Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey

Ensaf Hussein
Senior Teaching Assistant, Computer Science Dept.,
Faculty of Computers & Information, Helwan Univ.,
Cairo, Egypt.

Mohamed A. Belal
Professor, Computer Science Dept.,
Faculty of Computers & Information, Helwan Univ.,
Cairo, Egypt.

Abstract

Digital watermarking techniques have been developed to protect the copyright of digital media. This paper aims to provide a detailed review and background about the watermarking definition, concept and the main contributions in this field. It begins with digital watermarking overview, general framework, attacks, application, and finally a comprehensive survey of existing and most recent watermarking techniques. We classify the techniques according various categories such as host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, and applications. In the survey our main concern is image only.

1. Introduction

Nowadays, the rapid development of technologies has led to the significant increase of digital information, particularly multimedia such as image, audio and video content. Such technological advances have led to the ease in which it is possible to illegally share, distribute, and copy Intellectual Property (IP) [1-3].

An obvious requirement, therefore, is the development of solutions for copyright protection and ownership identification for digital content.

Digital watermarking is the process of embedding relevant ownership information (such as a logo, fingerprint and serial number), into a media in order to protect the ownership of different media formats [2-5]. This technique can be applied to different media types such as video, audio and image content. For the purpose of copyright protection and ownership identification, robust watermarking schemes are mainly used as they can tolerate a host of signal processing attacks that can be both unintentional and intentional.

The paper begins with the fundamental concept, general framework, attacks and application of digital watermarking; follow by a more detailed survey of different transform based watermarking techniques.

The paper is organized as follows:

- In Section 2, we briefly describe the background of digital watermarking, then we discuss the concept of digital image watermarking, the effectiveness requirements, the embedding and extraction processes, and finally present the general framework.
- Section 3 presents classification and analysis of digital watermarking techniques according different criteria such as host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, and applications.
- Section 4 presents a survey of various robust image watermarking algorithms operating in the transform domain. We review algorithms applied in the spatial domain, and then extensively review transform-based robust watermarking methods.
- Section 5 explores watermarking attacks.
- Section 6 gives the concluding remarks.

2. Digital Watermarking Overview

2.1Watermarking Background

Historically [1, 7], postage stamps and currency were commonly watermarked. Indeed, the currency watermark is still used today when printing banknotes. A digital watermark can be either visible or invisible. An example of digital visible watermark is the translucent logos that are often seen embedded at the corner of videos or images, in an attempt to prevent copyright infringement. However, these visible watermarks can be targeted and removed rather simply by cropping the media, or overwriting the logos. Subsequently, the field of digital watermarking is primarily focused on embedding invisible watermarks, which operate by tweaking the content of the media imperceptibly. As the watermark cannot be seen, there must exist a robustness property that ensures the watermark data survives if the image is altered. Typical applications of digital watermarking can include broadcast monitoring, owner identification, proof of ownership, transaction tracking, content authentication, copy control, device control legacy enhancement and content description

Watermarking is the process of embedding a special data into media such as image, audio and video. This embedded information, known as a watermark, can be extracted from the multimedia contents later and used for supporting the ownership.

2.2 General Watermarking Framework

Mathematically [6], watermark embedding can be expressed like Eq.(1). If an original image λ and a watermark λ_W are given, the watermarked image λ' is represented as the following Eq(1).

$$\lambda' = \lambda + \alpha.\lambda_W \qquad (1)$$

Figure 1 shows watermark embedding process. An original image λ, a watermark λ_W enter to the system, α is a scaling factor and an optional public or secret key K may be used to guide the process. The output of the watermarking scheme is the watermarked image λ' [5].

