Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Digital Watermarking Techniques and Various Attacks Study for Copyright Protection

Shivanjali Kashyap
Department of Electronics and Communication Engineering
Guru Nanak Dev University, Regional Campus,
Gurdaspur, Punjab, India

Abstract-* with *the rapid development of digital multimedia and the web technology, the application of multimedia (video, audio and image etc) has been widely spread. By increasing of this there is a requirement of copyright protection and authentication of digital images. Digital image watermarking methods have been design and implemented for the purpose of protection. Digital image watermarking schemes mainly fall into two broad categories: Spatial-domain and Frequency-domain techniques. It can be done in both spatial as well as frequency domain technique. In this paper we have presented the concept of a comparative study of different digital watermarking techniques in spatial and transform domain. In spatial domain based watermarking technique LSB method is normally used, whereas on the other hand in frequency domain based watermarking technique DWT method is normally used. This paper focuses on different domains of digital image watermarking techniques and various attacks on watermarked images.

Keywords- Robustness, Spatial domain, Frequency domain, LSB, DWT, watermark.

I. INTRODUCTION

The extraordinary raise in piracy and digital criminality more, in the earlier period has inspired attention within the field of watermarking to increase security against violation of copyrighted digital material such as digital image. With the rapid growth of digital multimedia and the web technology, the application of multimedia (video, audio and image etc), has been extensively extended. As the application increases, the issue on the security of the copyright has been receiving more and more interest recently. This digital watermarking could be used to prove the reliability of products, track the pirates and authenticate the owner's right on the product. This means that the use of digital media for image sequences has put some serious implications for copyright control issues. For example, if a particular of a website, which contains photograph, if anyone looking at the page can use their browser to keep the image in digital type at diskette. The captured image Can be then used again in ways not intended by the copyright owner of the material [1].

In order to address these issues, Digital Watermarking has emerged as a solution. Embedding of digital watermarks into multimedia data helped a lot to avoid unlawful photocopying and alteration of data. Digital Watermarking is basically a method of embedding information in a carrier or host image are arrange to protect the user of Image and the signal embedded into the host image to be protected are known as a watermark. A digital watermark is information that is invisibly and vigorously embedded in the host data such that it cannot be altered. A watermark typically contains information about the origin, status or recipient if host data [2]. The basic requirements of the watermarking are

a) **Robustness:** It means the embedded image should be secure against different types of attacks. A good watermarking algorithm should be robust against signal processing operations, geometric attacks such as rotation, scaling and translation and lossy compression.
b) **Imperceptibility:** Invisibility is the most important concern of the watermarked image. The embedded watermark should not be visible in the cover image. The cover image fidelity should be maintained.
c) **Capacity:** The maximum amount of information that can be hidden without degrading the image quality is known as the capacity of the watermark. This amount depends upon the different kinds of application e.g. copyright protection, content validation, fingerprints, broad-cast monitoring etc.

II. HISTORY

The earliest reference to Watermarking in history dates back to the B.C era. The present day Watermarking has developed basically from two different streams. Cryptography meaning, Secret information which can be encrypted and decrypted using binary form whereas Stegno-graph, which in the Greek language means, concealed writing. **Cryptography** is the basic study of methods of sending messages in distinct form so that only the intended recipients can remove the disguise and read the message. However, after receipt and consequent decryption which mean to get information. The information is no longer secure and is in the form of obvious. Reference to cryptography and some of its applications can be found in [3-8].

The watermarks use is almost as old as paper manufacturing. Our ancients poured their half-stuff slurry of fibre and water on to mesh molds to collecting the fibre, and then diffuse the slurry within deckle frames to add shape, and

equality, and finally applied great pressure to expel the water and fiber coherence. This process has not been too much changed in 2000 years. One by-product of this process is the **watermark** – the technique of impressing into the paper a form of image, or text derived from the mold in the negative, as the paper fibres are squeezed, and dried. Paper Watermarks have been widely use in since the late middle Ages. Today most developed countries watermark their paper, currencies, logo and postage stamps to make copy more difficult. The digitization process of our world has been raising the concept of watermarking

III. PROCESS OF WATERMARKING

The watermarking process begins when the encoder inserts watermark into image which producing watermarked image. The decoder extracts and validates the existence of watermarked input or unmarked input. The decoder is not required, if the Watermark is observable. Otherwise, the decoder can or cannot need a duplicate of decoder to perform this work. If Input image or watermarked images are used, then the system is called a secret key system; otherwise, the scheme is public key system. The decoder is so designed to process both marked as well as unmarked image. Finally, the decoder needs to compare the extracted watermark by original image and estimate the outcome to a pre-defined threshold to sets the quantity of resemblance accepted as an equivalent. If the threshold value is detected, i.e. original image is related to the user or else the information does not relate to the user [9].

