

Digital Image Watermarking: A Study on Techniques & Issues

Jobin Abraham

Abstract - Digital data can be easily copied and modified to create duplicate copies. These modified images are then redistributed through the Internet. As these illegal activities are becoming more and more common, mechanisms to protect digital resources are in high demand. Watermarking is an effective method for restricting abuses of published digital contents and to protect ownership rights of the owner. However, while watermarking, special care should be taken not to affect the visual quality of the host image. At the same time it must be reasonably robust and able to withstand illegal watermark removal attempts. This paper presents a study on watermarking techniques and associated issues.

Index Terms – attacks, frequency domain transforms, image watermarking, performance evaluation, watermark embedding and extraction

1 INTRODUCTION

The data published in digital formats especially in Internet can be easily copied and modified compared to analog counterparts [1]. Today Internet is viewed as the gateway for many e-commerce applications, content-on-demand services and more. The data transferred via Internet is open to the risk of being stolen and reused without permission from actual creator or the publisher. These concerns have fuelled intense research and development in the field of watermarking techniques that are able to conceal the watermark information from the unauthorized users attempting to modify the original contents.

Increased use and dependence of the Internet has adversely challenged the ownership rights of digital contents hosted in the net. Illegal activities as copying, alteration and reselling pose a serious threat to commercial and non-commercial multimedia contents like image, audio, video etc. In short digital multimedia contents are thus exposed to security challenges as authentication, integrity verification and protection.

1.1 E-security vs. Digital watermarking

For content data protection firewalls and anti-virus software's are widely used. The term e-security now has boarder meaning. It is not just firewalls and anti-viruses for intruder prevention and protecting digital contents. Conventional access control and other firewall mechanism though effectively protect the resources stored in the data bases fails when digital resources are publicly available as in the case of Internet. Pitfalls in conventional protections mechanism can lead to data losses in the form of unauthorized downloads and illegal tampering. Several other data protection mechanism such as cryptography, steganography, watermarking, digital rights management (DRM) etc are available and can be applied in different ways along with other mechanisms for enhancing the security of the system [2].

This paper discusses about recent trends and approaches in digital image watermarking. Digital watermarking is a powerful tool for protecting the ownership and copyrights of digital multimedia documents. During the watermarking

process identification information or a logo pertaining to the owner is imperceptibly embedded in the digital multimedia data. This hidden watermark information serves as a seal or mark of its owner whenever the ownership rights have to be ascertained.

2 TYPES OF DIGITAL WATERMARKING

Digital watermarking can be classified along different lines. Four general classifications possible are on the basis of visibility of embedded watermark, robustness, technique used for watermarking and watermarking media.

2.1 Visible or Invisible Watermarking

Watermarking is classified as Visible or Invisible based on the perceptibility of the embedded watermark in the host media. Visible Watermarking is visible to human eyes and are usually used as a means for overt assertion of ownership rights. Invisible watermarks are imperceptible to the viewers and they provide means for covert protection of copyright. Invisible watermarks are extracted from their host images when the content is exposed to an ownership threat at some later point of time.

2.2 Fragile or Robust watermarking

Watermarking is classified as fragile or robust based on the ability of the embedded watermark to withstand attacks on images. Robust watermarking techniques are designed to withstand degradations or signal processing attacks on watermarked resources. Fragile watermarking however is broken or lost when watermarked images are subject to any intentional or unintentional attacks. Yet another related category of fragile watermarking known as semi-fragile watermarking is widely used for verifying the content integrity. Tamper proofing of images using watermarking is possible with semi-fragile watermarking. By checking the correctness of the extracted watermark the extent of tampering can be measured. And also the portions in the image that were affected by illegal modifications can be identified.

2.3 Spatial or Transform domain watermarking

This classification is based on the domain in which the watermark embedding operation is performed. An image can be viewed as a two dimensional array of values that represent a shade or color for distinct regions in the given area or frame. Each of these values otherwise can be described to represent the intensity of pixels. During the process of watermark integration, either these values could directly be altered or the entire array be transformed to another form using a mathematical operation and the variations necessary for watermark inclusion be effected. Thus two different classes originate and are named as spatial domain watermarking [5-8] and transformed domain watermarking [9]. Transform domain watermarking methods generally uses frequency domain transforms as DCT (Discrete Cosine Transform) [10-13] or DFT (Discrete Fourier Transform) [14-16].

