Volume 3, Issue 10, October 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Analysis and Survey of Digital Watermarking Techniques

Monika Patel
Computer Science Dept,
N.V. Patel Science College
Vallabh Vidyanagar, India

Priti Srinivas Sajja
Computer Science Dept,
Sardar Patel University,
Vallabh Vidyanagar, India

Ravi K. Sheth
Dept. of Information Technology,
Raksha Shakti University
Ahmedabad, India

Abstract: The growth of the Internet along with the increasing availability of multimedia applications has produced a number of copyright issues. The digital data can be duplicated and edited with great ease which has led to a need for effective copyright protection tools. One of the areas that this growth has fueled is that of digital watermarking. Digital watermarking is the general technique of embedding some information in the original file, such that an altered file is obtained. This information serves as one of different uses, such as, identifying piracy, sensing tampering, or reassuring integrity. The approaches to watermarking are diverse and can be broadly classified based on their visibility, robustness, or fragility. Their uses are also versatile, as they can be applied to text, images, audio, or video. In this paper, we have presented history of digital watermarking, working principle of digital watermarking. We also discussed some of the watermarking techniques for digital images in spatial domain such as LSB, Patchwork and in frequency domain DCT, DWT and DFT along with their comparison, advantages and disadvantages.

Keywords – Copyright, Digital Watermarking, Spatial Domain, Frequency Domain, LSB, DCT, DWT, DFT

I. Introduction To Digital Watermarking

The extreme development of the Internet in the past years has rapidly increased the availability of digital data such as audio, images, text and videos to the public. Thus, the problem of protecting multimedia information becomes more and more important. So the solution of this problem is Digital Watermarking, which is the most common and possibly strongest technique for protecting digital data. Digital watermarking is a method to assert an intellectual copyright in the electronic world. Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures or video. The embedded information is known as a watermark that can be extracted or detected. A watermark may be a digital signal or pattern which is inserted into a digital data. Since this signal or pattern is present in each unaltered copy of the original data, the digital watermark may also serve as a digital signature for the copies.

II. History Of Digital Watermarking

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne, in their paper named as “Electronic Water Mark”. The term used by Tirkel and Osborne was originally used in Japanese as "denshi sukashi" in Japan which is pronounced as an "electronic watermark"[1].

More than 700 years ago, paper watermarks were used in Fabriano, Italy to indicate the paper brand and the mill that produced it. After their invention, watermarks quickly spread over Italy and then over Europe. By the eighteenth century, watermarks on paper made in Europe and America had become used as trademarks, to record the date the paper was manufactured and to indicate the sizes of original sheets, paper format, quality and strength. It was also about this time that watermarks began to be used as anticounterfeiting measures on money and other documents. They are still widely used as security features in currency today [2].

III. Why Digital Watermarking Is Required?

- To prove authenticity of an image
- Verification messages or copyright notices
- To Avoid Forgery
- Security purpose like privacy

IV. The Working Principle Of Watermarking

A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in fig 1 and fig 2[3].

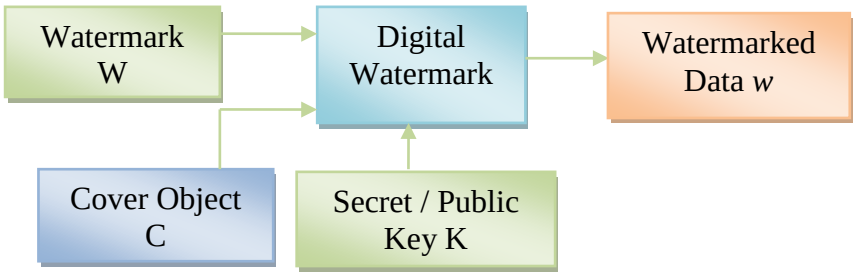

Fig 1Digital Watermarking - Embedding Process

For the embedding process the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data *W.*

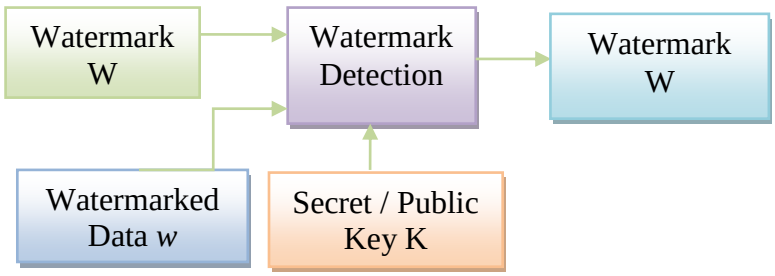

Fig 2 Digital Watermarking - Extracting process

The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark W.

