

A Comparative Study of various Digital Image Watermarking **Techniques**

¹**Prachi Mishra**, ²**Pankaj Sahu**, ³**Ritesh Beohar** ¹Research Scholar, ²Assistant Professor, ³Assistant Professor M. Tech., Communication Systems, Dept. of ECE, GGITS, Jabalpur

ABSTRACT

Digital watermarking of multimedia content has become a very active research area over the last several years. Watermarking is a very important field for copyrights of various electronic documents and media. With images widely available on the internet, it may sometimes be desirable to use watermarks. Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. In this paper we aim to present a survey on different types of digital watermarks and methods to do image watermarking. Problems and challenges to produce watermarked images are also analyzed and reported.

Keywords : Digital Watermark, Steganography, Authentication, Frequency Domain, Spatial Domain, Least Significant Bit.

I. INTRODUCTION

Over the past few years, there has been tremendous growth in computer networks and more specifically the world wide web. This phenomenon, coupled with the exponential increase of computer performance, has facilitated the distribution of multimedia data such as Publishers, artists, and photographers, images. however, may be unwilling to distribute pictures over the internet due to a lack of security, images can be easily duplicated and distributed without the owner's consent. Digital watermarks have been proposed as a way to tackle this tough issue. This digital signature could discourage copyright violation, and may help determine the authenticity and ownership of an image.

Digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity [1]. Watermarking is very similar to steganography in a number of respects. Both seek to embed information inside a cover message with little to no degradation of the cover-object. Watermarking however adds the

additional requirement of robustness. An ideal steganographic system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. Copyright protection has now become a challenging domain in real life scenario. Digital watermarking scheme is an important tool for copyright protection technique. A good quality watermarking scheme should have high perceptual transparency, and should also be robust enough against possible attacks [1]. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable.

We can also define a watermark as the digital data embedded in multimedia objects such that the watermark can be detected or extracted at later times in order to make an assertion about the object. The main purpose of digital watermarking is to embed information imperceptibly and robustly in the host data. Typically, the watermark contains information about the origin, ownership, destination, copy control, transaction etc. [2].

Digital Watermark (DW) is the signal that is embedded into some digital media to protect their copyrights or to authenticate them. Digital image watermarking is the technique in which watermark information is embedded into some digital image. The image in which watermark is inserted is called host or cover or carrier image. After embedding watermark signal in the host image, it becomes watermarked image.

In the literature, there are several watermarking scheme. Cox et al. propose to insert watermark into DCT domain spectral components of host image using techniques similar to spread spectrum communication. Podilchuk et al. introduces two watermarking techniques in DCT and DWT domain based on human visual system which have been developed in context of image compression by Watson et al. Rao et al. utilized Lewis and Knowles pixel wise masking HVS model to design image adaptive watermarking. Barni et al. modified Lewis and Knowles model based on statistical characteristics of human vision. The modified model is exploited for efficient adaptive image watermarking through pixel wise masking. Ganic et al. introduced DWT-SVD based non blind robust watermarking having better stability, rotation invariance properties. Li et al.proposed an image adaptive DWT-SVD based image watermarking based on HVS. [1]

A well-known (Lewis-Barni) Human Visual System (HVS) based watermarking model is fairly successful with respect to the first mentioned criterion, though its effectiveness in color images has not been claimed. Furthermore, it is true that although several watermarking schemes are available in literature for grayscale images, relatively few works have been done in color image watermarking, and the little that have been done, have mostly been tested in RGB, YUV, YIQ color spaces. Thus the question remains that, which is the optimal color space for color image watermarking and whether this HVS model is applicable for that color space. There are two main contributions of the present work with respect to the above. First, it claims that for color image watermarking, the YCbCr space can be used as the perceptually optimum color space, the Cb component being the optimal color channel here. Second, it also tests the effectiveness of the above-mentioned HVS model in that color space. These have been achieved by using the HVS model to propose a new non-blind (original image and the watermark logo image both are needed for extraction) image adaptive Discrete Wavelet transform and Singular Value Decomposition (DWT-SVD) based color image watermarking scheme in YCbCr color space. The multi-resolution property of DWT and stability of SVD additionally makes the scheme robust against attacks, while the Arnold scrambling, of the watermark, enhances the security in our method [1].

