Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Digital Watermarking Methodologies - A Survey

Ekta Miglani[*]
M.Tech Scholar, ECE Department
SRM, Haryana, India
ekta_miglani2000@yahoo.com

Sachin Gupta
HOD, ECE Department
SRM, Haryana, India
sachinguptasrm@gmail.com

***Abstract*— Today, in the market, the protection of copyrighted material has become a new challenge, as the importance of the internet is increasing day by day in information acquisition. For protection of copyright material watermarking is introduced. Digital Watermarking is the process to authenticate user files by embedding and hiding digital code behind an image, text, audio and video file. For examples copyright symbols, signature or even images are used. This paper categorizes the various watermarking techniques along with the comparison that can help to know which one technique is more robust and better than others.**

***Keywords*— Digital Watermarking, Frequency Domain, spatial Domain, DFT, DCT, DWT**

I. Introduction

The usage of internet has been enormously achieved heights recently in multimedia technology. As the usage of internet is increasing the insecurity of copyright protection, modification and distribution of digital data is also leading. A large amount of data is pirated, edited and distributed without the knowledge of owner [1]. Economic losses occur each year due to movie and music industry respectively through digital piracy. So, the need of digital watermarking is growing day by day as the watermarking applications use against digital piracy. Hence, for multimedia data the copyright protection has become the main focus of the owner. Digital watermarking Technology is the significant and urgent component for protecting the copyright protection. Nowadays, video based applications are video conferencing, video broadcasting, set top box, wireless videos, videophone, video on demand and multimedia internet are becoming more and more popular and increasing the demand for secure videos distribution. The conception of watermarks derived the term 'watermark' and it is used to prevent the fake currency notes. The embedding information such as signature of the owner, status, recipient etc. embedded into the host data in such a way that it should not be transparent or removable even after many false, invalid or sensitive attempts and remains irremovable or undetectable [2]. The research is done in the field of digital watermarking is to protect and track illegal copy, transmission of digital products and to provide the copyright protection.

II. Digital Watermarking

A watermark is a form of image or text that is applied on paper, on still image and also on running video which provide the confirmation and verification of its authenticity. In the digital world, the digital watermarking is the protraction of this concept. The astounding extension of the internet in recent years has been prominent the demand for the system or technique to preserve the ownership of digital media. A mechanism of digital watermarking that issues a solution to the longstanding problems experienced with copyrighting digital data [3].

The main concept in watermarking is first take the host image then add a watermark signal into it and the watermark signal should not be conspicuous and insecure in the signal fusion. It can be easily extracted from the signal fusion later on if the secret key is used for recovery.

There are three important classes in the design of a watermarking system.

- Firstly, implement the watermark signal W which is to be added in host signal. The watermark signal W depends upon a secret key K and watermark information I.

$$W = f_0(I, K) \tag{1}$$

Perhaps, watermark signal W may also depend on host data X into which it is embedded.

$$W = f_0(I, K, X) \tag{2}$$

- Secondly, implementation of watermarked data Y that depends upon the host data X or the watermark signal W.

$$Y = f_1(X, W) \tag{3}$$

- Finally, Implement the extracted information i.e. I from the signal fusion using the secret key. With the help of the original signal or host signal.

$$\check{I} = g(X, Y, K)$$

(4)

Without the original signal

$$\ddot{I} = g(Y, K) \qquad (5)$$

The first two classes show the implementation of watermark signal W and Watermark embedding signal Y, are many times considered as one, especially for methods where the embedded watermark is flexible.

Fig. 1 and Fig. 2 illustrate the basic concept. Fig. 2 shows the common digital watermarking method for the embedding process. The L.H.S. of the fig. shows the Watermark, data and secret/public key that is the input to the system and R.H.S. of the shows the watermarked data that is the output to the system.

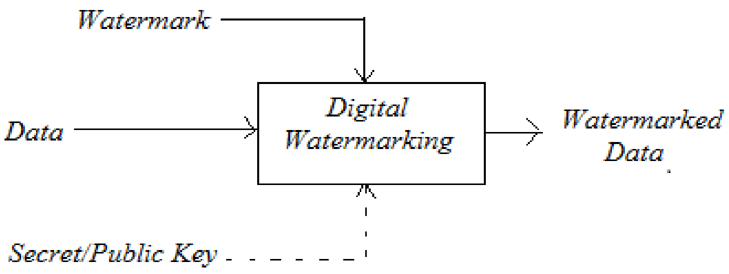


Fig. 1 Common digital watermarking method

The host data may be compressed or uncompressed depending on the application. Most present methods work on uncompressed. Another input is the watermark, may be a number, text or an image. Next input is secret/public key used for authentication. It means watermark cannot be read by the unauthorized person. This secret key is used to prevent the watermark. When the secret key is preferred then it is referred to as secret watermarking techniques otherwise public watermarking techniques, respectively [4]. The outputs of the watermarking method are modified, i.e. watermarked data.