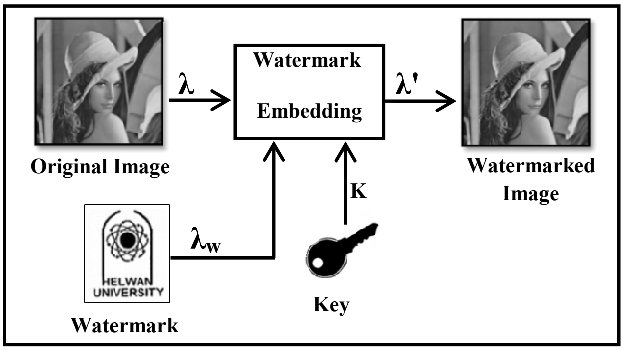

Figure1: Watermark embedding

The embedded watermark can be extracted later by two ways or more, either the original image is used to compare and find out the watermark (*non-blind watermark*) or a correlation measure is used to detect the watermark (*blind watermarking*).

In non-blind watermarking, the extraction of the embedded watermark can simply achieved by applying Eq. 2 , in which simply subtract the original signal from the watermarked one then divide it by the gain factor.

$$\lambda_W = (\lambda' - \lambda)/\alpha \qquad (2)$$

In blind watermarking, the extraction of the watermark can be achieved by using similarity measures as shown in Figure 2.

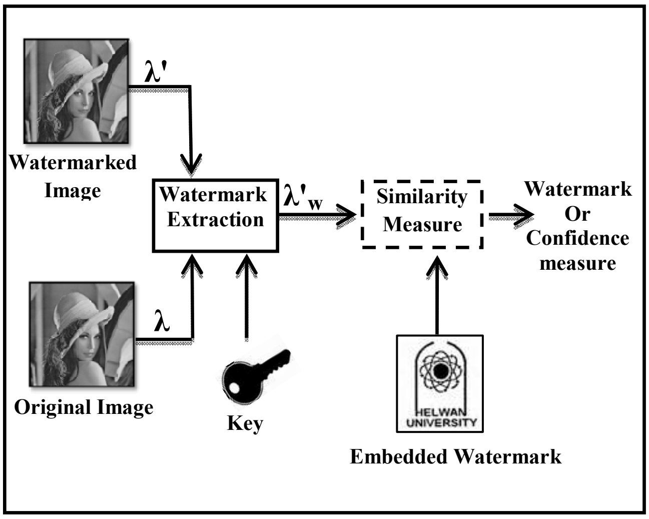

Figure2: Watermark extraction and detection.

There are some ways which can evaluate the similarity between the original and extracted watermarks. However, mostly used similarity measures are the correlation-based method. The following Eq.(3) is widely used as a watermark similarity measure. Generally, the extracted watermark λ'_W will not be identical to the original watermark λ_W. Eq. (3) computes the similarity between λ_W and λ'_W as the follows;

$$sim(\lambda_W, \lambda'_W) = \frac{\lambda'_W . \lambda_W}{\sqrt{\lambda'_W . \lambda'_W}} \qquad (3)$$

To decide whether λ_W and λ'_W match, one may determine, sim(λ_W, λ'_W) >T, where T is some threshold [5, 6].

2.3 Requirements of Watermarking

There are three main requirements of digital watermarking. They are transparency, robustness, and capacity [8].

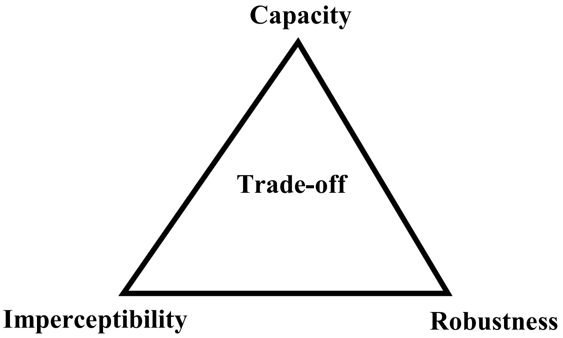

Figure 3: Trade-off among the imperceptibility, robustness and capacity

- **Transparency**

Transparency or fidelity is perceptual similarity between the original and the watermarked versions of the cover work.
The digital watermark should not affect the quality of the original image after it is watermarked.

- **Robustness**

Rrobustness is the ability to detect the watermark after common signal processing operations.
Watermarks should be robust against variety of geometrical and non-geometrical attacks.

- **Capacity**

Capacity or data payload is the number of bits a watermark encodes within a unit of time or work. This property describes how much data should be embedded as a watermark to successfully detect during extraction.

