. Three numbers of the watermark sequences are embedded in low frequency coefficients of each block. However, it could not satisfy the image visual model exactly and smoothly.

In 1999, Kim et al.'s[3] proposed a watermarking method using the human visual system based on wavelet transform. The number of watermark elements are proportional to the energy contained in each wavelet transform bands. To estimate the characteristic of the image, the changing rate of a sinusoidal pattern per subtended visual angle in cycles per degree is calculated. The result is used as the visual weight of watermarks in each wavelet transform band.

In 2000, Chen et al.'s [4] proposed an adaptive watermarking scheme. This scheme embeds a binary image as watermark in DCT approach. The watermarked image is imperceptible by human visual system. It uses a feature-based method to locate the watermark positions during embedding and extracting. The feature-based method uses the Sobel edge-detector to obtain the gradient magnitude and this result is proportional to the amount of watermark bits.

In 2011, Aree Ali Mohammed & Haval Mohammed Sidqi [5] proposed an image watermarking scheme based on multi bands wavelet transformation method. At first, the proposed scheme is tested on the spatial domain (for both a non and semi blind techniques) in order to compare its results with a frequency domain. In the frequency domain, an adaptive scheme is designed and implemented based on

the bands selection criteria to embed the watermark. These criteria depend on the number of wavelet passes. In this work three methods are developed to embed the watermark (one band(LL|HH|HL|LH), two bands (LL&HH | LL&HL | LL&LH | HL&LH | HL&HH | LH&HH) and three bands (LL&HL&LH | LL&HH&HL | LL&HH&LH | LH&HH&HL) selection. The disadvantage of the scheme is the involvement of a large number of wavelet bands in the embedding process.

In 2013, G. Dayalin Leena and S. Selva Dhayanithy [6] proposed a watermarking scheme **i**n which digital image is watermarked by using wavelet transforms which is an efficient multi-resolution frequency domain technique. The low frequencies of wavelet decomposition of the carrier image which is a color image is watermarked with a color logo shuffled by using a chaotic map technique. Embedding process is highly secured as chaotic map technique shuffles the watermark in order to confuse any unauthorized person who tries to modify or remove the corresponding watermark. The Peak Signal to Noise Ratio (PSNR) of watermarked image has proved that the original image and the watermarked image are visually indistinguishable by human observers. Robustness is checked well by extracting the original watermark perfectly without any degradation in the original image. A chaotic map known as the Arnold's Cat Map (ACM) is a discrete system that folds up the trajectories in time space, which is a torus. ACM constantly apply its map to a given image and each of its iterations moves the image elements called pixels to a unique equivalent peak along the same torus. Ultimately the images will return to the original image at certain iteration.

B. Literature Survey on Fragile Watermarking Techniques

According to embedding and retrieval criteria, fragile watermarking techniques for image authentication can be divided into two categories: spatial domain and transform domain.

In 2006, H. Guo et al.[7] proposed a fragile watermarking scheme to detect malicious modifications of database relations. In this scheme, all tuples in a database relation are first securely divided into groups; watermarks are embedded and verified group by group independently. The embedded watermarks cannot only detect but also localize, and even characterize, the modifications made to the database. In the worst case, the modifications can be narrowed down to tuples in a group.

In 2006, C.-M. Chou, D.-C.Tseng [8] Proposed a public fragile watermarking scheme based on the sensitivity of vertex geometry for 3D model authentication. In the 3D fragile watermarking embedding, slightly perturbing the positions of a subset of vertices is usually needed to keep them in some predefined relationship with their neighboring vertices. Two problems frequently arise in the embedding stage i.e. the causality problem and the convergence problem. The causality problem arises while the neighboring relationship of a former processed vertex is influenced by the perturbing of its latter processed neighboring vertices. The convergence problem means that the original model has been heavily distorted before some vertices reach the predefined relationship. In this case the author proposed a multi-function vertex embedding method and an adjusting-vertex method to overcome these two problems. The proposed method does not need the original model and watermarks for authentication.

In 2009,Chen et al.,[9] proposed a spatial domain watermarking technique based on the idea of incorporating block-wise dependency information in watermarking procedure for thwarting VQ attack without compromising on localization capabilities of the scheme. The block-wise dependency relationship between the blocks of the image is established using fuzzy clustering criteria; a fuzzy C-means algorithm is used for this purpose. This method allows one piece of data to belong to two or more clusters unlike other traditional hard clustering schemes like k-means algorithm that assign data points to a specific cluster. The scheme consists of authentication data embedding procedure and tamper detection procedure.

In 2011, Bhattacharya et. al.,[10] proposed a new approach which makes use of both fragile and robust watermarking techniques. The embedded fragile watermark is used to assess the degradation undergone by the transmitted images. Robust image features are used to construct the reference watermark from the received image, for assessing the amount of degradation of the fragile watermark.