V. CLASSIFICATION OF DIGITAL WATERMARKING TECHNIQUES

Watermarking techniques can be classified based on several criteria as shown in below fig 3.

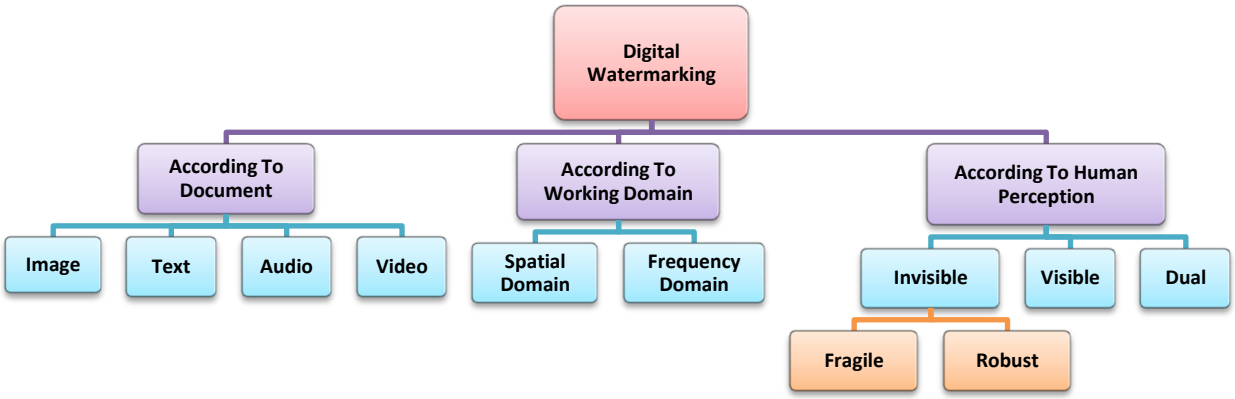

Fig.3 Classification of Digital Watermarking Techniques

A. According to Document:

1) **Image watermarking:** This is used to hide the special information into the image and to detect and extract that special information for the author's ownership.
2) **Video watermarking:** This adds watermark into the video stream to control video applications. It is the extension of image watermarking. This method requires real time quality extraction and robustness for compression.
3) **Audio watermarking:** This application area is one of the most popular and hot issue due to internet music, MP3.
4) **Text watermarking:** This adds watermark to the PDF, DOC and other text file to prevent the changes made to text. The watermark is inserted in the font shape and the space between characters and line spaces.

B. According to working domain:

1. **Spatial domain:** This domain focuses on modifying pixels of one or two randomly selected subsets of images. It directly loads the raw data into the image pixels. Spatial domain method embeds the data by directly modifying the pixel values of the original image. Some of its algorithms are LSB, patch work based technique.

1) **Least Significant Bit (LSB) Technique:** This method is one of the simplest to implement. It involves adding the watermark signal to the lowest order bit of each pixel. The detection method is just as simple as the embedded method. The last bit of each pixel is read, in turn, to disclose the watermark data. The extent of the image degradation depends on how many of the lower order bits are used. The advantage of this method is that even if a part of the watermarked image is cropped the receiver can still get the required message, as the message is embedded a number of times. This technique doesn't show robustness to watermarked image. The following table I shows advantages and disadvantages of LSB technique [10][11].

TABLE I
ADVANTAGES AND DISADVANTAGES OF LSB TECHNIQUE

Advantages	Disadvantages
1. It is most straight forward and the simplest method. 2. It is easy to implement. 3. LSB coding requires very little computation cost for both the watermark encoder and decoder. 4. It has low complexity.	1. With LSB technique the transformed pixels are lost. 2. LSB coding has very little robustness. Simple attack like random cropping or shuffling will destroy the coded watermark. 3. The depth of LSB is limited. In order to minimize the possible audible distortion, only the least 4 significant bits can be used for watermark coding purpose. 4. It is less robust to various attacks.

2) **Patchwork Technique:** Patchwork is a data hiding technique developed by Bender et alii and published on IBM Systems Journal, 1996. It is based on a pseudorandom, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. A pseudo randomly selection of two patches is carried out where the first one is A and the second is B. Patch A image data is brightened where as that of patch B is darkened (for purposes of this illustration this is magnified). Patchwork being statistical methods uses redundant pattern encoding to insert message within an image [5]. Following table II shows the characteristics and drawbacks of Spatial domain watermarking techniques [1][5][14][15][22].