The common watermarking recovery method is shown in Fig. 2. This process consists the three inputs i.e. watermarked and/or original image, secret or public key and the text data.

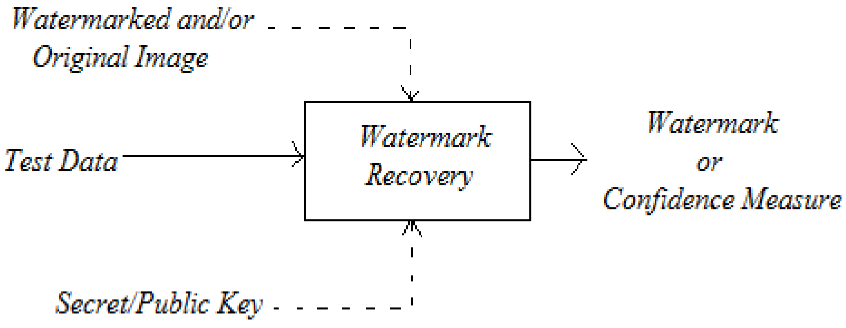

Watermarked and/or Original Image
Test Data
Watermark Recovery
Watermark or Confidence Measure
Secret/Public Key

Fig. 2 Common watermarking recovery method

The output of the this process is either the recovered watermark or some class of confidence measure shows how accurately it is for the watermark at the input to be presented in the data under inspection.

III. Applications Of Digital Watermarking

There are various applications where watermarking can be used. Some of them listed below.

A. *Ownership Declaration*

To declare the ownership over the content by watermarking used the term ownership declaration. An invisible watermark is more secure for this application.

B. *Authentication and integrity verification*

To maintain the integrity of the content used the term integrity verification. This is protected by the secure key. That must be placed at the time of embedding and this verification key should not be approachable without authentication.

C. *Usage Control*

To limit the no. of copyright material by allowing the owner to set usage restrictions using watermark.

D. *Content Labeling*

Embedded bits into the data such as labeling or captioning give extra information [3].

IV. Types Of Digital Watermarking

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked [5]. As illustrated in Fig. 3.

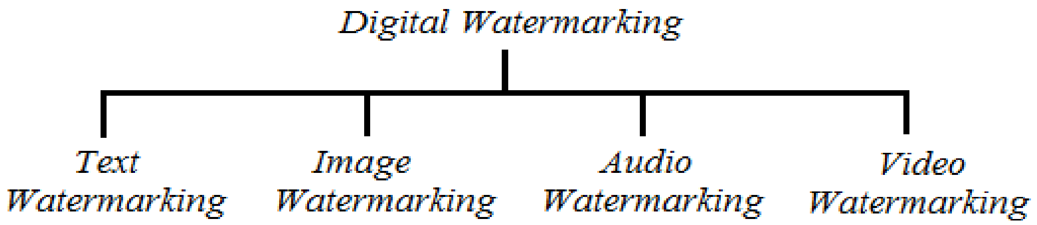


Fig. 3 Types of digital watermarking

A. Text Watermarking

In the text watermarking, watermark is used to operate as a watermark text image. It can be visible or non visible. It can be applied in the layout and background of appearances of the images [6].

B. Image Watermarking

In the image watermarking, watermark is inserted invisibly in the host image so that watermark can be extracted later for the proof of rightful ownership [7].

C. Audio Watermarking

In audio water*marking, additional signal is embedded as a water*mark into the audio signal [8].

D. Video Watermarking

In the video watermarking, first the host video is divided into video shots. Then from each video shot one video frame is selected that is known as identical frame. It is used for watermark embedding [9].

In other way, the digital watermark can be divided into three different ways which are discussed as:

A. Visible Watermark

This watermark signal is different from actual or original signal. This is a semi transparent text or image that overspread into the image. In this, watermark is visible to a viewer.

