



A Comparative Analysis on Digital Watermarking with Techniques and Attacks

Smita Pandey, Rohit Gupta

Department of CSE, Vikarant Institute of Technology & Management, Gwalior, Madhya Pradesh, India

Abstract— Digital media is the need of a people now a day as the alternate of paper media. As the technology grown up digital media required protection while transferring through internet or others mediums. Watermarking techniques have been developed to fulfill this requirement. This paper aims to provide a detailed survey of all watermarking techniques specially focuses on image watermarking types and its applications in today's world.

Keywords— Watermarking, DWT, Copyright, PSNR.

I. INTRODUCTION

Today's generation is witness of developments of digital media. A very simplest example of digital media is a photo captured by phone camera. The use of Digital media is common in present era. Other example of Digital media is text, audio, video etc. We know an internet is the fastest medium of transferring data to any place in a world. As this technology grown up the threat of piracy and copyright very obvious thought is in owners mind. So Watermarking is a process of secure data from these threats, in which owner identification (watermark) is merged with the digital media at the sender end and at the receiver end this owner identification is used to recognize the authentication of data. This technique can be applied to all digital media types such as image, audio, video and documents. From many years researchers and developers worked in this area to gain best results[1].

II. PRINCIPLE OF WATERMARKING

A watermarking system is usually divided into three distinct steps, embedding, attack and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself[2].

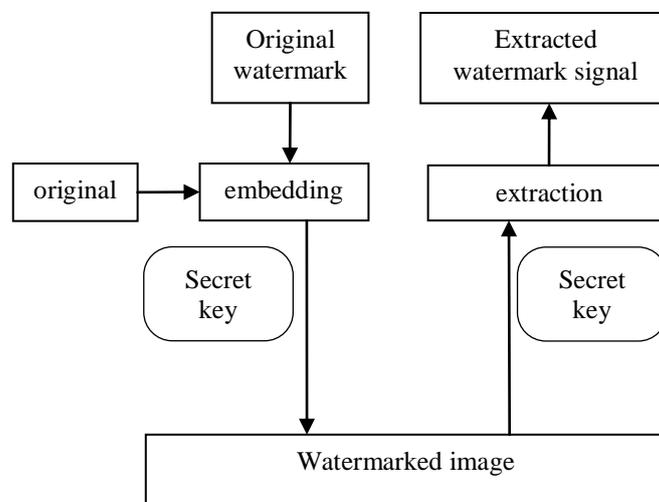


Fig. 1 Block diagram of Watermarking Process

The original image and the desired watermark are embedded using one of the various schemes that are currently available. The obtained watermarked image is passed through a decoder in which usually a reverse process to that employed during the embedding stage is applied to retrieve the watermark. The different techniques differ in the way in

which it embeds the watermark on to the cover object. A secret key is used during the embedding and the extraction process in order to prevent illegal access to the watermark[2].

III. TYPES OF WATERMARKING

a) Visible:

The watermark is visible that can be a text or a logo. It is used to identify the owner [3].

b) Invisible:

The watermark is embedded into the image in such a way that it cannot be seen by human eye. It is used to protect the image authentication and also prevent it from being copied [3]. Invisible watermark can be further classified into three types:

i. Robust Watermark:

Robust Watermark aims to embed information in a file that cannot be easily destroyed. They are designed to resist any manipulations that may be encountered. All applications where security is the main issue use robust watermarks [3].

ii. Fragile Watermark:

They are designed with very low robustness. It is used to check the integrity of objects [3].

iii. Public and Private Watermark:

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

IV. WATERMARKING TECHNIQUES

The various watermarking techniques are:

A. Spatial Domain Techniques

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

a) Least Significant Bit Coding (LSB):

LSB coding is one of the earliest methods. Least significant bit can be applied in any form of watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component [3].

b) Predictive Coding Schemes:

A predictive coding scheme was proposed by Matsui and Tanaka for grayscale images. In this method the correlation between adjacent pixels are exploited. A set of pixels where the watermark has to be embedded is chosen and alternate pixels are replaced by the difference between the adjacent pixels. This can be further improved by adding a constant to all the differences. A cipher key is created which enables the retrieval of the embedded watermark at the receiver. This is much more robust as compared to LSB coding [3].