Digital image watermarking system involves two phases, as figure 1 shows it. First phase is the watermark insertion phase, in which watermark information is embedded into a host image to generate the watermarked image. The information is embedded into the cover image such that it does not degrade the original watermarked image. Second phase of the watermarking system is watermark extraction, in which watermark is extracted from the watermarked image (attacked maliciously or non-maliciously) & is matched with actual watermark to verify the watermarked image.



Figure 1: Digital image watermarking

The watermarking technique that does not use the watermark during extraction process is termed as the "blind watermarking". Blind watermarking is better technique over the other watermarking which has watermark for extraction as watermarked signal & owner key are sufficient to find the embedded secret information[2] [10].







Figure 3: Digital watermarking extraction

This paper is organized as follows. Section 2 shows the classification of image watermarking. Section 3 is focused on applications of digital image watermarking. Section 4 explains different techniques of describes watermarking. Section 5 various characteristics of image watermarking. Section 6 presents various limitations and challenges to watermarking. Section 7 represent attacks on system and section 8 represents conclusion.

II. Digital image watermarking classification

Some of the important types of watermarking based on different watermarks [3] are given below:

2.1 Visible watermarks

Visible watermarks are an extension of the concept of logos. Such watermarks are applicable to images only. These logos are inlaid into the image but they are transparent. Such watermarks cannot be removed by cropping the center part of the image.

2.2 Invisible watermark

Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content and author authentication and for detecting unauthorized copier.

2.3 Fragile watermark

Fragile watermark are also known as tamper-proof watermarks. Such watermark are destroyed by data manipulation or in other words it is a watermarks designed to be destroyed by any form of copying or encoding other than a bit-for-bit digital copy. Absence of the watermark indicates that a copy has been made.

III. Applications of digital image watermarking

There are various watermarking applications for images, as listed below [4] [5]:

3.1 Fingerprints

The fingerprint embeds information about the legal receiver in the image. This involves embedding a different watermark into each distributed image and allows the owner to locate and monitor pirated images that are illegally obtained. Associating unique information about each distributed copy of digital content is called fingerprinting, and watermarking is an appropriate solution for that application because it is invisible and inseparable from the content [6].prevention of unauthorized copying is accomplished by embedding information about how often an image can be legally copied [7].

3.2 Tamper detection

Fragile watermarks are used for tamper detection. If the watermark is destroyed or degraded, it indicates presence of tampering and hence digital content cannot be trusted [21].

3.3 Image and content authentication

In an image authentication application, the intent is to detect modifications to the data. The characteristics of the image, such as its edges, are embedded and compared with the current images for differences. A solution to this problem could be borrowed from cryptography, where digital signature has been studied as a message authentication method. Digital signature essentially represents some kind of summary of the content. If any part of the content is modified, its summary, the signature, will change making it possible to detect that some kind of tampering has taken place. One example of digital signature technology being used for image authentication is the trustworthy digital camera [8].

3.4 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 [9].

3.5 Broadcast monitoring

In 1997, a scandal broke out in japan regarding television advertising. At least two stations had been routinely overbooking air time. Advertisers were paying for thousands of commercials that were never aired [19].

IV. Classification of image watermarking techniques

The frequency sensitivity refers to the eye's response to spatial, spectral, or time frequency changes. Spatial frequencies are perceived as patterns or textures, and spatial frequency sensitivity is usually described as the eye's sensitivity to luminance changes [10]. It has been shown that an eye is the most sensitive to luminance changes in the mid-range spatial frequencies, and that sensitivity decreases at lower and higher spatial frequencies. Digital image watermarking schemes mainly fall into two broad categories:

- ✓ Spatial-domain techniques.
- ✓ Frequency-domain techniques.

4.1 Spatial domain techniques

Spatial watermarking can also be applied using color separation. In this way, the watermark appears in only one of the color bands. This renders the watermark visibly subtle such that it is difficult to detect under regular viewing. However, the mark appears immediately when the colors are separated for printing. This renders the document useless for the printer; the watermark can be removed from the color band. This approach is used commercially for journalists to inspect digital pictures from a photo-stockhouse before buying unmarked versions.