TABLE II
CHARACTERISTICS OF SPATIAL DOMAIN WATERMARKING TECHNIQUES

Characteristics of Spatial Domain Watermarking Techniques
1. Both these methods were robust against all common image processing operations, such as median filter, scaling, rotation, etc. 2. The watermark is applied in the pixel domain. 3. No transforms are applied to the host signal during watermark embedding. 4. Combination with the host signal is based on simple operations, in the pixel domain. 5. The watermark can be detected by correlating the expected pattern with the received signal.
Drawbacks of Spatial Domain Watermarking Techniques
1. The drawback of almost all the spatial domain techniques is that, they alter the host image during embedding phase. In addition, they have the lowest bit capacity and the lowest resistance to JPEG compression. 2. It can survive simple operation such as cropping, any addition of noise. However lossy compression is going to defeat the watermark. 3. Once the algorithm was discovered, it would be very easy for an intermediate party to alter the watermark. 4. One of the major limitations in spatial domain is the capacity of an image to hold the watermark.

2. **Frequency Domain:** This technique is also called transform domain. Values of certain frequencies are altered from their original. Values of certain frequencies are altered from their original. There are several common used transform domain methods, such as DCT, DWT, and DFT.

1) **The Discrete Cosine Transform:** One of the most widely used transform domains for watermarking of still digital images is the Discrete Cosine Transform domain. DCT represents the entire image as coefficients of different frequencies of cosines. The DCT of the image is calculated by taking 8x8 blocks of the image, which are then transformed individually. The 2D DCT of an image gives the result matrix such that top left corner represents lowest frequency coefficient while the bottom right corner is the highest frequency coefficient. Following figure represents different frequency bands of 8x8 block of DCT. FM represents the mid band frequencies of 8x8 block, FL represents lowest frequency components and FH represents higher frequency components. Any of the bands can be used as embedding region. But if watermark is embedded to the FL band then it will create more visual effect. If FH is taken as embedding band then it cannot withstand the image processing operations like compression. That's why FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, without doing significant modification of the cover image.

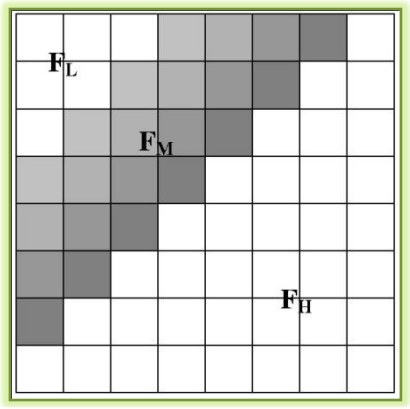

Fig 4 Various Frequency Bands

2) **Discrete Wavelet Transform:** Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The wavelet transform provides the time-frequency representation of a given signal. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). A two dimensional transform can be accomplished by performing two separate one-dimensional transforms. First, the image is filtered along the x-dimension using low pass and high pass analysis filters and decimated by two. Low pass filtered coefficients are stored on the left part of the matrix and high pass filtered on the right. Because of decimation the total size of the transformed image is same as the original image. Then, it is followed by filtering the sub-image along the y-dimension and decimated by two. Finally, we have split the image into four bands denoted by LL, HL, LH and HH and one level decomposition and figure shows one level and second level decomposition [6].