B. Transform Domain Watermarking

The transform domain watermarking is achieving very much success as compared to the spatial domain watermarking. In the transform domain watermarking, the image is represented in the form of frequency. In the transform domain watermarking techniques, firstly the original image is converted by a predefined transformation. Then the watermark is embedded in the transform image or in the transformation coefficients. Finally, the inverse transform is performed to obtain the watermarked image [4]. Most commonly used transform domain methods is Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT).

a) Discrete Fourier Transformation (DFT)

It is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks. DFT uses complex numbers, while DCT uses just real numbers[2].

b) Discrete Cosine Transformation (DCT)

It is a kind of transform whose kernel is in cosine function. It works for complex numbers. It converts an image from spatial domain to transform domain and vice versa. When an image is transformed using DCT it divides given image into 8*8 blocks. Then it finds low and high frequency components by zigzagcanning. And then embeds watermark in low frequency components. This method provides high robustness against JPEG compression. DCT methods lack resistance to strong geometric attacks[5].

a) Discrete wavelet transforms (DWT):

Wavelet Transform is a modern technique frequently used in digital image processing, compression, watermarking etc. The transforms are based on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely.

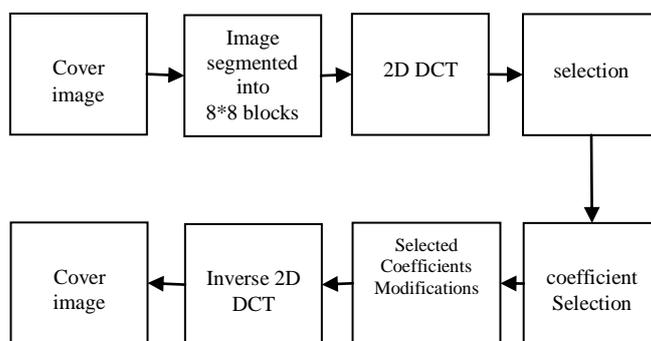


Fig.2 Typical structure of DCT based watermarking

Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL). 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.

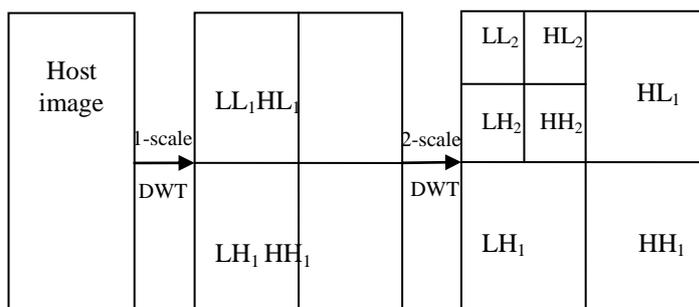


Fig. 3 Wavelet based transforms

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 [6]. 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 [6]. However, DWT is much preferred because it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image [7]. The basic idea of discrete wavelet transform in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequencies.

b) Singular Value Decomposition Watermarking

Singular value decomposition is one of the most powerful numerical analysis tool used to analyze matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the same size as original matrix. SVD transformation preserves both one-way and non-symmetric properties, usually not obtainable in DCT and DFT transformations. Wie Cao et.al developed SVD in DT-CWT domain [8]. Using SVD in digital image processing has advantages like the size of the matrices from SVD transformation is not fixed and can be a square or a rectangle; singular values in a digital image are less affected if general image processing is performed and singular values contain intrinsic algebraic image properties. The singular values of the host image are modified to embed the watermark image by employing multiple singular functions. Watermark is embedded and extracted by adjusting value between selected coefficients and actual output trained by support vector regression. SVD factorization is done on different nonoverlapping blocks by taking wavelet transform. Watermarks are generated by singular value of different block.

c) Principal Component Analysis:

PCA is generally used dimensionality step-down method for image recognition, compression and retrieval [9]. PCA is a regular scheme applied in signal processing and statistical pattern recognition for dimensionality step-down and feature extraction.