B. Invisible Robust Watermark

In this type of invisible watermarking, the watermark can be in any form, e.g. image, text or signature is invisibly inserted in most symbolic area of the host image and can be extracted by an authenticated person who knows the appropriate decoding algorithm.

C. Invisible Fragile Watermark

In invisible fragile watermarking, the watermark is inserted in the host image in a way that any change in the image would destroy the watermark because it is very sensitive to attacks [10].

V. PROPERTIES OF DIGITAL WATERMARKING

A. Robustness

Robustness defines how much the noise or attack is tolerable in the system. Watermark should be more robust. It means it is impossible to remove the watermark from the watermarked video or image. It can be but with the sufficient knowledge of embedding process [11].

B. Security

Authentication of Watermark should be exceptionally well so that no unauthorized party could detect the watermark even after recognizing the exact embedding and extraction algorithms [2].

C. Unambiguous

The Copyright owner of the content should be distinctively identified by the retrieved watermark, or in case of fingerprinting applications, the authorized recipient of the content should be specifically recognized [1].

D. Imperceptibility

Imperceptibility means impossible or difficult to perceive by the mind or senses. The watermark embedded into the digital video sequence should be indiscernible to Human Vision System (HVS) [11].

E. Irremovable

It must be difficult or impossible for a hacker to remove the watermark without perceptibly demeaning the original signal. Detection of watermark by comparing several watermarked signals belonging to the same author should be impossible for a pirate.

F. Computational Cost

Different applications entail the detection to work and embedding at different speeds. Embedding and detection ought to work in real time in broadcast monitoring, thus they have to be rather fast and be supposed to have low computational complexity [2].

G. Loyalty

A watermark is considered to be having a high reliability if it is difficult for a viewer to recognize the degradation caused by it [11].

H. Fidelity

A watermark is considered to be having high fidelity if it is difficult for a viewer to recognize the degradation it causes. Though, the watermark needs to be imperceptible only at the time that the media is viewed [2].

I. Constant Bit Rate(CBR)

Watermarking should not increase the bit rate in the bit stream domain [11].

VI. Attacks On Digital Watermarking

The basic categorization of attacks on watermarks is as under:

A. Simple Attacks

In such attacks, attempts are made to damage the embedded watermark by making modifications in whole image without trying to identify and isolate the watermark. These attacks include addition of noise, D/A conversion, cropping, correction and frequency based compression [1].

B. Detection Disabling Attacks

In these attacks, attempts are made to shatter the correlation and to make it impossible for the watermark detector to recover the watermark, generally by geometrical distortions like rotation, shearing, cropping, zooming, scaling, and shifting in spatial or temporal direction and removal or insertion of pixels clusters [2]. The watermark can still be recovered with increased aptitude of the watermark detector as it remains in the attacked data.

C. Ambiguity Attacks

In such attacks, attempts are made to confuse the detector by producing fake watermarked data or fake original data.

D. Removal Attacks

In such attacks, attempts are made to analyse the watermarked data, thereafter estimating the watermark or the host data. Afterwards the watermark is separated from the watermarked data to discard it evenly over the object in order to degrade the watermark to make it undetectable/unreadable.

Various types of attacks are possible. These can be classified as under:

1) Subtractive Attacks: In such an attack, efforts are made to detect the presence, location of the watermark and to extract it. A subtractive attack is one where the cropped object has retained sufficient original content of great value.

2) Distortive Attacks: In such attacks, an inimical user applies some distortive transformation evenly over the object in order to degrade the watermark to make it undetectable or unreadable. In an effective distortive attack, watermark is no longer detected by anyone, but the value of the degraded data still has importance for the enemy.

3) Additive Attacks: In such attacks, a malicious user can supplement host by inserting his own watermark. In the additive attack, adversary's mark completely overrides original watermark and it is impossible to detect if there was any original mark prior to the adversary's mark.

4) Filtering and Cropping: Low-pass filtering does not affect considerable degradation in watermarked images, videos or audio, but can significantly affect the performance as spread-spectrum-like watermarks have non negligible high-frequency spectral contents.

5) Compression: Such types of attacks are generally unintentional and very common in multimedia applications. The data distributed via Internet is sometimes compressed. It is generally advisable to perform the watermark insertion in the same domain where the compression takes place to enable the watermark to resist different levels of compression. For instance, DWT domain image watermarking is more robust to JPEG compression than spatial domain watermarking.