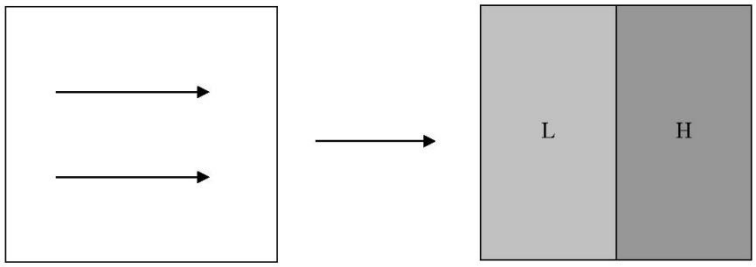

Fig 5 Horizontal Transform-2 subbands

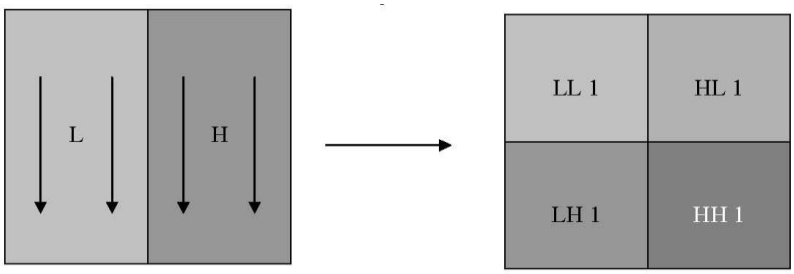

Fig 6 Vertical Transform-4 subbands

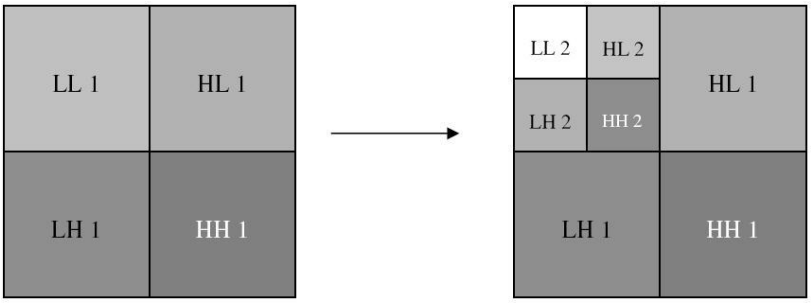

Fig 7 Second level filtering

After decomposing the cover image and the watermark at the desired level, the watermark coefficients are hidden to the appropriate coefficients of the cover image [7].

TABLE III
CHARACTERISTICS OF DWT WATERMARKING TECHNIQUE

Characteristics of DWT
1. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. 2. Wavelet transform is computationally efficient and can be implemented by using simple filter convolution. 3. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL). 4. The larger the magnitude of the wavelet coefficient the more significant it is. 5. Watermark detection at lower resolution is computationally effective because at every successive resolution level there are few frequency bands involved. 6. High resolution sub bands helps to easily locate edge and texture patterns in an image.

3) **Discrete Fourier Transform:** Fourier Transform (FT) is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete valued function requires the Discrete Fourier Transform (DFT). In digital image processing, the even functions that are not periodic can be expressed as the integral of sine and/or cosine multiplied by a weighing function. This weighing function makes up the coefficients of the Fourier Transform of the signal. It has robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation, or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform. Fourier Transform allows analysis and processing of the signal in its frequency domain by means of analyzing and modifying these coefficients [8]. The following table IV shows characteristics of DFT watermarking technique [23][24].

TABLE IV
CHARACTERISTICS OF DFT WATERMARKING TECHNIQUE

Characteristics of DFT
1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions. 2. DFT of a real image is generally complex valued, which results in the phase and magnitude representation of an image. 3. DFT is also resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, which are normalized coordinates, there is no need of any synchronization. 4. The strongest components of the DFT are the central components which contain the low frequencies.

DCT based frequency domain watermarking useful in pan card, i-card of employee of companies, fingerprint identification, medical imaging where is low cost required, whereas DWT based frequency domain watermarking mainly used when we want to transfer more confidential matter through internet to anyone, in military application, government application, broadcast monitoring i.e. entertainment & advertisements, & banks applications [21]. Following table V shows the comparison between spatial domain and frequency domain digital watermarking [16][17][18].

TABLE V
COMPARISON BETWEEN DOMAIN AND FREQUENCY DOMAIN DIGITAL WATERMARKING

Factors	Spatial Domain	Frequency Domain
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Capacity	High(depends on the size of the image)	Low
Effectiveness	Less effective	More effective
Computational Time	More	Less
Computational Complexity	Less	More
Watermarking Techniques	LSB, Patchwork	DCT,DWT,DFT
Example of Applications	Mainly Authentication	Copy Rights

By referring various papers we prepared following table VI which provides summary of different watermarking techniques with advantages and disadvantages [16-18].

TABLE VI
ADVANTAGES AND DISADVANTAGES OF WATERMARKING TECHNIQUES

Watermarking Techniques	Advantages	Disadvantages
LSB	1. Easy to implement and understand 2. Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
Patchwork	High level of robustness against most type of attacks.	It can hide only a very small amount of information.
DCT	The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system. 2. Certain higher frequency components tend to be suppressed during the quantization step. 3. DCT technique doesn't work with scaling attacks.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception. 3. More robust to cropping. 4. It has multi resolution characteristics and is hierarchical. 5. DWT has effective also in structural attacks.	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions.	1. Complex implementation 2. Cost of computing may be higher.