Algorithm	Advantages	Disadvantages
LSB	1.Easy to implement and understand 2.Low degradation of image quality 3. High perceptual transparency.	1. It lacks basic robustness 2. Vulnerable to noise 3. Vulnerable to cropping, scaling.
Patchwork	1. High level of robustness against most type of attacks	1. It can hide only a very small amount of information

DCT	1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not get affected and the watermark will not be removed by any kind of attack.	1. Block wise DCT destroys the invariance properties of the system.
DWT	1. Allows good localization both in time and spatial frequency domain 2. Higher compression ratio which is relevant to human perception	1. Cost of computing may be higher. 2. Longer compression time. 3. Noise/blur near edges of images or video frames.
DFT	1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions	1. Complex implementation 2. Cost of computing may be higher.

V. WATERMARKING APPLICATIONS

Watermarking technologies is applied in every digital media whereas security and owner identification is needed[10]

A. Owner Identification

The application of watermarking to which he developed is to identify the owner of any media. Some paper watermark is easily removed by some small exercise of attackers. So the digital watermark was introduced. In that the watermark is the internal part of digital media so that it cannot be easily detected and removed.

B. Copy Protection

Illegal copying is also prevent by watermarking with copy protect bit. This protection requires copying devices to be integrated with the watermark detecting circuitry.

C. Medical Applications

Medical media and documents also digitally verified, having the information of patient and the visiting doctors. These watermarks can be both visible and invisible. This watermarking helps doctors and medical applications to verify that the reports are not edited by illegal means.

D. Data Authentication

Authentication is the process of identify that the received content or data should be exact as it was sent. There should be no tampering done with it. So for that purpose sender embedded the digital watermark with the host data and it would be extracted at the receivers end and verified.

E. Fingerprinting

A fingerprinting is a technique by which a work can be assigned a unique identification by storing some digital information in it in the form of watermark. Detecting the watermark from any illegal copy can lead to the identification of the person who has leaked the original content. In cinema halls the movies are played digitally through satellite which has the watermark having theater identification so if theater identification detected from a pirated copy then action against a theater can be taken.

VI. WATERMARKING ATTACKS

There are various possible malicious intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing soft wares made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is prevent the watermark from performing its intended purpose[11].

a) Removal Attack:

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.

b) Interference attack:

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.

c) Geometric attack:

All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

d) Low pass filtering attack:

A low pass filtering is done over the watermarked image and it results in a difference map composed of noise.

e) Forgery attack:

The forgery attacks that result in object insertion and deletion, scene background changes are all tantamount to substitution.

f) Security Attack:

In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. The watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged.

g) Protocol Attack:

The protocol attacks do neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark's implementation. Consequently, a robust watermark must not be invertible or to be copied. A copy attack, for example, would aim at copying a watermark from one media into another without knowledge of the secret key.

h) Cryptographic attacks:

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 [12]. 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.

VII. LITERATURE REVIEW

Shaikh et.al [13] in this paper video watermarking with 3-level DWT is proposed which is perceptually invisible. Perceptually invisible means that the watermark is embedded in video in such a way that the modification to the pixels values is not noticed. In proposed work using two different videos and different logo images and shown how watermark is detected and watermarks not detected. The secret key is given to watermark image during embedding process and while extracting the watermark image the same secret key is used. The result of MSE should be as low as possible to have less error and the PSNR should be as high as possible to have better quality of reconstructed video.

Uma Rajput et.al [14] in this paper proposed a novel technique for RGB digital watermarking based on 2-Discrete Cosine Transform with discrete wavelet transform algorithm. For this use of two images- first one is cover image and second one is secret image. For providing better security, we worked on RGB elements. In this performed on two algorithms first one is 2-DWT and secondly 2-DCT applied on RGB elements. Experimental results Shows that PSNR, NE value, and PSNR reach up to 56%.

Baiying et.al [15] in this paper proposed a robust audio watermarking scheme based on LWT-DCTSVD, DWT-DCT-SVD with exploration of DE optimization and DM quantization. The attractive properties of SVD, LWT/DWT-DCT, DE and quantization technique make our scheme very robust to various common signal processing attacks. Meanwhile, the proposed scheme is not only robust against hybrid and desynchronization attacks, but also robust against the Strimark for audio attacks. The experimental results validate that the proposed watermarking scheme has good imperceptibility too. The comparison results with other SVD-based and similar algorithms indicate the superiority of scheme.