4.1.1 Least Significant Bit (LSB)

The earliest work of digital image watermarking schemes embeds watermarks in the lsb of the pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant) bit, of selected pixels of the image. This method is easy to implement and does not generate serious distortion to the image; however, it is not very robust against attacks. For instance, an attacker could simply randomize all lsbs, which effectively destroys the hidden information.

4.1.2 SS Modulation based technique

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection. When applied to the context of image watermarking, ssm based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

4.2 Frequency domain techniques

Compared to spatial-domain methods, frequencydomain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image. The most commonly used transforms are the discrete cosine transform (dct), discrete fourier transform (dft), discrete wavelet transform (dwt), the reason for watermarking in the frequency domain is that the characteristics of the human visual system (hvs) are better captured by the spectral coefficients. For example, the hvs is more sensitive to low- frequency coefficients, and less sensitive to high- frequency coefficients. In other words, low- frequency coefficients are perceptually significant, which means alterations to those components might cause distortion to the original image. On the other hand, highfrequency coefficients are considered insignificant; thus, processing techniques, such as compression, tend to remove high- frequency coefficients aggressively. To obtain a balance between imperceptibility and robustness, most algorithms embed watermarks in the midrange frequencies.

4.2.1 Discrete Cosine Transformation (DCT)

Dct like a fourier transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. Dct based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation. scaling, cropping etc. Dct domain watermarking can be classified into global dct watermarking and block based dct watermarking. Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image.

4.2.2 Discrete Wavelet Transformation (DWT)

The discrete wavelet transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time- varying signals. Since most of the real life signals encountered are time varying in nature, the wavelet transform suits many applications very well [11]. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark, but the visible distortion would be increased as well [12]. However, dwt is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image [13]. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into subimage of different spatial domain and independent frequencies [14].

V. Characteristics of Watermarking

There are many characteristics [15] [16] [20] that watermarking hold are as follows:

5.1 Invisibility

An embedded watermark is not visible. Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content or author authentication and for detecting unauthorized copier.

5.2 Computational complexity

Computational complexity indicates the amount of time watermarking algorithm takes to encode and decode. To ensure security and validity of watermark, more computational complexity is needed. Conversely, real-time applications necessitate both speed and efficiency.

5.3 Robustness

Piracy attacks or image processing should not affect the embedded watermark. Even if the visible watermark is removed (by an attack), there is the invisible one as the backup. The visible watermark is inserted into the original image while the invisible water mark is added to it. Therefore, it is a watermark within a watermark creating a dual watermarked image. This is another method of developing robust watermarking techniques. For robustness we can also add watermark at more than one position in the image, if one or two are removed then the other is there.

5.4 Fidelity

Fidelity can be considered as a measure of perceptual transparency or imperceptibility of watermark. It refers to the similarity of un-watermarked and watermarked images. This perspective of watermarking exploits limitation of human vision. Watermarking should not introduce visible distortions as it reduces commercial value of the watermarked image.

5.5 Data payload

Data payload is also known as capacity of watermarking. It is the maximum amount of information that can be hidden without degrading image quality. It can be evaluated by the amount of hidden data. This property describes how much data should be embedded as a watermark so that it can be successfully detected during extraction.

5.6 Security

A watermark should be secret and must be undetectable by an unauthorized user in general. A watermark should only be accessible by authorized parties. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys. As information security techniques, the details of a digital watermark algorithm must be published to everyone. A particular watermark signal is related with a special number used embedding and extracting. The special number is kept secretly and is used for confirming legal owners of digital products later. If we lay strong stress on robustness, and then invisibility may be weak. Therefore, developing robustness watermark with invisibility is an important issue.

Secret key has to be used for embedding and detection process in case security is a major concern. There are three types of keys used in watermark systems: private-key, detection-key and public-key. Hackers should not be able to remove watermark with anti-reverse engineering research algorithm.

5.7 Non-perceptibility

Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits.