C. According to Human Perception:

1. **Visible watermarking:** Visible watermarking was the first and most primitive way of watermarking. Visible watermarks are ones, which are embedded in visual content in such a way that they are visible when the content is viewed. In this method the cover object is taken and the watermark in added on it. This makes the watermark visible on the cover object. Visible watermarking is shown in fig 8.

Fig 8 Visible Watermarking

2. **Invisible Watermarking:** In invisible watermarking, information is added as digital data to audio, picture or video but it cannot be perceive. An invisible watermark is an overlaid image, which cannot be seen, but which can be detected algorithmically. The watermark, usually a personal Identification Number, is digitally embedded within the image. While these watermarks can be defeated, they offer proof of your ownership if they ever turn up in a publication without your permission. Invisible watermark is used as evidence of ownership and to detect misappropriated images. An invisible watermark is used as a backup for the visible watermark [10].
3. **Dual watermarking:** This technique is a combination of visible and invisible watermark. It contains both visible and invisible watermark inside the cover.

1) **Robust Watermarking:** Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark. The term robust watermark describes those watermarks that can be detected within an object after significant levels of tampering of all kinds. The detection process of watermark can give just the probability of availability of watermark if the tampering level is too high. However, when an object is tampered with, it is automatically modified from the original, and in that sense its quality is degraded. This degradation can either be detected or not by the human sensors. Therefore, we can define some limits for the

maximum required robustness of the embedded watermark. In robust watermarking applications, the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong.

2) **Fragile Watermarking:** Fragile watermarking is a technique in which watermark gets destroyed when watermarked content is modified or tampered with. A watermark that potentially exhibits selective robustness, generally called fragile watermark, is required for tamper-proofing purposes. In short, fragile watermarking involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been tampered with, such as using a file as evidence in a court of law, since any tampering would have removed the watermark. Fragile watermarking techniques tend to be easier to implement than robust methods [9]. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal.

VI. APPLICATIONS OF DIGITAL WATERMARKING

Watermarking system can be really useful in several areas of interest. The requirements that a watermarking system needs to comply with depends upon the specific type of application. A few most common applications involve:

1) **Owner Identification:** The owner identification can be printed on the covers or mentioned somewhere on the item. Examples are the identification mark of an audio company on the CD case or the mark of the paper manufacturer on top corner of the paper. These types of watermarks can be easily removed by cropping the image or by tearing the part that has the identification. Digital watermarking helps to overcome this problem by embedding the watermark in the form of bits and forming an integral part of the content.

2) **Broadcast Monitoring:** By embedding a watermark in commercial advertisements, an automated monitoring system can verify whether the advertisements are broadcasted as contracted or not. In order to help the automated identification of broadcasted programs, original watermarks can be inserted in any type of data to be widely broadcasted on network. Broadcast monitoring can protect not only the commercials but also the valuable TV products.

3) **Fingerprinting:** A fingerprinting technique can be used to trace the source of illegal copy. Every copy available can be watermarked with a unique bit sequence. For the owner, embedding a unique serial number-like watermark is a good way to detect customers who break their license agreement by copying the protected data and supplying it to a third party.

4) **Medical applications:** Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster. Therefore embedding the date and patient's name in medical images could increase the confidentiality of medical information as well as the security.

5) **Proof of ownership:** To avoid unauthorized modification of the object, the owner's identification is watermarked in the original object itself.

6) **Data Authentication:** A given set of data (images) can be easily tampered without even being detected. To avoid this and maintain the originality of the image a watermark like signature, a set of words, may be embedded into the image. If the image is now being tampered it can be easily detected as the pixel values of the embedded data would change and not match the original pixel values. If the image is being copied it would lose its authentication as the embedded data would not be copied along with the image.

7) **Covert communication (Steganography) / Data Hiding:** One of the earliest applications of watermarking, or more precisely, data hiding, is as a method of sending secret messages. In this message will pass in such a way that would prevent any unauthorized person to detect it. The application has been formulated by Simmons as "the prisoner's problem", in which we imagine two prisoners in separate cells trying to pass messages back and forth. Their problem is that they cannot pass these messages directly, but rather, must rely on the prison warden to act as a messenger. The warden is willing to carry innocuous messages between them, but will punish them if he finds that, for example, their messages relate to a plan for escape. The solution is to disguise the escape-plan messages by hiding them in innocuous messages. There are several commercially available programs designed for this application, including stegoTools.