3. Watermarking Classification

In this section digital watermarks and their techniques is classified and segmented into various categories; Figure 4 shows Classification of watermarking techniques, for example, they can be classified according to [1-7]:

3.1 According host signal

The host or cover signal could be:

- **Text watermarking:** it inserts a watermark in the font shape and the space between characters and line spaces.
- **Image watermarking**: this embeds special information to an image and detects or extracts it later for ownership confirmation.
- **Video watermarking**: it is an extension of image watermarking. This method requires real time extraction and robustness for compression.
- **Audio watermarking:** this application area becomes a hot issue because of the internet music, MP3.

3.2 According to perceptivity

Digital watermarking is divided into two main categories: visible and invisible.

- **Visible watermark:** it is equivalent to stamping a watermark on paper, (ex.) television channels, like BBC, whose logo is visibly superimposed on the corner of the TV picture.
- **Invisible watermarking:** It is used to identify copyright data, like author, distributor, and so forth but it's more complex.

3.3 According to robustness

Watermarks need robustness to protect the ownership from various attacks. The followings show the classification dependent on the robustness of a watermark.

- **Robust:** resist various attacks, geometrical or non-geometrical without affecting embedded watermark.
- **Semi-fragile:** is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression.
- **Fragile:** fragile watermark is designed to be easily destroyed if a watermarked image is manipulated in the slightest manner. This watermarking method be used for the protection and the verification of original contents.

3.4 According to watermark type

Watermark types can be classified into two types: noise type and image type.

- **Noise types** have pseudo noise, Gaussian random and chaotic sequences.
- **Image types**, there are binary image, stamp, logo and label.