Digital image watermarking process involves three phases: watermark embedding phase, communication channel phase and watermark detection phase. The watermark embedded which can produce watermarked image by combining original image and watermark.

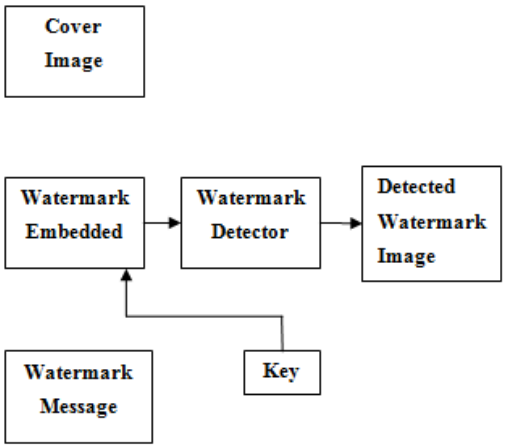

Fig1. Process of watermarking

Then, to the receiver side the watermarked image is transferred. But during the Communication channel process noise can be concerned. In the communication phase noise means any signal interference during transmission and any attacks such as cropping the image or making the brightness changes to the image. The host image which is known as cover work is the digital information created by an owner, or producer. After the message embedding into the original image, the outcome is known as watermarked image. In the detection phase, all the noise has been overcome, so that to correctly extracted and decoded the watermark from the output received image and distinguish with the copyright data, we encoded in step one. If the copyright information and the detected message match, the watermark presents in this image.

IV. TYPES OF WATERMARKING

- Image watermarking
- Video watermarking
- Audio watermarking
- Text watermarking
- 3D watermarking

4.1 TYPES OF DIGITAL IMAGE WATERMARKING ALGORITHM

Generally, any watermarking systems for digital media can be divided into two essential stages: (1) Watermark embedding (2) watermark extraction [14] embedded data should remain the superiority of the host media and the Watermarked image should be related to the original image.

A. Watermark Embedding

At this point the original watermark signal can be embedded into the original host image. The watermark image is after that transmitted or available. The embedding process is illustrated in Figure 1, in which the watermark is embedded into a host image through a key file, either for visible or invisible watermarking. Thus, the watermarked image can be obtained.

B. Watermark extraction

The final action is the use of detection algorithm to remove the watermark and verify for its authentication. While the extraction stage as illustrated in figure 2 on the other hand requires evaluation the watermarked image and the key file to

extract the watermark. The watermark will be extracted using the similar key used in the embedding phase The watermarking process begins with watermark information being inserted into digital media information as the host image. The output Image is the watermarked image. In the embedding process, a secret parameter is need for embedding to generate a more protected watermark. The communication channel is to be requiring for transmitted the watermarked image. At the receiver, watermark can be detected and extracted later. On the other hand, watermarking methods are of two type.

1. TYPES OF WATERMARKING ACC TO HUMAN PERCEPTION:

a) ***Visible watermarks****:* It is that which can be seen by the viewer, logo, and the owner detail are known by the person. This method can change the original signal.

b) ***Invisible watermarks*****:** It is that which cannot be seen by the other party and output signal cannot be change when compared with the original signal.

2. TYPES OF WATERMARKING ACC TO APPLICATION

a) ***Fragile Watermarks:*** **Th**ese are those methods which are most sensitive than other and on small modification it can be easily destroyed.

b) ***Semi-Fragile Watermarks:*** These methods are those which broken easily when the modification of watermark image are greater than their previous threshold.

c) ***Robust Watermarks:*** These method mainly used for copyright protection because it cannot be remove or alter and broken easily.

