



## A Review of Digital Water Marking Techniques and Uses

Abhigyakari, Neetesh Raghuvanshi and Anurag Rishishwar  
Department of Electronic and Communication Engineering,  
RKDF Bhopal, (MP), India

(Corresponding author: Abhigyakari)

(Received 03 September, 2015 Accepted 12 October, 2015)

(Published by Research Trend, Website: www.researchtrend.net)

**ABSTRACT:** Nowadays peoples are using extensive amount of digital in form of audio, video and images or even secret message in the digital images for value-added functionality and probably secret communication. So we need to protect our digital information and copyright info privacy. The watermarking is one of the methods of entrenched data into digital multimedia content. This is specifically used to authenticate the credibility of the content or to distinguish the identity of the digital content's vendor and protection of intellectual property rights (IPR). To provide security to our digital data various water marking techniques has been proposed and implemented. In this paper, we present the literature study of watermarking techniques with their advantages and disadvantages also discuss the different areas of application.

**Keywords:** Digital data, Watermarking, Techniques, Uses, IPR

### I. INTRODUCTION

Due to the widespread use of internet connections leads to the vibrant accessing of digital content. The computer networks are more susceptible to penetration and thus steal or transform digital data. For this reason it becomes the need to provide the security of digital data and the means is to protect the property rights of these data led to more interest in the improvement of novel methods for watermark signs. Watermarking is not a latest method. It is a descendent of a method known as steganography, which has been in subsistence for at least a few hundred years. Steganography is a technique for concealed communication. In contrast to cryptography where the content of a communicated message is secret, in steganography the very existence of the message is a surreptitious and solitary parties involved in the communication know its presence. Steganography is an approach where a secret message is hidden within an additional unrelated message and then communicated to the other party. Some of the techniques of steganography like use of invisible ink, pin puncture, word spacing patterns in a printed document, coding messages in music compositions, etc. have been used by military intelligence since the times of ancient Greek civilization. Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called the watermark and it depicts some metadata, like security or rights information about the main signal.

The main signal in which the watermark is embedded is referred to as the cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format. The information to be hidden (watermark, or in the general case of steganography, a secret message) embedded in a cover object (a cover CD, video or text), giving a stego object, which we may also call a marked object. The embedding is performed with the help of a key, a secret variable that is in general known to the object's owner. Recovery of the embedded watermark may or may not require a key. If it does, the key may be equal to or derived from the key used in the embedding process. For making our digital data secure or to maintain the integrity various watermarking techniques has been developed. In this paper, we present the literature survey of some of the watermarking techniques with their merits and demerits.

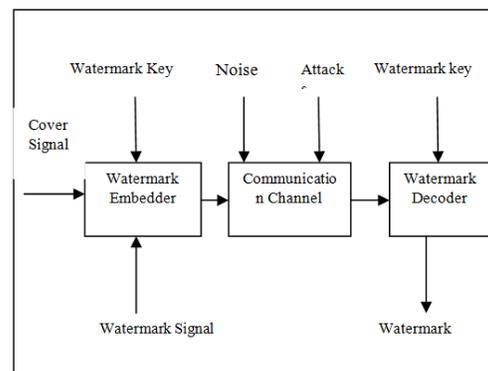


Fig. 1. Digital Watermarking System.

The arrangement of the rest section of the paper is done accordingly: In section II discusses about Watermarking, its classification and application. Section III presents explanation about the literature of the approaches presented by different researcher. Section IV outlines the different techniques of digital watermarking with their merits and demerits. Last section presents conclusion of the paper.

## II. DIGITAL WATERMARKING

The watermark embedding operation is actually the image content information change; there are addition and multiplication of two main kinds of commonly used modification rule [11]:

Additive criteria:

$$I_w(x, y) = I(x, y) + k'W(x, y) \quad (1)$$

Multiplication rule:

$$I_w(x, y) = I(x, y) * (1 + k * W(x, y)) \quad (2)$$

Among them,  $I(x, y)$  on behalf of the carrier image,  $I(x, y)$  on behalf of the watermarked image, the  $w(x, y)$  represents the watermark embedding strength factor, said  $k$ . Extraction of digital image watermarking, also need first to the carrier image, then under the control of the secret key, the watermark extraction algorithm to extract the watermark information is embedded procedure from extraction from the region.