In 2011, Yan et. al.,[11] presented a blind watermarking approach to protect vector geo-spatial data from illegal use. The presented method is rarely affected by data format change, random noise, similarity transformation of the data, and data editing.

In 2012, Chen et. al. [12] proposed a watermarking technique based on the frequency domain. A modified algorithm is presented to improve the defect of the JPEG quantification in order to reduce the bit error rate (BER) of the retrieved watermark. In Addition, two parameters called controlling factors are used to adjust the value of the DCT coefficient in order to trade-off the qualities between the watermarked images and retrieve watermark. Moreover, the proposed algorithm is design as a blind mechanism. Thus, the original image and watermark are not needed for extracting watermark.

Frequency domain techniques have proved to be more effective than spatial domain techniques in achieving high robustness against attacks and can embed more bits of watermark. A brief description of some frequency domain techniques for image authentication is described below.

In 2008, Wang H. et al.[13] proposed a chaotic watermarking scheme for authentication of JPEG images. The quantized DCT coefficients after entropy decoding are mapped to the initial values of the chaotic system, and then the generated watermark information by chaotic iteration is embedded into JPEG compressed domain. Requantization operation does not invalidate tamper detection due to direct modification of DCT coefficient after quantization. Extraction is also performed in the compression domain. Extraction is fast and complexity of method is claimed to be low.

In 2012, Kannammal et.al.[14] proposed a digital watermarking framework in which the Electrocardiograph (ECG) and Patients demographic text ID act as double watermarks. By this method the medical information of the patient is protected and mismatching of diagnostic

information is prevented. Transform domain techniques are in greater use now a days in place of spatial domain techniques as much is known about the properties of these transforms to achieve better watermark characteristics.

C. Literature Survey on Semi-fragile watermarking Technique

Semi-fragile watermark combines the characteristics of both robust and fragile watermarks. Like that of Fragile watermark it is applied to detect the presence of alterations in the image and it is more robust to user's manipulations. In Semi-fragile watermarking technique the Peak Signal to Noise Ratio (PSNR) metric is widely used to measure the amount of difference between two images based on pixel differences. High value of PSNR shows the watermarked image has a better quality, the difference between the original image and the watermarked image is imperceptible. Various semi-fragile watermarking algorithms[16] are:

In 2003, Bassen Abdul Aziz proposed a Semi Fragile watermarking technique that uses a DWT insertion domain by using Tellate having a PSNR of 44 dB and is applied to real work applications. In 2004, A Piva proposed a Semi Fragile watermarking technique that uses DWT using scrambling insertion domain having a 36 dB PSNR and is applied to Video surveillance and remote sensing of images. In 2004, Yuan liang Tang proposed a Semi Fragile watermarking technique that uses DWT domain as insertion domain having a PSNR of 33 dB and there are no specific applications where it is applied. In 2005, Guo rui Feng proposed a Semi Fragile watermarking technique that uses DCT quantization technique having a 37.04 dB PSNR and is applied to Still images for multimedia. In 2005,Anthony T. S. proposed a Semi-fragile watermarking technique that uses Pinned sine transform as insertion domain having a 40 dB PSNR and is applied to Satellite remote sensing of images. In 2006, Kurato maeno proposed a Semi Fragile watermarking technique that uses Wavelet domain as insertion domain having a 65 dB PSNR and is applied to all natural, printed and real time images. In 2007, Xiaoping liang proposed a Semi Fragile watermarking technique that uses I W T using reversible semi fragile watermark as insertion domain having a 43.4 dB PSNR and is applied to Law, commerce, defense, journalism applications. In 2008, Zhu Xian proposed a Semi Fragile watermarking technique that uses D C T domain as insertion domain having a 39.1 dB PSNR and there are no specific applications where it is applied. In 2009, Ching Yu Yang proposed a Semi Fragile watermarking technique that uses IWT coefficient bias algorithm as insertion domain having a 33.91 dB PSNR and there are no specific applications where it is applied. In 2010 Jordi Serrwa Ruiz proposed a Semi Fragile watermarking technique that uses DWT and vector quantization as insertion domain having IDWT as verification method and is applied to Remote sensing of images.

In 2012, Chitla Arathi[17] presented a semi-fragile watermarking technique based on block based SVD(singular value decomposition).Semi-fragile watermark is fragile to malicious modifications while robust to incidental manipulations .The scheme can extract the watermark without the original image. SVD transformation preserves both one-way and non-symmetric properties that is not obtainable in DCT and DFT transformations. This technique can also detect tamper made on the image.

VI. APPLICATIONS

Digital watermarking can be used for the following purposes:

A. *Copyright Protection:* This is by far the most prominent application of watermarks. With tons of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking an image will prevent redistribution of copyrighted images.

B. *Authentication:* Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

C. *Broadcast Monitoring***:** As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.

D. *Content Labeling***:** Watermarks can be used to give more information about the cover object. This process is named as content labeling.