3. TYPES OF WATERMARKING ACC TO LEVEL OF IMFORMATION

a) ***Blind Watermarks*****:** It detects the embedded information without use of original information. These are more robust to any attacks.

b) ***Semi Blind Watermarks:*** Semi blind watermark is that which needed some special information to detect the embedded information in the watermark signal.

c) ***Non Blind Watermarks:*** It detects the embedded information with use of original information. These are more robust to blind watermark.

4. TYPES OF WATERMARKING ACC TO USER AUTHOURIZATION

a) ***Public Watermark:*** This process of watermarking is that in which an authorized user can detect the information of image.

b) ***Private watermark:*** This process of watermarking is that in which an unauthorized user can also detect information into the image. The robustness of private watermarking are more than the public watermarking.

5. TYPES OF WATERMARKING ACC TO KEY

a) ***Symmetric Watermarking:*** symmetric watermarking is a technique which is used for inserting and extracting the watermark by using the similar keys.

b) ***Asymmetric Watermarking:*** Asymmetric watermarking is a technique which is used for inserting and extracting the watermark by using different keys. This is also known as asymmetric key watermarking.

4.2 CLASSIFICATION OF DIGITAL WATERMARKING

In terms of embedding domain, watermarking algorithms are divided into two groups: Spatial Domain method and Frequency Domain method [15] as shown in figure given below. Frequency Further comparison is given below the table 1, where we get that frequency domain technique is better than the spatial domain technique. Spatial domain technique are further classified into two parts that are least significant bit (LSB) and information tagging whereas frequency domain technique are also classified into two parts that are discrete cosine transformation (DCT) and discrete wavelet transform (DWT).

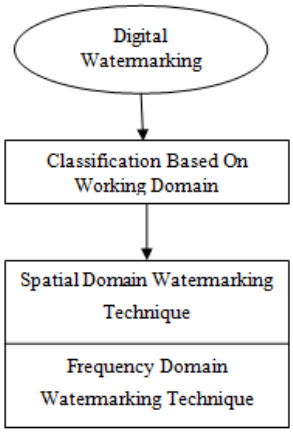

Fig 2. Classification of digital watermarking domain

a) ***Spatial Domain:*** In this domain value of image pixel is directly modified. Watermark pixel embedded in into it. Such method are simpler and computational competent and also not much robust. These methods developed previously are not resistant enough to image compression and other image processing operations. In spatial domain technique, comparison can be done at the extraction process is in between the original image and watermarked image. Least Significant Bit (LSB) is examples of this type of the category domain. For example
LSB of image pixels are
-00100111 11101001 11001000
-00100111 11001000 11101001
-11001000 00100111 11101001
Hide a binary value for 'A'**10000011**
-00100111 11101000 11001000
-00100110 11001000 11101000
-11001001 00100111 11101001

b) ***Frequency Domain:*** In the domain embedding is done after taking image transforms coefficient. This method insert watermark with more robustness and imperceptibility. In this domain technique transform coefficient are to be modified and not the pixel value, image is first converted to frequency domain method such as DWT. Such method is complex and higher computational but are most robust than spatial. The inverse transform is finally applied in order to achieve the watermarked image.

c) ***Comparison Between Spatial and Frequency Domain***

Table 1. Comparison Between Spatial and Frequency Domain

S.no.	Factors	Spatial Domain	Frequency Domain
1.	cost	Very Low	Very High
2.	Robustness	Fragile	More Robust
3.	Perceptually	Highly controllable	Low Controllable
4.	Computational complexity	Low	High
5.	Time Consumption	Less	More
6.	Application	Authenticate Purpose	Copyright Protection

4.3 SPATIAL DOMAIN TECHNIQUE TYPES

A. Information Tagging

Information tagging is one of the method of spatial domain technique in which the properties of the cover image, which be limited to be an image which is depending on the watermarking. According to the carnoni manipulates the intensity locality in the image, while brassil et al. suggests a watermarking method only used for images which containing text. According to camonoi and brassil both methods are defeated without problems.