2.4 Image, Audio or Video watermarking

This class is based on the media on which watermark is embedded. The host resource can be image, audio or video. Different approaches are required for each case as the format used for image, audio and video is dissimilar. Thus we have image watermarking [15-16], audio watermarking [17] and video watermarking [18] schemes.

A fifth sub-classification often described in literature is blind or non-blind watermarking. The difference between the both is along the lines of use or non-use of the original or base resource at the time of watermark extraction. Non-blind watermarking method requires the original image for extracting the hidden watermark signal whereas the blind method are able to extract the hidden watermark without making reference to the original non-watermarked copy of the image.

3 APPLICATIONS OF WATERMARKING

The prime objective of digital watermarking is copyright protection. Digital watermarking integrates the owner name or a logo within the digital media. This identification information can later be used as proof of ownership. In addition to this, there are numerous other applications for digital watermarking [2]. Popular application scenarios include:

- **Proof of Ownership** - This is the most popular watermarking application and hence has received the most attention in literature. The embedded watermark could be extracted when illegal uses of restricted resources are detected and the watermark be used as evidence to prove the ownership of such digital documents in a court of law.
- **Transaction Tracking** - This is otherwise known as fingerprinting. A watermark unique to each copy is embedded into the resource before distributing to different recipients. Because of this permanent marking whenever unauthorized copies are spotted, source of redistribution could be tracked with the help of the hidden watermark.
- **Authentication** - The embedded watermark can be used as a tool to assure the integrity of data. The watermark data inserted for content protection remain imperceptible

and whenever an intruder modifies or manipulates the original data, the watermark gets ruptured. This leads to a situation where the watermark extraction will be non-continuous and faulty. This allows estimations about the depth of tampering with the help of watermarks. Hence this is also known as tamper-proofing.

- **Captioning** - The watermark employed serves more or less as a hidden label here. The invisible watermark is embedded together with detailed information as title of the work, name of the author, date etc. This associated information could also be used later to match a work to its copies or similar versions stored in the owner's database.
- **Covert communication** - Information or secret messages can be embedded in a cover image, and exchanged between two parties without getting noticed. Most important requirement to be fulfilled here is that the embedding process should not introduce distortions to a level that catches attention of viewers.
- **Visible Notes** - Watermarking in this application scenario conveys visible information to viewers. The embedded watermark could be used to issue warnings or serve as a line of caution against illegal copying or duplications. The objective here is to warn end users against redistribution or on operations that are not allowed.

4 WATERMARKING TECHNIQUES

Technically image watermarking can be defined as the process of integrating external information into a digital resource. Expression 1 shows the image I embedded by α times watermark signal W. Here α is the strength factor and varies in the range 0-1.

$$E(I) = I + \alpha W \quad (1)$$

Extraction is the reverse process that detects the imperceptibly hidden watermark. Equation.2 describes the extraction process that decodes the watermark signal from a marked image I_w .

$$D(I_w) = W \quad (2)$$

As mentioned earlier, watermarking methods are broadly classed as: spatial domain method and transform domain methods based on the domain in which embedding is applied. In spatial domain, watermark embedding is done by modifying the intensity of certain selected pixels in the host image. Histogram based methods [6-8] and least significant bit (LSB) replacement methods [9] are the two popular spatial domain watermarking techniques. In LSB methods, the watermark is embedded in the least significant bits (LSB) of the original image. Usually the least significant bits, $b_2 - b_0$, of the pixel is modified or replaced to contain the watermark bits. Spatial domain methods though simple, suffer serious setbacks in terms of their ability to withstand even simple image processing attacks. Spatial domain watermarking schemes are preferred because of their less computational overhead compared to frequency domain watermarking methods.

Transform domain watermarking methods uses transforms as DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform) or DWT (Discrete Wavelet Transform) to translate

the image array into a different set of values. Transform domain watermarking methods have gained popularity and wider acceptance due to their robustness to watermark removal attacks. Greater robustness of transform methods can best be explained as follows. When an image is inverse transformed during the embedding process the watermark is distributed irregularly over the entire host image making the removal of watermark almost impossible for attackers. Two transform techniques widely used are DCT and DWT. DCT is widely used for image compression and this fact has motivated the wide use of DCT for watermarking.

4.1 DCT Domain Watermarking

DCT breaks the image in to three bands: low frequency (L.F), mid-frequency (M.F) and high-frequency (H.F) regions. The fig.1 shows the distinct regions resulted on DCT transform operation. The low frequency bands carry most of the visual features of the image. The high-frequency bands are highly susceptible to compression and noise.