5.8 Verifiability

Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

VI. Challenges and limitations of digital mage watermarking

Watermarking research has many technical challenges. The robustness and imperceptibility trade-off makes research quite interesting. the То attain imperceptibility, the watermark should be added to the high frequency components of the original signal. On the other hand, for robustness the watermark can be added to the low frequency components only. Thus, the watermarking scheme can be successful if the low frequency components of the original signal are used as the host for watermark insertion. In this section, we discuss the various technical issues related to watermarking, such as properties of the human visual system and spread-spectrum communication, which are commonly exploited for making watermarking schemes successful.

6.1 Properties of visual signal

Since image and videos are visual signals, it is necessary to understand the behavior of visual signals in order to find ways to hide additional information in them. Visual signals are generally recognized as amplitude plots, intensity versus space displays of image information and intensity versus space and time displays of video scenes. These waveforms reveal a lot of information about the properties of the signals. Some of the properties of visual signals are listed below:

6.1.1 Nonstationarity

Nonstationarity property is common to all signals. Image and video signals contain a wealth of segments of flat or slowly changing intensity, as well as edges and textured regions. While the edges need to be preserved to maintain perceptual quality, the textured regions need to be judiciously used to store additional information.

6.1.2 Periodicity

There exists line to line and frame to frame periodicity in image and video signals. They are not exactly periodic but there exists redundancy between frames and lines. These redundancies are exploited in any compression scheme, and need to be considered during the watermarking process.

6.2 Properties of the human visual system (HVS)

The success of any watermarking scheme lies in making the best use of the human visual system (hvs). In this section, we discuss the various properties of the human visual system which are exploited in designing watermarking algorithms.

6.2.1 Texture Sensitivity

The visibility of distortion depends on the background texture. The distortion visibility is low when the background has a strong texture. In a highly textured image block, energy tends to be more evenly distributed among the different dct coefficients. In a flat- featured portion of the image the energy is concentrated in the low frequency components of the spectrum. This indicates that in strong texture regions more watermark signal can be added.

6.2.2 Brightness sensitivity

The human eye is sensitive in perceiving a low intensity signal in the presence of backgrounds of different intensity. As the surrounding region intensity is increased, the relative intensity in dark areas is reduced and the sensitivity in the light areas is increased. When the mean value of the noise square is the same as that of the background, the noise square tends to be most visible against a mid- grey background. This characteristic is known as weber's law. This means that the eye has high sensitivity at low intensity levels and greatly reduced sensitivity at high intensity levels.

7. Attacks on watermarking system

A watermarked object is likely to be subjected to certain manipulative processes before it reaches the receiver. Common signal processing functions such as conversion, analog-to-digital digital-to-analog conversion, sampling, quantization, requantization, recompression, linear and nonlinear filtering, low-pass and high-pass filtering, addition of gaussian and nongaussian noise are common manipulations. An attack is any processing that impairs or misleads the watermark detector. The performance of а watermarking algorithm against these attacks reflects its quality. Similarly, it is anticipated that an embedded system realization of watermarking can face several physical attacks similar to the ones suggested for cryptography. The requirements for fulfilling desired characteristics and the requirements for performance against attacks are mutually conflicting. There are many watermarking algorithms proposed and metrics has been developed for their comparison so that the user can make a decision to use one of the algorithms that best suits his need.

7.1 Attacks

We discuss various possible intentional and unintentional attacks that a watermarked object is likely to be subjected to. We classify the attacks into four different types, such as removal and interference attacks, geometric attacks, cryptographic attacks, and protocol attacks. Besides these four types, there is another class of attacks called estimation based attacks. In estimation based attacks, estimates of either the watermark data or the original object can be obtained using stochastic methods. The estimation based attacks can be classified as removal, protocol, or desynchronization depending on the way the estimate is used [17].

7.1.1 Removal & interference attacks

Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal. Moreover, interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion, denoising, remodulation, averaging, and noise storm are some examples of this category of attacks. The collusion attack occurs when a number of authorized recipients of the multimedia object come together to generate an un-watermarked object by averaging all the different watermarked objects.