B. Least significant bit method (LSB)

The most common technique of watermark embedding is to embed the watermark into the least significant bits of the cover object [14]. In spite of being an easy scheme LSB substitution suffers from various drawbacks. Even though it can survive transformations like cropping, any addition of unwanted noise or lossy compression but a more sophisticated attack that might simply set the LSB bits of every pixel to one can be totally defeats the Watermark by small impact on the cover object. Once the algorithm is known to a hacker, the embedded watermark could be simply modified by him without any obscurity. LSB of images pixel are modified in the form of binary data. Here the image can be modified in the form of pixel data that is in 0 and 1 form.

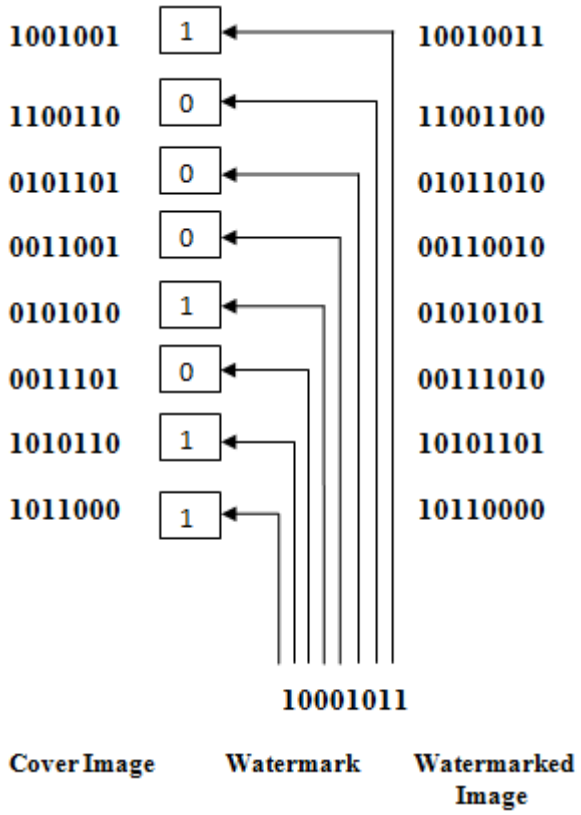

Fig2. Least Significant Bit Method

4.4 FREQUENCY DOMAIN TECHNIQUES TYPES

A. Discrete cosine transformation (DCT)

Discrete Cosine Transform (DCT) is same like as discrete Fourier transform (DFT). DCT is a method which is used for converting elementary frequency components into a signal. DCT based watermarking method are robust than to spatial domain method [16]. The uppermost left corner of the matrix defined the lowest frequency coefficients, while the bottom most right corner defined the highest frequency transform coefficients. DCT techniques with watermarking are robust with comparison to the spatial domain techniques. This type of algorithms are robust against processing operations like low pass filtering (LPF), blurring, intensity and contrast modification etc. Yet, their implement is more difficult and are computationally more costly. By the same time DCT are weak against geometric attacks which are like scaling, cropping and rotation [21].

B. Discrete wavelet transform method (DWT)

DWT decomposes an image into a set of band limited components which can be rearranged to recreate the original image not including fault [16]. Wavelet Transform mainly describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis functions. The basic idea of DWT is to split frequency detail, which is what we call multi-resolution decomposition. At one point decomposition can be split main image into four sub graph as the size of a section [17, 18]. The DWT transform separates the image into a lower resolution approximation (LL) as well as horizontal (HL), vertical (VL) and diagonal (HH) detail components. It is assumed to more exactly model aspects of the HVS (Human Visual System).

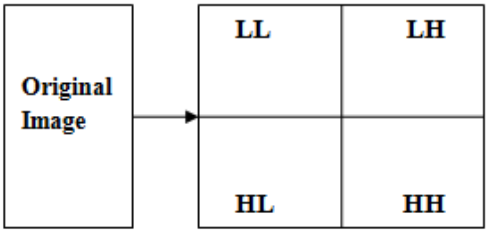

Fig3. Discrete Wavelet Transform

Embedding watermark in the lower resolution frequency band LL may be destroyed the image, because the most of the image energy is concentrated here. Whereas the high resolution frequency band HH include the corner, edges, and textures of the image. The human visibility is not generally perceptive to changes this sub bands [20]. The watermark should be allows to be embedded without being perceived by the human eye. Hence the middle frequency sub bands LH and HL where this allow watermark to be embedded. Here suitable performance of invisibility and robustness which could be achieved.