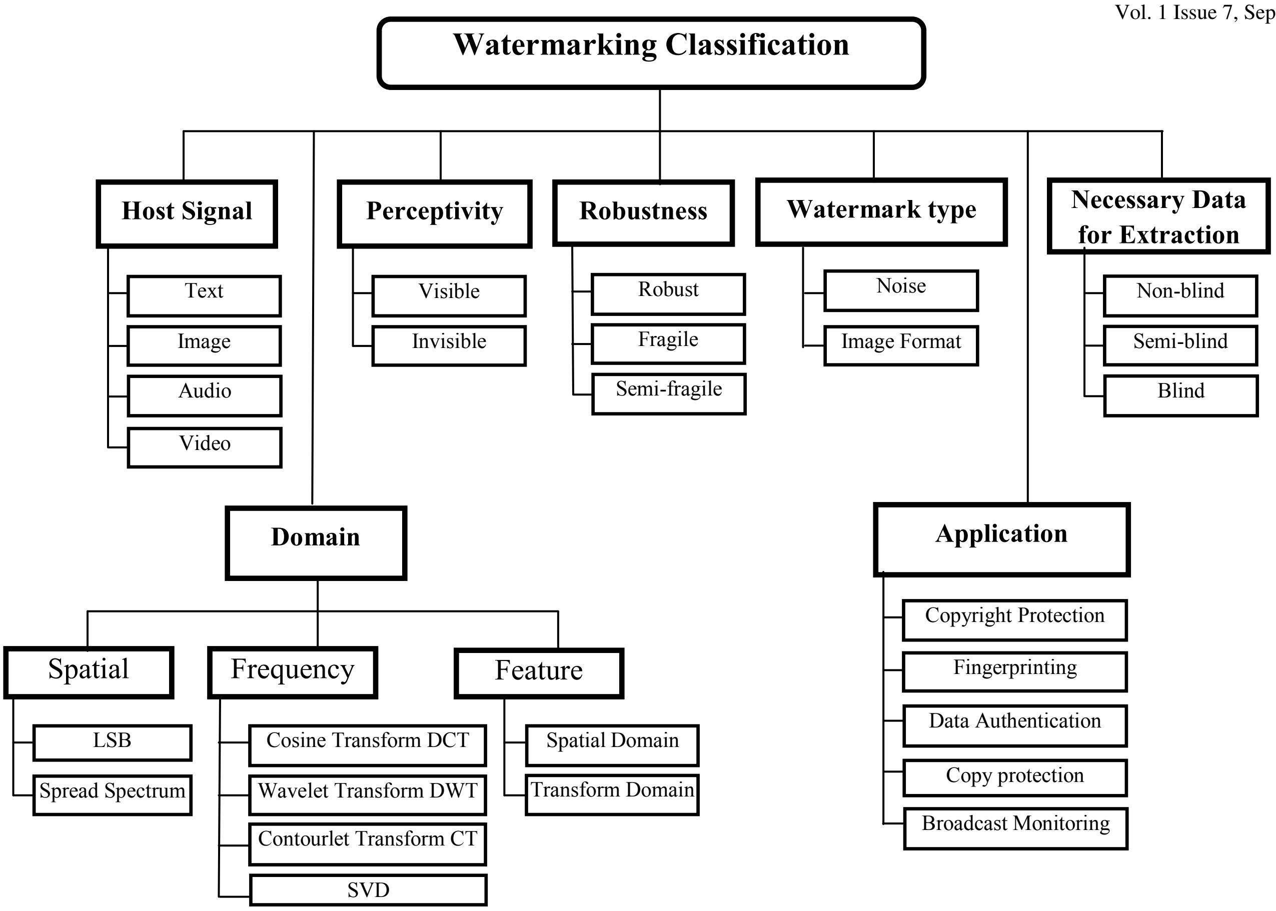

Figure 4: Classification of watermarking techniques

3.5 According to necessary data for extraction

In order to detect the watermark information, blind, semi-blind and non-blind techniques are used.

- **Non-blind:** this requires at least an original media. It extracts a watermark from the possibly distorted image and the original media.
- **Semi-blind:** it does not require an original media for detection.
- **Blind:** it requires neither an original media nor the embedded watermark. It is also referred to as public watermarking.

3.6 According to Processing Domain

Image watermarking can be applied to spatial domain and transform domain [1-3].

In **spatial domain** the watermark is inserted into the intensity values. The best widely known algorithm is LSB techniques; it is based on modifying the least significant bit layer of images. This technique based on the fact that the changes in least significant bits in an image would not have any effect on an image.

Another approach for embedding in spatial domain is correlation based techniques. The noise that statistically resembles common processing distortion is introduced to pixels in random walk. The noise is produced by a pseudo random generator using a shared key.

In **Transform Domain** image is represented in terms of frequencies , to transfer image to its frequency representation we can use several reversible transform like Discrete Cosine Transform DCT, Discrete Wavelet Transform DWT, Discrete Fourier Transform DFT, Contourlet Transform CT, or Singular Value Decomposition SVD. Each of the transforms has its own characteristics and represents the image indifferent ways.

Table 1: Comparison between watermarking techniques

Characteristics	***Spatial Domain***	***Transform Domain***
Computation Cost	Low	High
Robustness	Fragile	Robust
Perceptual quality	High Control	Low control

Capacity	High(depends on image size)	Low
Application	Authentication	Copyright

3.7 According to Applications

Digital watermarking can be applied to [1]:

- Copyright Protection and Authentication
- Fingerprinting and Digital "Signatures"
- Copy Protection and Device Control
- Broadcast Monitoring
- Data Authentication

4. Image Watermarking Survey

In this paper we would focus on robust image watermarking algorithms in transform domain like DCT, DWT, CT and SVD.
Table 2 presents briefly the most recent algorithms presented in robust image watermarking.

The classic and still most popular domain for image processing is that of the Discrete-Cosine-Transform, or DCT. Although changing the DCT coefficients will cause unnoticeable visual artifices, they do cause detectable statistical changes.

Another transform domain which is being exploited is Singular Value Decomposition (SVD) due to its simplicity in implementation and attractive mathematical features. It is one of the most powerful numerical analysis technique and used in various applications. Some SVD based algorithms are purely SVD based in a sense that only SVD domain is used to embed watermark into image.

Another domain exploited for embedding the watermark is the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to computes multiple "scale" wavelet decomposition.

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH, HL, HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.