6) Rotation and Scaling: Rotation and scaling is quite successful with still images. When rotation or scaling is performed, detection based on correlation and extraction fails as the embedded watermark and the locally generated version do not share the same spatial pattern anymore [2].

7) Statistical Averaging: In such an attack, an adversary may try to estimate the watermark and then 'unwatermark' the object by subtracting the estimate. It can be hazardous if the watermark does not depend on the data. With different objects that are watermarked, it would be feasible to improve the estimate by simple averaging.

8) Multiple Watermarking: In such an attack, an already watermarked object is watermarked by an adversary who may later stake claims of ownership. Time stamping the concealed information by a certification authority is the right solution.

9) Collusion Attacks: In these attacks, several copies of one piece of media are used by a hacker. Each copy is used with a different watermark to create a copy with no watermark [2].

10) Forgery Attacks: In forgery attack, the hacker attempts to embed a new watermark that is legitimate except removing it.

VII. Different Techniques Of Digital Watermarking

The Digital watermarking techniques are categorized into two dissimilar domains: pixel domain or spatial domain and transform domain or frequency domain.

A. Spatial Domain

In this technique, watermark is embedded by directly amending the pixel values of the host image/video. The foremost advantages of pixel based methods are that they are conceptually simple having very low computational intricacies. These methods are, therefore, commonly used in video watermarking where the prime concern is real-time performance [1]. The resulting watermark may or may not be perceptible, depending upon the intensity value. For example picture cropping, commonly used by image editors, can be used to remove the watermark [12].

Some methods of watermarking in spatial domains are:

1) *Correlation based Techniques:* In this technique, the watermark W(x, y) is added to the original content O(x, y) according to the equation (5).

$$O_w(x, y) = O(x, y) + kW(x, y) \tag{5}$$

In equation (5), k is a gain factor and O_w is the watermarked content. As we increase the value of k, it will expense the quality of watermarked contents.

2) *Least Significant Bit Modification (LSB):* Least Significant Bit modification (LSB) is the simplest technique of this domain. In this method, the watermark is just embedded into the least significant bits of the original video or flips the LSB. Though it is the most popular scheme due to its simplicity, but has some limitations like incompetence in dealing with a range of attacks, poor quality of the produced video, least robustness and lack of imperceptibility [11].

B. Frequency Domain

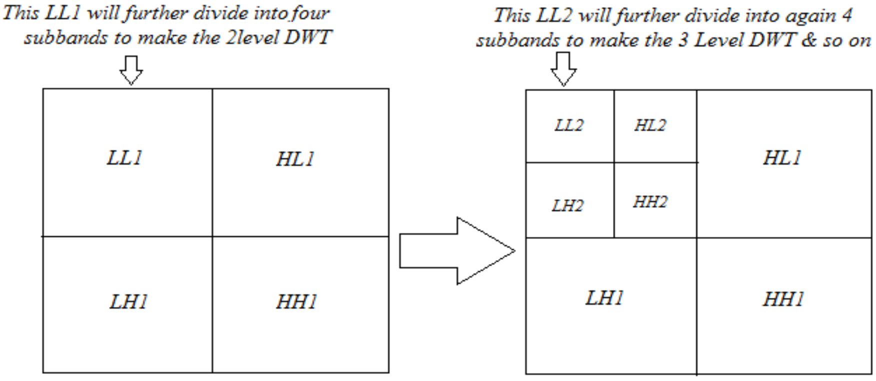
In such techniques, embedding of watermark is done by altering the transform coefficients of the frames of the video sequence. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) are the most commonly used transforms. The watermark is embedded evenly in overall domain of an original data. Initially, the host image/video is converted into frequency domain by transformation techniques. Thereafter, the transformed domain coefficients are changed to store the watermark information. Ultimately, the watermarked image/video is obtained by applying the inverse transform. Due to its multi resolution characteristics, a number of researches concentrated on using DWT [1]. It provides both spatial and frequency domain characteristics thus making it compatible with the Human Visual System (HVS). Furthermore, DWT can be combined with other algorithms to enhance robustness and invisibility. The transforms that comes under frequency domain are as follows:

1) *Discrete Fourier Transform (DFT):* Fourier Transform (FT) is a process which transforms a continuous function into its frequency components. The corresponding transform requires the Discrete Fourier Transform (DFT) for discrete valued function. In digital image processing, the even functions that are non periodic can be defined as the integral of sine and/or cosine multiplied by a weighing function. This weighing function formulates the coefficients of the Fourier transform of the signal. Fourier Transform grants examine and processing of the signal in its frequency domain by means of analysing and modifying these coefficients. DCT having two parts of watermarking, one is a template which does not include any information in itself but is able to detect any transformations undergone by the image, and another one is a spread spectrum message containing hidden information. The length of the hidden information is assumed to be short and it is deal with the pre-processing algorithm to construct the new message of length. The luminance component of the cover image is extracted and is used to calculate the DFT coefficients prior to embedding the hidden message. Thereafter, the hidden data and the template are embedded in these coefficients [13]. The template is embedded along two lines in the cover image which go through the origin. The idea is to detect any attacks/transformation the image has undergone.

2) *Discrete Cosine Transform (DCT):* DCT is vastly used method in image watermarking and provides accurate result. DCT is faster and can be implemented in O (n log n) operations. In Discrete Cosine Transform, images get decomposed into different frequency bands, and we mainly focused on middle frequency band. In this, watermark information is easily embedded into the middle frequency band. The middle frequency bands are chosen to avoid the most visual important parts of the image which are of low frequency without revealing themselves to elimination through compression and noise attacks. DCT is important method for video processing. It also gives accurate result in video watermarking and resists various attacks. Another advantage of DCT is that it breaks a video frame is into different frequency band which enables it to easily embed watermarking information into the middle frequency bands of a video frame [14]. DCT not only improves the peak signal to noise ratio but is also more robust against various attacks like frame dropping and frame averaging.

3) *Discrete wavelet Transform (DWT)*

Discrete wavelet transform (DWT) is based on small waves, called wavelets. It is a mathematical tool for hierarchically decomposing an image. Non stationary signals can be processed by DWT. Both frequency and spatial description of an image provided by the wavelet transform. Temporal information is retained in this transformation process unlike conventional Fourier transform translations and dilations of a fixed function created the wavelets called mother wavelet. This section analyse the suitability of DWT for image watermarking and represent the advantages of using DWT as against other transform. Apply DWT corresponds to processing the image for 2D images by 2D filters in each dimension. Input image is divided by the filters into four non overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub- band LL1 is different from other sub-bands in terms of scale [15].



This LL1 will further divide into four subbands to make the 2level DWT
This LL2 will further divide into again 4 subbands to make the 3 Level DWT & so on
LL1
HL1
LH1
HH1
LL2
HL2
LH2
HH2
HL1
LH1
HH1

Fig. 4 Single level DWT and second level decomposition

The LL1 represents the Coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the final scale of DWT coefficients. As illustrated in Fig. 4, for obtaining the next coarse scale of DWT coefficients, the sub-band LL1 is further processed until some final scale N is reached. When N is reached will have 3N+1 sub-bands consisting of multi-resolution sub-bands LL_N, LH_X, HL_X and HH_X where X ranges from 1 until N. DWT is appropriate transform to identify the areas in the host image where a watermark can be embedded effectively. Most of the image energy is determined at the lower frequency sub-bands LL_X and therefore embedded watermarks in these sub-bands degrade the image considerably. Robustness increase significantly when watermark is embedded in low frequency sub-bands [15]. On the other hand, the high frequency sub bands HH_X include the edges and textures of the image. The human eye is not very sensitive to predict the changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye.

VIII. Comparison Between DCT, DFT And DWT

In this section survey is done on different techniques and the result is DWT is more robust than other Techniques. Following reasons are mentioned here:

- An image can be shown at different levels of resolution and can be perform a series from low resolution to high resolution because of the feature of wavelet coded image that is a multi-resolution description of image. The advantage of such approach is that if the features of an image might be undetected at one resolution that may be easily recognized at another resolution.
- Wavelet coded images introduced visual artefacts that are less noticeable compared to DCT because wavelet transform decompose image into blocks for processing. Blocking artefacts are evident in DCT at high compression ratios as against wavelet transformed images [15].
- DWT has special frequency locality whereas DFT and DCT are full frame transform. Hence, any change in the transform coefficients affect entire image in DFT and DCT. Except block based approach is applied on DCT. In DWT, it will image locally not the entire image.
- DWT method is more robust than the DCT and DFT. Wavelet transform can accurately model human visual system (HVS) than other transforms. This allows higher energy watermarks in that region where HVS is less sensitive. This further allows in the system to increase the robustness of the watermark.
- Latest image compression standard JPEG 2000 is based on wavelet transform. This is the other advantage of DWT when compare with DCT and DFT.