4.5 FEATURES OF DIGITAL WATERMARKING

a. Robustness:

Robustness is an essential property of digital watermarking. In this the digital watermark is always present in image after attacks and can be easily visible by the owner. It means the embedded image should be secure against different types of attacks. A good watermarking algorithm should be robust against signal processing operations, geometric attacks such as rotation, scaling and translation and lossy compression

b. Imperceptibility:

This refers to the perceptual similarity in between the original image and watermark image. By the presence of watermark the quality of the host image cannot be destroyed. Invisibility is the most important concern of the watermarked image. The embedded watermark in the cover image should not be visible. The capability should be maintained of the cover image.

c. Readability:

It is an essential feature of the watermark. A watermark should consists as much information as possible.

d. Unambiguous:

The watermark reclamation should unambiguously recognize the data user.

e. Security:

A watermark should be secret and cannot be identity by the unauthorized user. Only the authorized user can be accessible the watermark. An unauthorized user cannot be able to read or change the watermark.

4.6 PRACTICAL CHALLENGES OF WATERMARKING

Watermark by itself is not sufficient to prevent abuses unless a proper protection protocol is established .The exact properties that a watermarking algorithm must satisfy cannot be defined exactly without considering the particular application scenario, the algorithm has to be used in. A brief analysis of requirements of data hiding algorithms from a protocol perspective permits to decide whether a given algorithm is suitable for a certain application or not.

Each watermarking application has its own specific requirements. Most often than not these requirements have conflicting effects on each other. A good watermarking algorithm obtains optimal trade off between these requirements; is not weakened/degraded by various attacks, which are malicious and non-malicious both; with the same time unambiguously user identification. These properties can be divided into two parts such as primary and secondary requirements. The primary requirements can be included as data hiding capacity, invisibility and robustness. The secondary requirements include performance i.e. the speed of embedding and of detection of the watermark.

4.7 WATERMARKING APPLICATIONS

Recently there has been an explosion in the use and distribution of digital multimedia data. Personal computers with (broadband) internet connections have become more and more common, and have made the distribution of multimedia data and applications much easier and faster. Electronic commerce applications and online services are developed being rapidly. However, this can also opens the risk of unrestricted duplication and manipulation of copyright material.

To prevent the unauthorized access or manipulation of digital multimedia data, two complementary techniques can be used namely encryption and watermarking [22]. Watermarking techniques complement encryption by embedding a secret imperceptible signal, a watermark, directly into the original data in such a way that it always exit here. The following purposes are used for such type of watermarks [23]:

1. ***Copyright protection*:** A watermark is used to carry copyright information as a proof in case of a copyright or ownership dispute.
2. ***Fingerprinting:*** The information which is unique, it can be directly coupled to authenticate user. This can be inserted in the data as a watermark. In case of copyright violation, this watermark can be used to trace the source of illegal copies.
3. ***Copy protection:*** A watermark is used to carry information prohibiting copying of protected data on compliant hardware.
4. ***Broadcast monitoring:*** A watermark is embedded into data, for example, commercials or copyrighted materials [24], to allow automatic monitoring of the data in the broadcasting channels. The monitoring results of this can be used for royalty or copyright protection purposes.

Digital watermarking can also be used in the other applications which are not dealing with copy or copyright protection:

1. ***Indexing:*** Indexing of video mail is that where the comments can be inserted into the video content: indexing of movies and news items where markers and comments can be inserted that can be used by search engines.
2. ***Medical application:*** Embedding the date and the patient's name in the medical images could be useful safety measure.
3. ***Data embedding:*** Watermarking techniques can be used to insert the message in the data. The data which embedded can be secret or private; but it can also be public. An example of the latter is Digimarc's Smart Images [25].

4. ***Error detection /Tamper proofing:*** In [26], the authors presented an error detection scheme in video coding using a fragile watermark. The authors show that this proposed scheme performs significantly better than a syntax-based error detection method. Similar approaches are also presented in [27, 28].
5. ***Compression:*** The authors in use watermarking techniques to improve the compression rate of colour images. The colour information of the image in this scheme is embedded as a watermark into the luminance data to reduce the data storage requirements.

4. ATTACKS ON DIGITAL WATERMARKING:

Attacks are the methods and processes which can degrade the strength of digital watermarking [29].