Table 2: Image Watermarking Survey

Year	Author Name	Processing Domain	Features
2004	Fangjun Huang et al. [9]	DCT SVD	- achieve the highest possible robustness without losing the transparency.
2006	Enping Li et al.[10]	DWT	- robust to both common image processing operations and geometric attacks such as rotation, scaling, cropping.
2006	Jayalakshmi M. et al. [11]	CLT	- contourlet based algorithm outperforms wavelet and DCT based methods
2007	R. A. Ghazy et al.[12]	SVD	- Robust
2008	Shu Zhibiao et al.[13]	DWT	- Blind - Robust - invisible - secure
2008	Hanane Mirza et al.[14]	DWT	- High robustness - Reassuring rate of image recovery.
2008	B.Chandra Mohan et al. [15]	CLT	- Robust
2008	Azadeh Mansouri et al. [16]	DCT SVD	- robust against large amount of attacks - the best quality for watermarked image
2009	Tang Wenliang et al. [17]	Features based	- robust - resist geometrical attacks
2009	Shereen Ghannam et al. [18]	CLT	- robust
2010	Zaho et al.[7]	CLT	- Robust - Excellent perceptual invisibility
2010	Akhaee et al. [19]	CLT	- Robust - good transparency
2010	Swanirbhar Majumder et al. [20]	SVD Neural Network	- Increase the robustness against malicious attacks.
2010	Hongbo BI et al. [21]	SVD CT	- very robust against scaling, JPEG compression, cropping
2011	R. H. Laskar et al.[22]	DCT DWT	- Good imperceptibility - Higher robustness

2011	Jianhua Song et al.[23]	DWT	- Invisible - Robust - Bears very good security.
2011	LI Xiuguang et al.[24]	SVD	- Blind - Robust - Resist rotation and scaling attacks
2011	Mingli Zhang et al. [25]	SVD DWT	- robust to a wide range of attacks, especially geometrical attacks.
2012	Chen Li et al.[26]	DWT	- Conclude that biorthogonal wavelet better than others
2012	Subramanyam et al.[27]	DWT	- A robust watermarking algorithm to watermark JPEG2000 compressed and encrypted images.
2012	Wang, Chuntao et al. [28]	DWT GA	- High robustness - Greatly reduced arithmetic complexity.
2012	Xiong Shunqing et al. [29]	NSCT SVD	- Good impercbtbilty - Good robustness

5. Watermarking Arracks

Watermark attacks is classified into four distinct categories namely removal attacks, geometric attacks, cryptographic attacks and Removal attacks [8]

- **Removal attacks** This type of watermark attack does not attempt to find out the encryption techniques used or how the watermark has been embedded. Included in this category noising, histogram equalization, blur and sharpen attacks.

Geometry attacks this type of attack intends to distort the watermark signal. It is however still theoretically possible for the detector to recover the original watermark if the detail of the geometry attack can be established and a countermeasure applied. The process of correcting this type of attack is often referred to as synchronization. However, the complexity of the required synchronization process might be too prohibitively expensive and slow. Included in this category of watermark attacks are image rotation, scaling, translation and skewing.

- The aim of **cryptographic attacks** is to crack the security methods in watermarking schemes and thus find a way to remove the embedded watermark information or to embed misleading watermarks. One of the techniques in this category is the brute-force search method.

- Another technique is called the **Oracle attack**, which is used to create a non-watermarked signal when a watermark detector device is available.

- **Protocol attacks** it add the attacker's own watermark signals onto the data in question. This results in ambiguities on the true owners question. Protocol attacks target the entire concept of using watermarking techniques as a solution to copyright protection. Another protocol attack is the copy attack: instead of destroying the watermark, the copy attack estimates a watermark from watermarked data and copies.