8) **Copy and Playback Control:** Traditional watermarks as well as watermarks for monitoring, identification, and proof of ownership do not prevent illegal copying. Rather, they serve as powerful deterrents and investigative tools. However, it is also possible for recording and playback devices to react to embedded signals. In this way, a recording device might inhibit recording of a signal if it detects a watermark that indicates recording is prohibited. For such a system to work, all manufactured recorders must include watermark detection circuitry. Such systems are currently being developed for DVD video and for digital music distribution.

9) **Indexing:** Watermarking offers a wide range of new capabilities to multimedia applications. It allows the indexing of video mail by permitting the insertion of comments in video content as well as the indexing of movies or news items by making available the utilization of markers that can be exploited in search engines. As the number of images and video contents online increases a lot faster than the capabilities of today's search engine, it is important to plan ahead for new ways to allow quick access to multimedia data and watermarking is certainly a promising way to do so.

VII. Conclusion

In this paper we have presented various aspects for digital watermarking like overview, history, working principle, classification, applications and techniques. Apart from it a brief and comparative analysis of watermarking techniques is presented with their advantages and disadvantages. In this paper we tried to give the complete information about the digital watermarking which will help the new researchers to get the maximum knowledge in this domain.

References

[1] http://www.watermarkingworld.com/digital_watermarking

[2] http://my.safaribooksonline.com/book/energy/9781558607149/chapter-1dot-introduction

[3] Navneet Kumar Mandhani, "Watermarking Using Digital Sequences", MS thesis, Andhra University, August 2004.

[4] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT),Volume 2, Issue 9, March 2013.

[5] K.P. Soman, K.I. Ramachandran – " Insight into Wavelets from Theory to Practice"

[6] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 0-7803-9094-6/05/$20.00 ©2005 IEEE.

[7] Chunlin Song, Sud Sudirman, Madjid Merabti "Recent Advances and Classification of Watermarking Techniques in Digital Images", School of Computing and Mathematical Sciences, Liverpool John Moores University

[8] Ioannis Retsas, "A DCT – Based Image Watermarking Algorithm Robust to Cropping and Compression", MS Thesis, Naval Postgraduate School Monterey, California, March 2002.

[9] B. Surekha, Dr. G. N. Swamy, "A Spatial Domain Public Image Watermarking ", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011

[10] Dr. Vipula Singh, "Digital Watermarking: A Tutorial', Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition, 2011

[11] www.igi-global.com/chapter/literature-review-selected-watermarking-schemes.pdf

[12] G. Rosline Nesa Kumari, B. Vijaya Kumar, L. Sumalatha, and Dr V. V. Krishna, Secure and Robust Digital Watermarking on Grey Level Images, International Journal of Advanced Science and Technology, 2009.

[13] Baisa L. Gunjal, R.R. Manthalkar, An overview of transform domain robust digital image watermarking algorithms, Journal of Emerging Trends in Computing and Information Sciences, 2010.

[14] Darshana Mistry, "Comparison of Digital Water Marking methods",(IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010.

[15] "Recent Advances and Classification of Watermarking Techniques in Digital Images.", Chunlin Song, Sud Sudirman, Madjid Merabti, School of Computing and Mathematical Sciences, Liverpool John Moores University, UK.

[16] "Watermarking Techniques Spatial Domain Digital Rights Seminar @", Mahmoud El-Gayyar, Media Informatics University of Bonn Germany.

[17] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT),Volume 2, Issue 9, March 2013.

[18] Jiang Xuehua, Digital Watermarking and Its Application in Image Copyright Protection, 2010 International Conference on Intelligent Computation Technology and Automation.

[19] Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, ―A Novel Technique for Digital Image Watermarking in Spatial Domain, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[20] http://www.ijsrp.org/research-paper-0213/ijsrp-p1498.pdf

[21] Munesh Chandra, Shikha Pandel, Rama Chaudhary" Digital watermarking technique for protecting digital images"226-233, IEEE 2010

[22] Gurpreet Kaur, Kamaljeet Kaur, Image Watermarking Using LSB (Least Significant Bit), International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013

[23] Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", School of Information Systems, Curtin University of Technology, Perth, Western Australia.

[24] Pereira S., Pun T., "Robust Template Matching for Affine Resistant Image Watermarks," in IEEE Transactions on Image Processing, vol. 9, no. 6, pp. 1123-1129, June 2000.