4.1 Attacks are mainly divided into these categories

- Removal Attacks
- Geometric Attacks
- Cryptographic Attacks
- Protocol Attacks

a. REMOVAL ATTACKS:

Removal attacks can be affected in such a way the watermark, which can be absolute or almost about to altered or degraded the watermark information. Examples are averaging, quantization, re-modulation, lossy compression collision attacks and noise storm. This attack is that in which the watermarked object can be remove the watermark data. Interference attacks are that in which the watermark information has an additional noise. The attack if any occur in the data that degraded the quality of data,

b. GEOMETRIC ATTACKS:

Geometric attacks are related to the videos and images. These attacks actually do not eliminate the watermark which can be manipulated the watermark so that

Watermark information cannot be observed by the detector. Examples are scaling of image, pixels shifting, translation, rotation of image, cropping warping and line/column removal. The watermark quality can be degraded by these types of attacks. Mosaic attack is another example of this attack. The efficient spatial domain geometric attack is Local pixel.

c. CRYPTOGRAPHIC ATTACKS:

Cryptographic attacks aim at cracking the security methods in watermarking schemes and the watermark information can be eliminated. The removal and geometric both the attacks' do not cracking the watermark algorithm security. For example brute-force attack and oracle attack [30]. In this type of attack like brute-force method is used for finding the secret key watermarking. On the other hand, this type of attack likes oracle attack is that when detector device is available public watermark, then unmarked information is created. These attacks are easily controlled when the embedding algorithm method is difficult.

d. PROTOCOL ATTACKS:

Protocols attacks are that in which watermark can be extracted from the watermarked information authenticate itself. The main purpose of this attack is to harm the application of watermark. In this attacker want to degrade the authenticate user information from the watermarked image. The protocol attacks use the watermark concept in the loopholes. The IBM attack is one of the examples of such attacks. The dead-lock attack, inversion attack and fake original attacks are also known as the IBM attack. This attack embeds one or several additional watermarks such that it is unclear which the watermark of the original owner was. Watermarked image of an already watermark is known as re-watermarking. For example copy attack and changing of watermark.

4.2 ESTIMATION BASED ATTACKS

These attacks needed the characteristics of data and a well knowledge in watermarking technology. The main concept of these attacks is that the original data or the watermark can be estimated by the attacker because the attacker has previous knowledge of the watermark statistics signals.

The estimation based attacks can be divided into different types of attacks like protocol attacks, elimination attacks, or de-synchronization attacks. By this we stop the attacks which are affecting the data and degraded the quality of the information.

4.2.1 ESTIMATE OF THE ORIGINAL DATA

The original data is an addition to the watermark. An extraction technique can be designed by the attacker to get the un - watermarked data. The extraction technique denoising and compression both depend on the watermarked signals. The removal attacks are classified as the denoising and compression attacks.

a) Re-modulation attacks:

Re-modulation attacks by using an opposite technique of the embedding algorithm modifies the watermark used with the original data, the estimated watermark can be subtracted from the original watermarked data, then an approximate estimation is made to the real watermark. This may affect the quality of the original data.

b) Copy attack

The implementation of a copy attack can be estimated by the watermark. The attacker adds the estimated watermark to a target data claiming the ownership of the falsely watermarked data.

c) Synchronization removal

This type of attack depends on the synchronization mechanisms, which used for the purpose of detection which can be used with the original data. After that by removing the synchronization can be applying for de-synchronization techniques. The original data can be extracted by these important characteristics. The original information is easy to get by this process.

V. RELATED WORK

J.J.K.O'Runaidh present a perceptual watermarking method operating in the frequency/transform domain. Watermarking needs can be argue by them to be adaptive in order to be robust and place the watermark in the perceptually most significant components of the image. A watermark is non-intrusive if it resembles the image that it is designed to protect. That means less information should be hidden on flat featureless regions of the image & more information in the parts of the image that contain more texture or around edges, provided edge integrity is maintained.

D.J.Fleet and D.J.Heeger describe method for embedding information in colour images. A model of human colour vision is used to embed signal which is invisible. Sinusoidal signals are inserted so that they can be detected without use of original image. The information which embedded is enough robust to be reliably extracted after being printed and scanned on common place equipment.