E. *Tamper Detection***:** Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

F. *Digital Fingerprinting:* This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

G. *Content protection:* In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

VII. CONCLUSIONS

This paper provides a comprehensive survey on various digital watermarking techniques, their requirements and applications. The use of different type of watermark is application dependent. Digital watermarking research has generally focused upon two classes of watermarks, fragile and robust. Robust watermarks are designed to be detected even after attempts are made to remove them. Fragile watermarks are used for authentication purposes and are capable of detecting even minute changes of the watermarked content. But neither type of watermark is ideal when considering "information preserving" transformations (such as compression) which preserve the meaning or expression of the content and "information altering" transformations (such as feature replacement) which change the expression of the content. To solve this problem a semi-fragile watermark for still images that can detect information altering transformations even after the watermarked content is subjected to information preserving alterations has to be used.

REFERENCES

[1] Cox, I. J., Kilian, J., Leighton, F. T., andShamoon, T.,"Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6,No. 12, pp. 1673-1687, 1997.

[2] Huang, J. and Shi, Y. Q., "Adaptive Image Watermarking Scheme Based on Visual masking," IEE Electronics Letters, Vol. 34, No. 8, pp. 748-750, 1998

[3] Kim, Y.-S., Kwon, O.-H., and Park, R.-H., "Wavelet Based Watermarking Method for Digital Images Using The Human Visual System," IEE Electronics Letters, Vol. 35, No. 6, pp. 466-468, 1999.

[4] Chen, D.-Y., Ouhyoung, M., and Wu, J.-L.,"A Shift-Resisting Public Watermark System for Protecting Image Processing Software," IEEE Transactions on Consumer Electronics, Vol. 46, No. 3, pp.404-414, 2000.

[5] Aree Ali Mohammed & Haval Mohammed Sidqi," Robust Image Watermarking Scheme Based on Wavelet Technique", International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (4) : 2011

[6] G. Dayalin Leena and S. Selva Dhayanithy," Robust Image Watermarking in Frequency Domain",International Journal of Innovation and Applied Studies ISSN 2028-9324 Vol. 2 No. 4 Apr. 2013, pp. 582-587

[7] H. Guo et al.," A fragile watermarking scheme for detecting malicious modifications of database relations", Information Sciences 176 (2006) 1350–1378

[8] C.-M. Chou, D.-C. Tseng," A public fragile watermarking scheme for 3D model authentication",Computer-AidedDesign 38 (2006) 1154–1165 Available:www.sciencedirect.com

[9] W.-C. Chen, M.-S. Wang (2009), "A Fuzzy c-Means Clustering based Fragile Watermarking Scheme for Image Authentication", Expert Systems with Applications, Volume 36, Issue 2, Part 1, pp. 1300-1307. Available:www.sciencedirect.com

[10] Ankan Bhattacharya, Sarbani Palit, Nivedita Chatterjee, and Gourav Roy (2011), "Blind assessment of image quality employing fragile watermarking", 7th International Sym. on Image and Signal Processing and Analysis (ISPA 2011) Dubrovnik, Croatia, pp. 431-436.

[11] Haowen Yan, Jonathan Li, Hong Wen (2011), "A key points-based blind watermarking approach for vector geo-spatial data", Elsevier Journal of Computers, Environment and Urban Systems, Volume 35, Issue 6, pp. 485–492.

[12] Huang-Chi Chen, Yu-Wen Chang, Rey-Chue Hwang (2012), "A Watermarking Technique based on the Frequency Domain", Journal of Multimedia, Vol. 7, No. 1, pp. 82-89.

[13] Hongxia Wang, Ke Ding, Changxing Liao (2008), "Chaotic Watermarking Scheme for Authentication of JPEG Images", International Symposium on Biometrics and Security Technologies, pp. 1-4.

[14] A. Kannammal, K. Pavithra, S. Subha Rani (2012), "Double Watermarking of Dicom Medical Images using Wavelet DecompositionTechnique", European Journal of Scientific Research, Vol. 70, No. 1, pp. 46-55.

[15] P.Jain and A. S. Rajawat," Fragile Watermarking for Image Authentication: Survey", International Journal of Electronics and Computer Science Engineering", Available: www.ijecse.org ISSN 2277-1956/V1N3-1232-1237

[16] Archana Tiwari, Manisha Sharma,"Semifragile Watermarking Schemes for Image Authentication- A Survey", I.J. Computer Network and Information Security, 2012, 2, 43-49

[17] Chitla Arathi,'' A Semi Fragile Image Watermarking Technique Using Block Based SVD",International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012,3644-3647

[18] T. C. Lin and C. M. Lin, "Wavelet based copyright protection scheme for digital images based on local features", Information Sciences: an International Journal, Vol. 179, Sept. 2009.