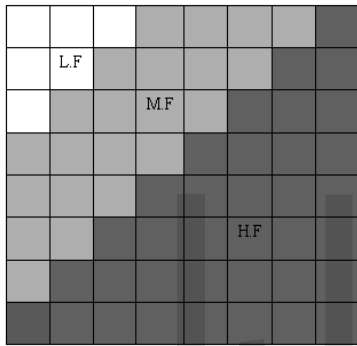


Fig.1 Distinct regions on DCT transformation

The choice of regions to be used for watermark integration in transformed domain is usually made based on the requirement or watermarking application. Low frequency region are extremely sensitive to human eyes. And the high frequency region gets curtailed at the time of compression. Hence these two regions are normally omitted and this leaves with the option of using mid-frequency region for embedding the watermark.

The 2-D DCT for two-dimensional data $f(x, y)$ is given by eqn.3.

$$c(u, v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (3)$$

The inverse 2-D DCT transform is found using eqn.4

$$f(x, y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \alpha(u)\alpha(v)c(u, v) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (4)$$

where $x, y = 0, 1, 2, 3, \dots, N-1$ and $\alpha(u), \alpha(v)$ is given by

$$\alpha(u), \alpha(v) = \begin{cases} \sqrt{\frac{1}{N}} & u, v = 0 \\ \sqrt{\frac{2}{N}} & u, v = 1, 2, \dots, N-1. \end{cases}$$

Most proposed scheme applies DCT after decomposing image into non-overlapping sub-blocks, normally of size 8x8. DCT of an 8x8 block results in 64 coefficients. The first component is called DC coefficient and remaining 63 are AC coefficients. As seen earlier the transformed data falls into three regions, low frequency region, medium frequency and high frequency region. Medium frequency region are less exposed to various attacks and hence is the most appropriate and preferred area for integrating the watermark signal [12].

4.2 DWT Domain Watermarking

2DWT transform operation decomposes the image array into four non-overlapping multi-resolution sub-bands namely, approximation matrix (LL), horizontal details (LH), vertical details (HL) and the diagonal detail matrix (HH) as shown in fig.2. The sub-band LL represents the coarse-scale coefficients and the other three bands represent the finer scale. Most of the image energy is concentrated at lower frequency (LL) band and the high frequency sub-bands represents the edges and textures of the image.

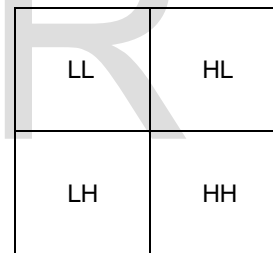


Fig.2 2-level DWT

For two dimensional arrays, applying DWT corresponds to application of two dimensional filters in each dimension. LL is the result of low pass filtering in row and column direction and HH is the result of high pass filtering in both directions. The LH and HL sub-bands are the results of low pass filtering in one direction and high pass filtering in the other direction. The decomposition process can be repeated to compute multiple scale decomposition. Fig.3 shows next level decomposition of LL sub-band.

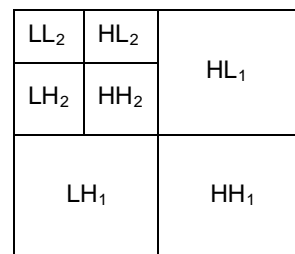


Fig.3 multi-resolution DWT

As it can be seen that most of the energy is concentrated in LL sub-band after processing the image using DWT, usually watermark embedding is imposed on any one detail band. This minimizes the effect of distortion. Most proposed watermarking algorithm embeds watermark in sub-bands LH or HL where acceptable performance of robustness and imperceptibility is experimentally assured.

4.3 Multi-transform domain Watermarking

Recent proposed schemes are increasingly found to make use of more than one frequency domain transform [17, 19-21]. This is so attempted to draw a wider set of the advantages that are unique to different techniques and make the scheme superior in performance in terms of robustness and watermark imperceptibility.

Yassine et al [17] proposes a method for audio watermarking using DWT and DST (Discrete Sine Transform). The original audio signal is first decomposed using wavelet transform. This stage is then followed by DST operation on approximation and detail coefficients over non-overlapping frames. Then the watermark is added to first five coefficients from each frame.

One of the earliest DWT-DCT combined watermarking is proposed in [21]. The paper claims the usage of combined transforms compensate the drawbacks of each other, resulting in a superior watermarking scheme than if the transforms were implemented independently. Image is decomposed using multi-resolution DWT. HL_2 or HH_2 sub-band is then divided into 4×4 blocks to which DCT is applied. A mid-frequency coefficient from one of these sub-bands is used for embedding the watermark bit. The robustness of the scheme is successfully tested to noise addition, compression and cropping attacks on watermarked image. Combined DWT-DCT is found to yields better results at the time of watermark extraction than otherwise.