Mauro Barni have proposed a scheme where in contrast to conventional methods operating in the wavelet transform domain , in which pixel by pixel masking is accomplished by taking into account the texture and the luminance content of all the image sub-bands. The watermark consists of a pseudorandom sequence which is adaptively added to the largest detail of the bands. As usual, computing the correlation can be detected by the watermark, between the watermarked coefficients. The watermarking code has been chosen for the detection threshold in such a way that the knowledge of the watermark energy used in the embedding phase is not needed, thus permitting to adapt it to the image at hand.

D. Kudur have proposed a scheme where a binary code is embedded by suitably quantizing some of the coefficients of the detail bands: for watermark recovery the embedded binary code is estimated by analyzing coefficients quantization, once the code has been estimated it is correlated with the watermark and the result compared to a threshold chosen on the basis of a given false positive probability No particular attention is given to visual masking.

H. Inoue and **H.-J. M.Wang** have proposed schemes where the most significant DWT coefficients are selected and modified to carry the watermark. In the first case, some side information (i.e., the location of the modified coefficients) is required to recover the watermark. In the second, an algorithm is proposed for identifying *a posteriori* the modified coefficients. To take into account visual effects, very large coefficients are left unchanged.

Nicchiotti choose to embed the watermark into the low pass band, by imposing a given difference among the mean values of two equally sized, randomly selected, subsets of the low pass image; the original image is not required for watermark detection. No particular care is taken with reference to perceptual masking.

F.M.BAYAT presents a new watermark embedding technique which is based on discrete wavelet transforms method. This proposed a technique of copyright material as digital image. This can be based on DWT technique for hiding little but usable data in image. In this result are that this is suitable for image which have better edge where these pixels are obtained from HL and LH of discrete wavelet transform (DWT). This technique of robustness is because of the fact that during the extracting phase, one of these two sub-bands, i.e. HL or LH, has been used role of backup for the other one.

VI. CONCLUSION

The purpose of this paper is to study digital image watermarking techniques and various attacks. Different types of watermarking techniques and attacks have been analyzed in this paper. We classified watermarking algorithms which can be based on the spatial and transform domain. Here we compare the both spatial and frequency domain technique. Then we get that transform domain is better than the spatial domain techniques in term of processing. In this paper spatial domain technique of the LSB method is used for security of images which can be simple and more efficient method. Digital watermarking method is very much impressive for protection for attacks or image authentication. Here the attacks are to be estimated.

ACKNOWLEDGEMENT

"The successful completion of any task would be incomplete without accomplishing the people who made it all possible and whose constant and encouragement secured as success**".** The author gratefully acknowledges the support of guides those who help him giving ideas about the work.

REFERENCE

[1] F. Lusson and K. Curran, (2013) A novel approach to digital watermarking, exploiting colour spaces", Elsevier Trans. on Signal Processing, pp. 1268-1294.

[2] R. G. van Schyndel, A. Z Amornraksa, "An Improving Method for Image Watermarking Using Image Averaging and Tuned Pixels Prediction," IEEE, ISCIT, pp. 755-760, 2010.

[3] Chien-Chang Chen and Yao-Hong Tsai, "Adaptive reversible image watermarking scheme", Elsevier , The Journal of Systems and Software vol. 84 pp 428–434, 2011.

[4] Han-Min Tsai, Long-Wen Chang, "Secure reversible visible image watermarking with authentication", Elsevier, Signal Processing: Image Communication vol. 25 pp 10–17, 2010.J.F.Delaiglee et. al., "Watermarking Algorithm based on Human Visual Model", Signal Processing, Vol 66, No 3, pp 319-335, May 1998.

[5] R. Bangaleea and H.C.S. Rughoopth, "Performance improvement of spread Spectrum Spatial Domain Watermarking Scheme Through Diversity and Attack Characterization" , in IEEE conference Africon , pp 293-298 ,2002.

[6] Dipti Prasad Mukherjee, Subhamoy Maitra and Scott T. Acton, "Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication", in IEEE transactions on multimedia, Vol 6. No. 1, Feb. 2004.

[7] C-T Hsu, J-LWu "Hidden digital watermarks in images," IEEE Trans. Image Processing, vol. 8, pp. 58–68, January 1999.