IX. Conclusions

There are many techniques to hide the data and copyright protection. From the survey, it is found that the digital watermarking is m ore intelligible and easier method for data hiding. Also this is more robust and more capable because of its efficiency than the other hiding techniques. Watermarking is focused on security by secret key applied in the method. The demand of security is increasing day by day because of cyber crime. It provides security not only for images but also for video, text and audio. Secure watermarking is an easy and efficient way of digital data.

Acknowledgment

The authors are greatly indebted to the Management of the Shree Ram Mulakh Institute of Engineering and Technology. The authors would further like to thank the Electronics department for giving us so much support and encouragement in every aspect. Last but not the least the authors are greatly indebted to their families for always encouraging them to attain their goal.

References

[1] A. A. Hood and Prof. N. J. Janwe, “Robust Video Watermarking Techniques and Attacks on Watermark – A Review”, *International Journal of Computer Trends and Technology*, vol. 4, Issue No. 1, pp. 30-34, 2013.

[2] A. Devasia, A. Menoth, S. Monis and M. George, “A Survey on Watermarking of Images Using Hybrid Techniques”, *International Technological Conference-2014 (I-TechCON)*, pp. 187-192, Jan. 03 – 04, 2014.

[3] G. Kaur and K. Kaur, “Digital Watermarking and Other Data Hiding Techniques”, *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* ISSN: 2278-3075, Vol. 2, Issue No. 5, pp. 181-183, April 2013.

[4] F. Hartung and M. Kutter, “Multimedia Watermarking Techniques”, *Proceedings of the IEEE*, Vol. 87, No. 7, pp. 1079-1107, July 1999.

[5] H. Berghel, “Watermarking Cyberspace”, *Comm. of the ACM*, Nov.1997, Vol. 40, No. 11, pp.19-24, Nov. 1997.

[6] Y. W. Kim, K. Ae. Moon and Il-S. Oh, “A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics”, *IEEE Proceedings of the Seventh International Conference on Document Analysis and Recognition*, (ICDAR 2003), ISBN: 0-7695-1960-1/03, pp. 775-779, 2003.

[7] Y. S. Singh, B. P. Devi, and Kh. M. Singh, “A Review of Different Techniques on Digital Image Watermarking Scheme”, *International Journal of Engineering Research,* ISSN : 2319-6890, Vol. 2, Issue No. 3, pp. 193-199, 01 July 2013.

[8] M. A. T. Alsalami and M. M. Al-Akaidi, “Digital Audio Watermarking: Survey”, *Proceedings 17th European Simulation Multiconference,* SCS Europe BVBA, pp. 543-556, 2003.

[9] T. Tabassum and S.M.M. Islam, "A Digital Video Watermarking Technique Based on Identical Frame Extraction in 3-Level DWT", *Proceedings of IEEE 15th International Conference on Computer and Information Technology, Chittagong,* pp. 101-106, 2012.

[10] G. W. Braudaway, et al., "Protecting Publicly Available Images with a Visible Image Watermark", *Proceedings of SPIE Conference on Optical Security and Counterfeit Deterrence Technique*, Vol. SPIE- 2659, pp. 126-132, Feb. 1996.

[11] S. Patel, A. K. Katharotiya and M. Goyani, "A Survey on Digital Video Watermarking", *International Journal Comp. Tech. Appl.,* Vol. 2 (6), pp. 3015-3018, Nov. - Dec. 2011.

[12] C. Podilchuk and E. Delp, "Digital Watermarking Algorithms and Applications*", In IEEE Signal Processing Magazine*, vol. 18, Issue No. 4, pp. 34-46, July 2001.

[13] C. Song, S. Sudirman and M. Merabti, "Recent Advances and Classification of Watermarking Techniques in Digital Images", *Proceeding of 10th of Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet),* ISBN: 978-1-902560-22-9, June 2009.

[14] N. A. Shelke and Dr. P.N. Chatur, "A Survey on Various Digital Video Watermarking Schemes", *International Journal of Computer Science & Engineering Technology (IJCSET),* ISSN: 2229-3345, Vol. 4, Issue No. 12, pp. 1447-1454, Dec. 2013.

[15] N. Chaturvedi, "Various Digital Image Watermarking Techniques And Wavelet Transforms", *International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459, Vol. 2, Issue No. 5, pp. 363-366, May 2012.