Vinita Gupta, Mr. Atul Barve [16] in 2014, here they surveyed the paper on digital image watermarking. They also classified the watermarking techniques based on the transform domain where the watermark is embedded. Also, explain the watermarking properties, applications and techniques used. This paper also shows the different techniques and discusses the important technology called QR code which can be used in future work.

Sasmita Mishra, Amitav Mahapatra, Pranati Mishra [2] in 2013, in this paper, they presented a comprehensive survey on various digital watermarking techniques their requirements and applications. The use of different type of watermark is application dependent. But there are neither type of watermarks are ideal when considering "information preserving" transformations that preserve the meaning of the content & "information altering" transformations that change the expression of the content. To solve this problem a semi fragile watermark is for images which can detect the information altering transformations even after the watermarked contents are subjected to information preserving alterations have to be used.

Prof. Manoj Ramaiya Richa Mishra [17] in 2012, in this paper a new robust watermarking technique for color images was performed. In this paper, the RGB image is converted to HSV and watermarked by using discrete wavelet transform. Watermarking embedded stage and extraction stage is designed using another low power invisible watermarking algorithm. In this, the host signal is an image and after embedding the secret data a watermarked image is obtained and then extracts secret image and original image separately. In future the resulted watermarked image was tested with several attackers to verify the robustness and VLSI implementation of invisible watermarking algorithm using VHDL code and also check various performances like power, PSNR and tamper detection and area.

Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh [18] in 2013, here they have reviewed some recent algorithms, proposed a classification based on their intrinsic features, inserting methods and extraction forms. Many watermarking algorithms are reviewed in the literatures which show advantages in systems using wavelet transforms with SVD. In this paper they also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, properties of watermarking and its applications have been presented. In future works, the use of coding and cryptography watermarks will be approached.

Chen Li, Cheng Yang, Wei Li [19] in "Wavelet Bases and Decomposition Series in the Digital Image Watermarking" analyzes and compares the performance of different wavelet bases in the digital image watermarking and the effect of

different wavelet decomposition series for the digital image watermarking embedding based on the application of wavelet in the digital image watermarking. The experiments proved the digital image watermarking embedding based on bi-orthogonal wavelet better than others.

Xiong Shunqing, Zhou Weihong, and Zhao Yong [20] in "A New Digital Watermarking Algorithm Based on NSCT and SVD" proposed a new algorithm of digital watermarking based on combining the Non Sub Sampled Contourlet Transform and SVD, they first applied the NSCT to the image and extract the low-frequency sub-band of image, and then decompose the low-frequency sub-band of image by SVD, finally embed the watermarking in the decomposed singular value. The experiment results show that the new algorithm has good ability in standing up to geometric attacking, especially rotation attacks.

VIII. PERFORMANCE MEASUREMENT

i) Mean square error (MSE)

The MSE in an image watermarking is to estimate or measures the average of the squares of the "errors", between host image and watermark image [21].

$$MSE = \frac{1}{MN} \sum_i^M \sum_j^N (W_{ij} - H_{ij})^2$$

Where M, N is pixel values in host image

W_{ij} = Pixel value in Watermarked Image

H_{ij} = Pixel value in Host Image

ii) Peak signal to noise ratio (PSNR)

PSNR is used to determine the Efficiency of Watermarking with respect to the noise. The noise will degrade the quality of image. The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio [21]. It is given by

$$PSNR = 10 * \log_{10} \left(\frac{p^2}{MSE} \right)$$

Where p = maximum value in host image.

iii) Bit Error Rate (BER)

This performance metric is suitable for random binary sequence watermark. The parameter is defined as ratio between number of incorrectly decoded bits and length of the binary sequence. BER indicates probability of incorrectly decoded binary patterns. It is defined as follows[8].

$$BER = \frac{DB}{NB}$$

where, DB : No. of incorrectly decoded bits , NB : Total no. of bits

IX. CONCLUSION

Digital watermarking is very useful method for providing security to the digital media on the internet technology. In this paper, survey of different techniques based on spatial domain (LSB) and the transform domain (DCT, DWT, DFT). In this paper we also have presented a review of the significant techniques in existence for watermarking those which are employed in copyright protection. Along with these, an introduction to digital watermarking, aspects of watermarking and its applications have been presented.