The previous classification of watermark attacks can be summarized in Figure 5. [8]

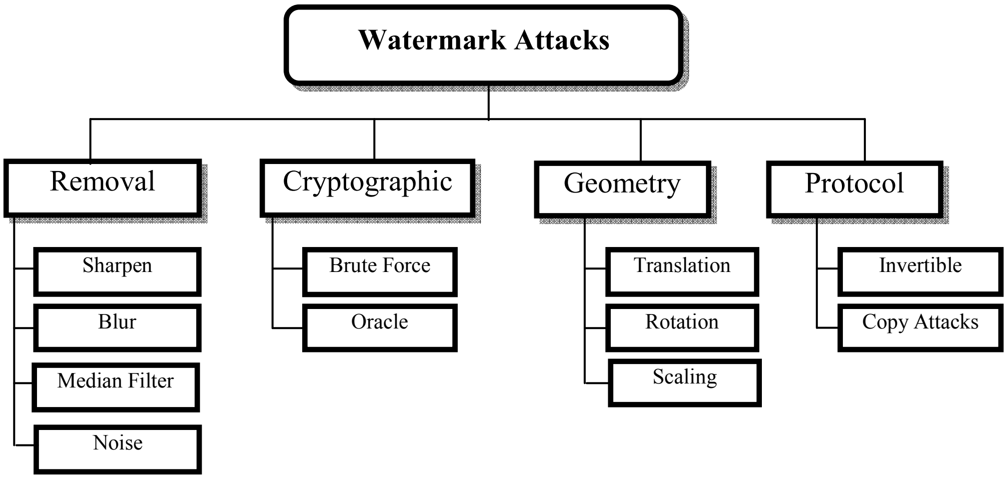

Figure 5 Classification of watermark attacks

6. Conclusion

In this paper we presented digital watermarking overview, application, attacks and techniques. We tried to classify and analyse many recent watermarking techniques to help new researchers in related areas.
We classified the previous researches from various point of views such as: host signal, perceptivity, robustness, watermark type, necessary data for extraction, processing domain, and applications.
Due to space limitation we presented image watermarking survey only, but audio and video techniques are also required to study intensively.

7. References

[1] C. S. Lu, *Multimedia Security: Steganography and Digital Watermarking for Protection of Intellectual Property*, Idea Group Publishing, 2005.

[2] F. Hartung, and M. Kutter, “*Multimedia Watermarking Techniques*”, IEEE Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, pp. 1079–1107, July 1999.

[4] Sin-Joo Lee and Sung-Hwan Jung,"*A Survey of Watermarking Techniques Applied toMultimedia*",ISIE 2001.

[5] Dickman Shawn D.,"*An Overview of Steganography"*, James Mandison University Infosec Transport, July 2007.

[6] Petitcolas Fabien A., Anderson Ross J., Kuhn Markus G., *"Information Hiding – A Survey"*, Proceedings of IEEE, Special issue on protection of multimedia content, pp 1062-1078,July 1999.

[7] Xi Zhao, Anthony T. S. Ho: *An Introduction to Robust Transform Based Image Watermarking Techniques*. Intelligent Multimedia Analysis for Security Applications 2010: 337-364

[8] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking and fundamentals, Morgan Kaufmann, San Francisco, 2002.

[9] Fangjun Huang, Zhi-Hong Guan: A hybrid SVD-DCT watermarking method based on LPSNR. Pattern Recognition Letters 25(15): 1769-1775 (2004)

[10] Enping Li, Huaqing Liang, Xinxin Niu. , Blind Image Watermarking Scheme Based on Wavelet Tree Quantization Robust to Geometric Attacks, Proceedings of the 6th World Congress on Intelligent Control and Automation, IEEE, 2006.

[11] Jayalakshmi M., S. N. Merchant, Uday B. Desai, Digital Watermarking in Contourlet Domain, The 18th International Conference on Pattern Recognition (ICPR'06), IEEE, 2006.

[12] R. A. Ghazy, N. A. El-Fishawy, M. M. Hadhoud, M. I. Dessouky, An Efficient Block-by-Block SVD-Based Image Watermarking Scheme, National Radio Science Conference, Vols. pp. 1–9, 2007.

[13] Shu Zhibiao, Lian Yulong, A blind watermarking algorithm for digital image based on DMWT and CBWT , Journal of Algorithms & Computational Technology, Vols. 2, No. 1, pp. 1748-3018,Springer, March 2008.