[8] I.J.Cox et. al., "Secure spread Spectrum Watermarking of Images, Audio and Video", Proc IEEE 1996 International Conf on Image Processing, Vol 3, pp 243-246 http://www.neci.nj.nec.com/tr/neci_tr_95_10.ps, 1996. [9] K. Watermarking digital Image and video data. IEEE Signal Processing Magazine, 17:20–46, 2000.

[10] M. I.J.Cox et. al., "A Secure Robust Watermarking for Multimedia", Proc of First International Workshop on Information Hiding, Lecture Notes in Comp. Sc., Springer-Verlag, Vol.1174, pp 185-206, 1996.

[11] A.G.Bors and I. Pitas, "Image Watermarking using Image Domain Constraints", Proc IEEE 1996 International Conf. On Image Processing, Vol 3, pp 231-234, 1996.

[12] C.Podilchuk and W.Zeng, "Perceptual Watermarking of Still Images", 1997 IEEE, First Workshop on Multimedia signal Processing, Priceton, New Jersy, USA, pp 363-368, June 23-25 1997

[13] R. G. van Schyndel, A. Z Amornraksa, "An Improving Method for Image Watermarking Using Image Averaging and Tuned Pixels Prediction," IEEE, ISCIT, pp. 755-760, 2010.

[14] M D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data embedding and watermarking technologies", Proceedings of the IEEE, Vol. 86, No. 6, 1998, pp. 1064–1087.

[15] C. Lin and Y. Ching, ―A Robust Image Hiding Method Using Wavelet Technique,‖ Journal of Information Science and Engineering, vol. 22, 2006, pp.163-174.

[16] M.Barni et al., "A DCT-Domain System for Robust Image Watermarking", Signal Processing, Vol 66, No 3, pp 357-372, May 1998.

[17] P. Meerwald, A. Uhl, A Survey of Wavelet-Domain Watermarking Algorithms. In Proc. of SPIE, Electronics Imaging, Security and Watermarking of Multimedia Contents III, CA, USA 4314, (2001), pp. 505-516.

[18] K. Hameed, A. Mumtaz, S. A. M. Gilani, Digital Image Watermarking in the Wavelet Transform Domain, World Academy of Science Engineering and Technology 13, 2006.

[19] Tay P., Havlicek J.P., "Image Watermarking using Wavelets". IEEE, pp 258-261, 2002.

[20] Yang Qianli,Cai Yanhong, "A Digital image watermark algorithm based on discrete wavelet transform and discrete cosine transform"978-I-4673-2108-2/12/$31.00 2012 IEEE,PP.1102-1105.

[21] Ouhsain, M., & Hamza, A. B. (2009). Image watermarking scheme using nonnegative matrix factorization and wavelet transform. Expert Systems with Applications, 36(2), 2123–2129.

[22] Shih-Hsuan, Yang, Hsin-Chang Chen, "Bit-Plane Watermarking for Zero Tree Coded Imageg "in IEEE pp. 73-78 2002.

[23] M. Acken, "How Watermarking Value to Digital Content",Comm. of ACM, Vol. 41, No.7, pp 75-77, July 1998.

[24] X.-G. Xia, C. G. Boncelet, and G. R. Arce,"A multiresolution watermark for digital images,"in International Conference on Image Processing,Vol. 111, pp. 548-551, 1997.

[25] X.-G. Xia, C. G. Boncelet, and G. R. Arce,"A multiresolution watermark for digital images,"in International Conference on Image Processing,Vol. 111, pp. 548-551, 1997.

[26] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scene based video watermarking using perceptual models," IEEE J. Select. Areas Commun., Vol.16, May 1998.

[27] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet based fusion," in International Conference on Image Processing, vol. 111, pp. 544-547, 1997.

[28] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-base for watermarking image," in Proc. Int. Conf. Image Processing, Vol. 2, pp. 419–423, 1998. . [29] A. Nikolaidis, S. Tsekeridou, A. Tefas, V Solachidi(Oct. 2001), "A survey on watermarking application scenarios and related attacks", IEEE international Conference on Image Processing, Vol.3, pp. 991– 993.

[30] G. Coatrieux, L. Lecornu, Member, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member IEEE, "a review of digital image watermarking health care".