REFERENCES

- [1] Lalit Kumar Saini, Vishal Shrivastava "A Survey of Digital Watermarking Techniques and its Applications" International Journal of Computer Science Trends and Technology (IJCSST) – Volume 2 Issue 3, May-Jun 2014.
- [2] Sasmita Mishra, Amitav Mahapatra, Pranati Mishra "A Survey on Digital Watermarking Techniques" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3) , 2013, 451-456
- [3] Manjinder Kaur and Varinder Kaur Attri "A Survey on Digital Image Watermarking and Its Techniques" International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 8, No. 5 (2015), pp. 145-150.
- [4] F. Daraee and S. Mozaffari, "Watermarking in binary document images using fractal codes", Pattern Recognition Letter (2013).
- [5] Urvi H. Panchal, Rohit Srivastava "A Comprehensive Survey on Digital Image Watermarking Techniques" Fifth International Conference on Communication Systems and Network Technologies 2015 IEEE.
- [6] Evelyn Brannock, Michael Weeks, Robert Harrison, Computer Science Department Georgia State University —Watermarking with Wavelets: Simplicity Leads to Robustness, Southeast on, IEEE, pages 587 – 592, 3-6 April 2008.
- [7] G. Bouridane. A, M. K. Ibrahim, —Digital Image Watermarking Using Balanced Multi wavelets, IEEE Transaction on Signal Processing 54(4), (2006), pp. 1519-1536.
- [8] Vaishali S. Jabade, Dr. Sachin R. Gengaje "Literature Review of Wavelet Based Digital Image Watermarking Techniques" International Journal of Computer Applications (0975 – 8887) Volume 31– No.1, October 2011.
- [9] Anand kumar, Mukesh gupta "Semi visible Watermarking Scheme Based on DWT and PCA" 2015 IEEE.

- [10] Mei Jiansheng, Li Sukang, “A Digital Watermarking Algorithm Based On DCT and DWT”, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107
- [11] Prabhishek Singh, R S Chadha “A Survey of Digital Watermarking Techniques, Applications and Attacks” International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.
- [12] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE “IA Review of digital image watermarking in health care”
- [13] Shaikh Shoaib, Prof. R. C. Mahajan “Authenticating Using Secret Key in Digital Video Watermarking Using 3-Level DWT” International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, IEEE 2015.
- [14] Uma Rajput, Nirupma Tiwari “A novel technique for RGB Invisible Watermarking Based on 2-DWT-DCT Algorithm” Proceedings of Global Conference on Communication Technologies (GCCT 2015) IEEE.
- [15] Baiying Lei, Ing Yann Soon, and Ee-Leng Tan “Robust SVD-Based Audio Watermarking Scheme With Differential Evolution Optimization” IEEE Transactions On Audio, Speech, And Language Processing, Vol. 21, No. 11, November 2013.
- [16] Vinita Gupta, Mr. Atul Barve, “ A Review on Image Watermarking and Its Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN:2277 128X, Volume 4, Issue 1, January 2014.
- [17] Prof. Manoj Ramaiya Richa Mishra, “ Digital Security using Watermarking Techniques via Discrete Wavelet Transform”, National Conference on Security Issues in Network Technologies August 11-12, 2012
- [18] Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, “A Review of Different Techniques on Digital Image Watermarking Scheme”, International Journal of Engineering Research, ISSN:2319- 6890, Volume No.2, Issue No.3, pp:193-199, 01 July 2013.
- [19] 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.
- [20] Xiong Shunqing, Zhou Weihong, Zhao Yong, “A New Digital Watermarking Algorithm Based on NSCT and SVD”. Advances in Control and Communication, LNEE, 2012, Vol.
- [21] Scott McCloskey, “Hiding Information in Images: An Overview of Watermarking”, Cryptography Research Paper ,11-9-2000