5 WATERMARKING PROCESS

Main stages in a watermarking process are Watermark embedding and Watermark extraction. Sometimes these two stages are preceded by a watermark preprocessing stage. The preprocessing stage is often used to optimize the watermark or to scramble the watermark using a key.

General steps in majority of frequency domain watermark embedding are:

- 1) Decompose the host image into sub-blocks
- 2) Apply DCT/DWT on image sub-block
- 3) Embed the watermark by altering the coefficients
- 4) Apply inverse DCT/DWT on all blocks and
- 5) Rebuilt the watermarked copy of image by recombining the sub-blocks.

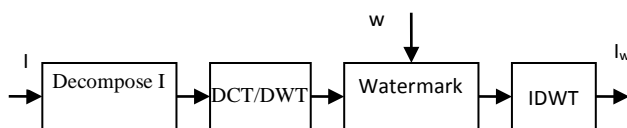


Fig.4 Watermark embedding

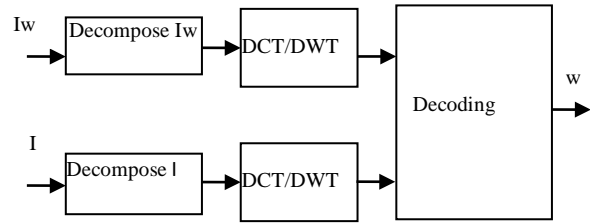


Fig.5 Stages in watermark extraction (non-blind)

Fig.4 shows the block diagram of a typical frequency domain watermark embedding process. The extraction process decomposes the image by the same considerations adopted in embedding algorithm. The DCT/DWT coefficients of sub-blocks host image is compared against that of watermarked image. The fig.5 shows the block diagram of stages in a general extraction process. Other than these kinds, there are also blind watermark extraction methods that do not ask for the original image whilst detecting the hidden watermark information.

5.1 Watermark

The identification pattern embedded in to the source digital resource is known as the watermark. Selection of watermark and the form in which embedding is implemented is different across the schemes. The pattern is usually a logo or a unique identification text that refer to the owner of the digital resource. In literature unveils watermarking schemes using various kinds watermark. They vary in size and shapes. Some schemes use a PN sequence, few use binary images and some schemes use grayscale image as the logo.

In majority of the papers binary images are used the logo for watermarking. And grayscale image, if adopted as the watermark, is converted into one dimensional binary image before embedding. The algorithm in [19] use a 256×256 grayscale image as watermark, however this watermark is converted to binary before embedding in the host image. Here two pseudorandom sequences, one for embedding bit 1 and the other for bit 0, generated using a key identifies the embedding coefficients from DCT coefficient block.

6 PERFORMANCE EVALUATIONS

The proposed algorithms are tested by implementing on various known test images. During the watermark decoding phase the accuracy of the hidden watermark extracted proclaims the success of the scheme. Most important is the robustness of the scheme. To estimate this factor, the watermarked image is subject different set of signal processing attacks including image compression. Extraction is again attempted to observe how far a recognizable watermark extraction is possible.

Two most common evaluation metrics used for performance evaluation of watermarking schemes are PSNR and Correlation Coefficient. Quality of the watermarked images is evaluated using PSNR (Peak Signal Noise Ratio) ratio. Bigger the PSNR value, better the quality of the watermarked image and the scheme in question. PSNR is found using the equ.5.

$$PSNR = 20 \log \left[\frac{255}{RMSE} \right] \quad (5)$$

Here, 255 is the maximum possible pixel intensity value in a gray scale image and RMSE is root mean square error. RMSE can be found by computing square root of MSE (mean square error) given by equ.6. Let I is the base image of size $N \times N$ and I_w is the watermarked copy of I , then MSE is given by

$$MSE = \sum (I(i, j) - I_w(i, j)) / N * N \quad (6)$$

The Normalized cross correlation (NCC) is calculated using the equation.7 to evaluate the effectiveness of the scheme especially after attacks. NCC ranges from 0 to 1. A value close to 1 indicates that the extracted signal closely resembles the original embedded watermark.

$$NCC = \frac{\sum_{i=1}^M \sum_{j=1}^N [W(i, j) \cdot W'(i, j)]}{\sum_{i=1}^M \sum_{j=1}^N [W(i, j)]^2} \quad (7)$$

In the above, W is the original watermark and W' is the extracted watermark. Size of the watermark is $M \times N$. NCC measurement on watermark extracted from attacked images may differ in precision and accuracy depending upon the intensity of attack undergone and also on the robustness of the scheme. In most cases a predefined threshold is accepted upon as a yardstick to decide whether the watermark extracted is acceptable or not.