7.1.2 Geometric attacks

Geometric attacks are specific to images and videos. Geometric attacks do not actually remove the watermark, but manipulate the watermarked object in such a way that the detector cannot find the watermark data. This type of attack includes affine transformations such as rotation, translation, and scaling. Warping, line/column removal and cropping are also included in this family of attacks. Another example of geometric attack is the mosaic attack. In the mosaic attack, the watermarked image is divided into several parts and rearranged using proper html code, thus constructing water- marked image in which the watermark detector will fail to provide desired results. Local pixel jittering is an efficient spatial domain geometric attack.

7.1.3 Cryptographic attacks

The above two type of attacks, removal and geometric, do not breach the security of the watermarking algorithm. On the other hand, cryptographic attacks deal with the cracking of the security. For example, finding the secret watermarking key using exhaustive brute force method is a cryptographic attack. Another example of this type of attack is the oracle attack [18]. In the oracle attack, a non-watermarked object is created when a public watermark detector device is available. These attacks are similar to the attacks used in cryptography.

7.1.4 Protocol attacks

The protocol attacks exploit the loopholes in the watermarking concept. One example of such attack is the ibm attack [10]. The ibm attack is also known as the deadlock attack, inversion attack, or fake-original attack. This attack embeds one or several additional watermarks such that it is unclear which the watermark of the original owner was. Watermarking of an already watermarked image is called rewatermarking. In some inversion attacks, a fake original object is created that produces the same results through the detector as that of the real original object.

VII. CONCLUSION

The purpose of this paper is to present a survey of image watermarking digital approaches. The comprehensive review of literature made has uncovered various aspects of digital image watermarking. An attempt is made to classify and analyze many previous watermarking methods for the understanding them and a help for new researchers in related areas. We classified the previous works from the various points of view: the inserted media category, the perceptivity, the robustness, the inserting watermark type, the processing method and the necessary data for the watermark extraction.

It is concluded that digital watermarking technique is very impressive for image authentication and for protection against attacks. Hence, we will try to increase the robustness of digital image watermarking techniques by reducing BER & to propose a secure algorithm of inserting & detecting watermark. The proposed work will deal with the development of improved watermarking algorithms, where improvements are made in terms of imperceptibility, robustness, speed & capacity. Efforts to improve the performance of existing watermarking techniques based on DWT will be done.

VIII. CONCLUSION

The proposed payment system combines the Iris recognition with the visual cryptography by which customer data privacy can be obtained and prevents theft through phishing attack [8]. This method provides best for legitimate user identification. This method can

also be implemented in computers using external iris recognition devices.

IX. REFERENCES

- Aniket Roy et-al, "A perception based color image adaptive watermarking scheme in YCbCr space", 2nd IEEE International Conference on Signal Processing and Integrated Networks (SPIN), Pp- 537 - 543, Noida, 2015.
- [2]. Neha Bansal et-al, "Comparative Analysis of LSB, DCT and DWT for Digital Watermarking", 2nd IEEE International Conference on Computing for Sustainable Global Development (INDIACom), Pp. 40 - 45, New Delhi, 2015.
- [3]. Sudip Ghosh et-al, "A New Algorithm on Wavelet Based Robust Invisible Digital Image Watermarking for Multimedia Security", IEEE International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV), Pp- 72 - 77, Shillong, 2015.
- [4]. S. Abolfazl Hosseini et-al, "A New Method for Color Image Watermarking Based on Combination of DCT and PCA", IEEE International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Pp. 1-5, Sharjah, 2015.
- [5]. Sha Wang et-al, "Adaptive Watermarking and Tree Structure Based Image Quality Estimation", IEEE Transactions on Multimedia, Volume 16, Number 2, February 2014.
- [6]. Dhananjay Yadav et-al, "Reversible Data Hiding Techniques", International Journal of Electronics and Computer Science Engineering (IJECSE), Volume 1, Number 2, 2013.
- [7]. Md. Iqbal Hasan Sarker et-al, "FFT-Based Audio Watermarking Method with a Gray Image for Copyright Protection", International Journal of Advanced Science and Technology, Volume 47, October, 2012.
- [8]. I.J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Morgan Kaufmann, 2008.
- [9]. M. El-Gayyar and J. von zur Gathen, "Watermarking techniques spatial domain," University of Bonn Germany, Tech. Rep., 2006.
- [10]. J. Liu and X. He, "A review study on digital watermarking," First International Conference on Information and Communication Technologies, pp. 337-341, 2005.