### A. Classification of Digital Watermarking

The classification of watermarking can be on the basis of characteristics, attacked media and on the basis of its purpose which are explaining below:

#### **Watermarking classification on the basis of characteristic [12]:**

The key attribute of watermarking is robust and fragile. The robust watermarking is principally used to sign copyright information of the digital works, the embedded watermark can oppose the common edit processing, image processing, lossy compression and the watermark is not destroyed subsequent to some attack and can still be detected to offer certification. It opposes a variety of attacks, geometrical or non-geometrical exclusive of affecting embedded watermark. Whereas fragile is chiefly used for integrity protection, which must be very sensitive to the changes of signal. We can determine whether the data has been tampered according to the state of fragile watermarking.

#### **Watermarking classification on the basis of attached media [12]:**

The watermarking can also be performs by using digital media like image, audio, video and text etc. Firstly, Image watermarking is used to hide the special information into the image and to later detect and extract that special information for the author's ownership it maintaining the Integrity of the Specifications. Secondly, video watermarking includes watermark in the video stream to organize video applications. It is the extension of image watermarking. This process entails real time extraction and robustness for compression and audio watermarking application area is one of the most popular and hot issue due to internet music, MP3.

#### **Watermarking classification on the basis of purpose [12]:**

In this classification of watermarking on the basis of purpose it is also categorized accordingly namely; copyright protection, tampering tip, anti-counterfeit watermarking etc.

In copyright protection, if the owner desires others to perceive the mark of the image watermark, after that the watermark can be seen subsequent to adding the watermark to the image, and the watermark still exists even if it is attacked. The tampering tip shields the veracity of the image content, labels the modified content and resists the usual lossy compression formats and anti-counterfeit watermarking added to the building progression of the paper notes and can be identified later than printing, scanning, and further processes.

### B. Application of Digital Watermarking

(i) **Copyright protection:** The visible watermarking is used for copyright protection which is the most important digital watermarking application. The copyright protection requires high level of robustness so that the embedded watermark cannot be removed without data distortion. Then this watermark is extracted to show as proof if someone claims the ownership of the data [23].

(ii) **Finger Printing:** The finger printing is similar to giving serial number to any product. Every spreaded multimedia copy is embedded with a distinct watermark [23]. We can use the concept of fingerprinting to detect the true owner of digital content. Each consumer of digital content has its unique identity as fingerprint [24]

(iii) **Broadcast Monitoring:** This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not [25].

(iv) **Tamper Detection:** Fragile watermarks are used for tamper detection. If the watermark is degraded or destroyed, it indicates the presence of tampering and hence digital content cannot be trusted.

(v) **Authentication and Integrity Verification:** Content authentication is able to detect any change in digital content. Integrity verification can be achieved by using fragile or semi fragile watermark which has the low robustness to modification of an image [25].

(vi) **Content Description:** The watermark can contain some detailed information of the host image such as labeling and captioning. The capacity of watermarking for this kind of application should be relatively large and there is no strict requirement of robustness.

(vii) **Medical Applications:** Digital Image Watermarking can also be used in medical images to protect the patient information from unauthorized people. Protection and authentication of such images are now becoming increasingly very significant in the telemedicine field where images are easily distributed over the internet.

(viii) **Fingerprinting:** Fingerprints are unique to the owner of digital content and used to tell when an illegal copy appeared [25]. This can be achieved by tracing the whole transaction by embedding unique robust watermark for each recipient.