Another commonly used metric for performance evaluation is BER (Bit error ratio). BER estimates the number of bits that are extracted correctly during the stage of extraction from a watermarked image. BER is computed using equ.8.

$$BER = \frac{\text{Number of extracted bits}}{\text{Number of embedded bits}} \quad (8)$$

The BER measure considers the count of correctly extracted watermark bit when compared to the originally embedded watermark. BER value ranges from 0 to 1. The maximum value of 1 means all the embedded bits of watermark are extracted successfully from their actual positions.

7 COMMON ATTACKS

Any operation, intentional or unintentional, on watermarked data that impairs or damages the hidden watermark is named as attack. Digital Images are targeted to various attacks as cropping, scaling, rotating, scaling, compression and noise addition. An ideal watermarking technique should be resilient to any such attacks. However, many times watermarked resources are unable to withstand such attacks. For instance, strong lossy compressions make watermark extraction almost impossible. Superior watermarking scheme with greater robustness to varied set of attacks is an issue to be tackled.

Two rather simple form of attack is cropping and watermark removal attempts by estimating the original image. Another kind of intentional attack to remove the watermark is by procuring many copies of differently watermarked images by an attacker and averaging all copies such action can eventually erase the traces of embedded watermark. [22] classifies the attacks into four namely, active attacks, passive attacks, collusion attack and forgery attack. The most common set of attacks as discussed in majority of the published papers are noise addition, compression and cropping [19, 23, 24].

The attacks on watermarked image are classified here into four as follows:

i. Noise Addition Attacks

Watermarked image is mixed with noise with the intension of making the watermark indictable. Usually salt and pepper noise, Gaussian noise or speckle noise is mixed with the actual contents. Random pixels irrespective of their location are selected during this process to accommodate the added noise. In the due process, this has the effect of making the hidden watermark contents meaningless.

ii. Geometric Attacks

Watermarked images are subject to malicious actions as rotation, scaling, resizing or shearing. These actions desynchronize the hidden watermark information and thus making the watermark non-extractable. Rotation, Scaling and Translation, known as RST attack, pose a difficult challenge as the main objective of these attacks is to nullify the synchronization between watermark embedding and extraction.

iii. Format change Attacks

This attack alters the measure used to represent each pixel. Compression is attempted usually to reduce the physical size of the image. Secondly, the file format is changed to another. The format of the file may be translated to a different format of interest. During these operations the pixel intensity values get altered. The changes induced there by need not be proportional and may vary across both dimensions. This adversely affects watermark extraction.

iv. Signal Processing Attacks

During this category of attacks the watermarked image is subjected to operations as histogram equalization, contrast adjustment median filtering or averaging. Most of these operations are image enhancement kind of operations that rework the image to build a required effect. Filtering operations use a sub-mask to modify the elements in the image array. The side effect introduced there by rupture the embedded watermark.

Each the above described attack may be intentional or unintentional. The most desirable requirement of any watermarking scheme is, irrespective of the motive behind the attack the scheme should be able to deliver the results at the time of watermark extraction. The scheme is said to be robust and reliable only if a recognizable watermark is extracted from the attacked watermarked image.

8 CONCLUSIONS

Watermarking can viewed as a blend of different fields such as communications, cryptography and image processing. The use

of Watermarking does not ensure that our digital data is protected from being copied and edited. On contrary watermarking permits us to prove the copyright of the content owner and also helps to a great extent in detecting the authenticity and correctness of the data. Two essentials in digital watermarking are the watermark embedding process should not degrade the quality of the base image and at the same must also be robust to various image processing attacks. The most desirable feature of any water marking system is that they must be able to withstand attacks. The watermark should be retained in the image even after the watermarked image is subjected to repeated modifications or manipulations. Most of the proposed conventional watermarks in literature are easily broken on attacks or on multiple attacks. Development of a robust watermarking scheme resilient to mixed set of watermark removal attacks remains as the main issue to be solved fully.