- [11]. M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection. Artech House, 2003.
- [12]. X. Wu, J. Hu, Z. Gu, and J. Huang, "A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters," Australasian Information Security Workshop, vol. 44, 2005.
- [13]. M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform," IEEE Transaction on Image Processing, vol. 1, pp. 205-220, 1992.
- [14]. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," SIAM Journal on Mathematical Analysis, 1997.
- [15]. V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," 3rd IEEE International Conference on Industrial Informatics, pp. 709-716, 2005.
- [16]. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, "Performance analysis of watermarking schemes based on skewtent chaotic sequences," NSIP'01, 2001.
- [17]. S.Teskeridou, V. Solochidis, N. Nikolaidis, A. Tefas, and I. Pitas, "Bernoulli shift generated chaoticwatermarks: Theoretic investigation," SCIA2001, 2001.
- [18]. W. Yan, Z. Shi-qiang, and W. Yan-chun, "Wavelet digital watermark based on chaotic sequence," ICICIC'08, 2008.
- [19]. K. L. W. G. Natasa Terzija, Markus Repges, "Digital image watermarking using discrete wavelet transform: Performance comparison of error correction codes," Visualization, Imaging and Image Processing, 2002.
- [20]. L. Haiyan, Z. Xuefeng, and W. Ying, "Analysis of the performance of error correcting coding in audio watermarking," 3rd IEEE Conference on Industrial Electronics and Applications, pp. 843-848, 2008.
- [21]. P. Cika, "Watermarking scheme based on discrete wavelet transform and error-correction codes," 16th International Conference on Systems, Signals and Image Processing, pp. 1-4, 2009.
- [22]. Bastug and B. Sankur, "Improving the payload of watermarking channels via ldpc coding," Signal Processing Letters, vol. 11, pp. 90-92, 2004.

- [23]. Nafornita, A. Isar, and M. Kovaci, "Increasing watermarking robustness using turbo codes," International Symposium on Intelligent Signal Processing, pp. 113-118, 2009.
- [24]. N. Pantuwong and N. Chotikakamthorn, "Line watermark embedding method for affine transformed images," ISSPA 2007, pp. 1-4, 2007.
- [25]. S. Riaz, M. Y. Javed, and M. A. Anjum, "Invisible watermarking schemes in spatial and frequency domains," International Conference on Emerging Technologies, 2008.
- [26]. R. Liu and T. Tan, "An svd-based watermarking scheme for protecting rightful ownership," IEEE Transactions on Multimedia, vol. 4, pp. 121-128, 2002.
- [27]. R. A. Ghazy, N. A. El-Fishawy, M. M. Hadhoud, M. I. Dessouky, and F. E. A. E.-S. Samie, "An efficient block-by-block svd-based image watermarking scheme," National Radio Science Conference, pp. 1-9, 2007.
- [28]. D. Taskovski, S. Bogdanova, and M. Bogdanov, "Digital watermarking in wavelet domain," FIRST IEEE Balkan Conference on Signal Processing, Communications, Circuits, And Systems, 2000.
- [29]. G. Hai-ying, L. Guo-qiang, L. Xu, and X. Yin, "A robust watermark algorithm for jpeg2000 images," Fifth International Conference on Information Assurance and Security, 2009.
- [30]. D. R. Sans, "Identificao de propriedade em imagens com marcas d'gua no domnio da transformada wavelet," Master's thesis, Universidade Federal do Paran - UFPR, 2008, in portuguese.
- [31]. E. Ganic and A. M. Eskicioglu, "Robust dwt-svd domain image watermarking: Embedding data in all frequencies," Proceedings of the 2004 workshop on Multimedia and security, pp. 166 -174, 2004.
- [32]. P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 15, Pp. 96-102, 2005.
- [33]. K. Loukhaoukha and J. Y. Chouinard, "Hybrid watermarking algorithm based on SVD and lifting wavelet transform for ownership verification," 11th Canadian Workshop on Information Theory, pp. 177-182, 2009.