[14] Hanane Mirza, Hien Thai,Zensho Nakao, Color Image Watermarking and Self-recovery Based on Independent Component Analysis, Artificial Intelligence and Soft Computing, – ICAISC, Vol. 5097/2008 .

[15] Kumar, B.Chandra Mohan and S.Srinivas, Robust Digital Watermarking Scheme using Contourlet, IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.2,February 2008.

[16] ecure Digital Image Watermarking Based on SVD-DCT. Azadeh Mansouri, Ahmad M. Aznaveh, and Farah T. Azar. s.l. : Springer-Verlag Berlin Heidelberg , 2008, Vols. pp. 645–652.

[17] A Feature-Based Digital Image Watermarking Algorithm Resisting to Geometrical Attacks. Wenliang, Tang. s.l. : Second International Symposium on Electronic Commerce and Security, IEEE, 2009.

[18] Shereem Ghanem and Fatma A.E. Abou-Chadi, "Contourlet Versus Wavelet Transform: A Performance Study for a Robust Image Watermarking", 2009.

[19] Contourlet-Based Image Watermarking Using Optimum Detector in a Noisy Environment . Akhaee, M.A., Sahraeian, S.M.E. and Marvasti, F. 4 , s.l. : IEEE, 2010, Vols. 19 , pp. 967- 980. 1057-7149 .

[20] Swanirbhar Majumder, Tirtha Shankar Das,Vijay H. Mankar,Subir K. Sarkar, SVD and Neural Network Based Watermarking Scheme. Communications in Computer and Information Science ,Information Processing and Management , 2010 : Springer, Vol. 70.

[21] Hongbo BI, Xueming LI, Yubo ZHANG , Yan XU, A Blind Robust Watermarking Scheme Based on CT an SVD. s.l. : IEEE, 2010.

[22] R. H. Laskar, Madhuchanda Choudhury,Krishna Chakraborty,Shoubhik Chakraborty, A Joint DWT-DCT Based Robust Digital Watermarking Algorithm for Ownership Verification of Digital Images. s.l. : Communications in Computer and Information Science, Springer, 2011, Vol. 157.

[23] Jianhua Song, Guoqiang Wang, A Wavelet Domain Digital Image-Watermarking by Double Encryption Based on Arnold Transform and Chaos. International Conference in Electrics, Communication and Automatic Control Proceedings, s.l. : Springer New York, 2011.

[24] Yang, Xiuguang Li and Xiaoyuan, A blind watermarking algorithm resisting to geometric transforms based on SVD. s.l. : WUHAN UNIVERSITY JOURNAL OF NATURAL SCIENCES, 2011, Vols. 16, Number 6 (2011), 487-49.

[25] Mingli Zhang, Qiang Zhang, and Changjun Zhou, Robust Digital Image Watermarking in DWT-SVD. s.l. : Springer-Verlag Berlin Heidelberg, 2011, Vols. Part II, LNAI 7003, pp. 75–84.

[26] Chen Li, Cheng Yang, Wei Li, Wavelet Bases and Decomposition Series in the Digital Image Watermarking. Advances in Intelligent and Soft Computing, Advances in Multimedia, Software Engineering and Computing Vol.2 , s.l. : Springer, 2012, Vol. 129/2012.

[27] Subramanyam, A.V., Emmanuel, S. and Kankanhalli, Robust Watermarking of Compressed and Encrypted JPEG2000 Images. M.S. 3, s.l. : Multimedia, IEEE Transactions on , 2012, Vols. 14 , Part:2, pp. 703-716. 1520-9210 .

[28] Wang, Chuntao, Ni, Jiangqun and Huang, Jiwu.3, An Informed Watermarking Scheme Using Hidden Markov Model in the Wavelet Domain. s.l. : Information Forensics and Security, IEEE Transactions on , Vols. 7, pp. 853-867. 1556-6013 .

[29] Xiong Shunqing, Zhou Weihong, Zhao Yong, A New Digital Watermarking Algorithm Based on NSCT and SVD. pages: 49-57,: ADVANCES IN CONTROL AND COMMUNICATION, Lecture Notes in Electrical Engineering, 2012, Vol. 137.