REFERENCE

- [1] Vidyasagar M Potdar, Song Han, Elizabeth Chang," A Survey of Digital Image Watermarking Techniques ", IEEE International Conference on Industrial Informatics, 2005
- [2] Shiguo Lian, Dimitris Kanellopoulos, Giancarlo Ruffo, " Recent advances in Multimedia Information System Security", PP 3-24, Informatics 33, 2009
- [3] Latha Parameswaran, K Anbumani, "Content-Based Watermarking for Images Authentication Using Independent Component Analysis", Informatica 32(2008) pp299-306.
- [4] S.S Bedi, Rakesh Ahuja, Himanshu Agarwal, Copyright Protection using Video Watermarking based on Wavelet Transformation in Multiband, International Journal of Computer Applications, March 2013.
- [5] Shumei Wang, Wenbao Hou," A Robust Watermarking Algorithm based on Histogram", Proceedings of IWISA 2009.
- [6] Soo-Chang Pei, Y Zeng.: Hiding Multiple Data in Color Images by Histogram Modification, Proceedings of 17th International Conference on Pattern Recognition (2004)
- [7] Zhicheng Ni, Yun-Quing Shi, Nirwan Ansari, Wei Su.: Reversible Data Hiding, IEEE Transactions on Circuits and Systems for Video Technology Vol16, (2006)
- [8] Shumei Wang, Wenbao Hou.: A Robust Watermarking Algorithm based on Histogram, Proceedings of IWISA (2009).
- [9] Baisa L Gunjal, R. R Manthalkar.: An overview of transform domain robust digital image watermarking Algorithms, Journal of Emerging trends in Computing and Information Science, Vol2 No.1, pp. 37- 42, (2010)
- [10] Neminath Hubballi, Kanyakumari D P," Novel DCT based Watermarking scheme for Images", International Journal of Recent Trends in Engineering., 2009, pp.430-433
- [11] Neminath Hubballi, Kanyakumari D P, Novel DCT based Watermarking scheme for Images, International Journal of Recent Trends in Engineering, Vol1, No.1, May 2009
- [12] Vikas Saxena, J.P Gupta, "A Novel Watermarking Scheme for JPEG Images", WSEAS Transaction on Signal Processing, 5(2), pp-74-83, 2009.
- [13] Tribhuvan Kumari, Vikas Saxena.: An Improved Robust DCT based Digital Image Watermarking Scheme, International Journal of Computer Applications, Vol3, (2010)
- [14] P. Meenakshi Devi , M. Venkatesan and K. Duraiswamy, "A Fragile Watermarking scheme for Image Authentication with Tamper Localization Using Integer Wavelet transform" , Journal of Computer Science 5(11) PP831-837, 2009.
- [15] Qing Liu and Jun Ying, "Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis", IEEE Symposium on Electrical & Electronics Engineering, 2012.
- [16] Nagaraj V Dharwadkar and B.B Amberker, "An efficient Non-blind Watermarking Scheme for Color Images using DWT", International Journal of Computer Applications, 2010.
- [17] Himeur Yassine, Boudraa Bachir, Khelalef Aziz, A Secure and High Robust Audio Watermarking System for Copyright Protection, International Journal of Computer Applications, Vol.53(17), 2012.
- [18] Ding Hai Yang, Zohu Ya Jain, Yang Yi-xian, Zhang Ru, Robust Blind Watermarking Algorithm in Transform Domain combining with 3D Video Correlation, Journal of Multimedia, Vol8(2), 2013.
- [19] Ali Al Haj.: Combined DWT-DCT Digital Image Watermarking, Journal of Computer Science, 3(9) pp.740-746, (2007)
- [20] S .Manikandan Prabu, Dr.S Ayyasamy, An Efficient Watermarking Algorithm Based on DWT and FFT Approach, International Journal on Computer Science and Engineering 2014, 6(6), 211-216.
- [21] Keqiang Ren and Huihuan Li, " Large Capacity Digital Audio Watermarking Algorithm Based on DWT and DCT" , IEEE International Conference on Mechatronic Science, Electric Engineering and Computer, China, pp-1765-1768, 2011.
- [22] Preeti Gupta, Cryptography based digital image watermarking algorithm to increase security of watermark data, International Journal of Scientific & Engineering Research, Vol.3(9), 2012.
- [23] Baisa l Gunjal, .R Manthalkar, An Overview of Tranform Domain Robust Digital Image Watermarking Algorithms, Journal of Emerging Trends in Computing and Information Science, 2010.
- [24] Yanwei Yu, Hefei Ling, Fuhao Zou, Zhending Lu, Liyun Wang, Robust Localized Image Watermarking based on Invariant Regions, Digital Signal Processing, pp170-180, 2012.