### III. RELATED WORK

Digital watermarking is widely used for protecting our digital data. Different researchers proposed various approaches for the security of information in which of these are explained. Shukla *et al.* "Enhancing security and integrity of data using watermarking and digital signature", [1] proposed as a novel method to compel ownership verification and defend data from tempering by unlawful user. To formulate digital watermarking more efficient digital signature or message authentication code is inserted in the complete message. This paper proposed a method using both Digital Watermarking and Signature so that data reliability can be confirmed at the receiver end of the network. Pradhan *et al.* "Enhanced digital watermarking scheme using fractal images in wavelets", [2] proposed a method to embed fractal images in discrete wavelet transform (DWT). The binary watermark image is engendered from fractal codes. The color cover image is divided into its grayscale equivalents. The grayscale counterparts of color image are used to embed the watermark image which is engendered from fractal codes in standard frequency blocks to defend the codes from attacker. Counterparts watermark images are embedded into grayscale equivalents disjointedly to enhance the robustness and security of the system. The consequence analysis showed that the robustness and imperceptibility of the algorithm. Bashardoost *et al.* "A novel approach to enhance robustness in digital image watermarking using multiple bit-planes of intermediate

significant bits", [3] introduced a new method to safeguard digital images' copyrights. For this reason, as ISB method was selected in relation to the approach in an endeavor overpower the concerns of robustness and imperceptibility in watermarked metaphors. According to the literature analysis, embedding the aimed surreptitious bits (Watermark) is a challenging concern inside a host image (ordinary 8-bit, grey-scale) in a sense to construct it imperceptible by the HVS (Human Visual System) in addition to the substance that it is predicted to accept any attacks. The recommended method here correspond to an improved method for the embedding of ISB which safeguards the robustness and cultivates the rate of sanctuary by employing repeated bits in different bit planes over an irregular order and it extends the LSB system exclusively in circumstances where robustness and imperceptibility are major concerns of assessment. Fadil *et al.* "Enhanced EPR data protection using cryptography & digital watermarking", [4] proposed a new system to embed electronic patient records (EPR) data in medical images. Definitely, later than liberating a region by compressing the image Least Significant Bit chart using the Huffman coding, the EPR is encrypted by an elliptic curve cryptosystem (ECC) and inserted into this zone. The proposed approach recovers medical security performance and lessens the computation cost associated to data encryption and decryption. Gotze *et al.* "Increased Robustness & Security of Digital Watermarking Using DS-CDMA", [5] presented a blind, robust and protected watermarking procedure based on DS-CDMA is presented. By using this method a watermark can be extracted at incredibly high PSNR value with extremely low BER. An adaptive system is used to choose the coefficients in the DCT domain, where the watermark is to conceal. This drastically diminishes BER. Numerous spreading codes can be used to make this system safe and more robust adjacent to JPEG compression, scaling and cropping. Patel, "Fusion of DWT and SVD digital watermarking Techniques for robustness", [6] adopted the usage of a mixed (hybrid) transformation to accomplish these objectives, The outlook behind applying a fusion transform or mixed transformation is that the cover image is personalized in its singular values rather than on the DWT sub-bands and also PSNR values of cooperation cover image and watermark can be transform, consequently the watermark makes it susceptible to vivid attacks and preserves its original state by checking the robustness. To maintain the methods and comparative study some simulation results were presented Jebaraj *et al.* "Secure data collection in clustered WSNs using digital signature", [7] scrutinized the predicament of adding security to cluster-based communication protocols for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources.

The proposed method guarantees data secrecy and the authentication among the nodes. The foremost benefit of the proposed system is the node detain attack does not influence the security of other nodes in the network. Malipatil et al. "Authentication watermarking for transmission of hidden data using biometrics technique", [8] suggested a novel method of defending concealed communication of biometrics using authentication watermarking. The proposed method uses watermark embedding algorithm. Evaluated with conventional personal identification methods such as passwords and personal identification number codes, automated biometrics authentication provides a well-situated and consistent method in different application but their legitimacy must be guaranteed. Watermarking technique presents solution to make certain the authority of biometrics; proposed method is composed of three divisions: watermark embedding, data embedding and data mining. One of the applications of their proposed method is authenticating data reliability for images transferred over the internet. Koutsouris, D. et al. "Digital Watermarking in Telemedicine Applications - Towards Enhanced Data Security & Accessibility", [9] suggested the utilization of watermarking in telemedical applications in order to augment safety of the transmitted susceptible medical data, disseminates the users with a telemedical system and a watermarking module that have previously been developed, and proposed an architecture that will facilitate the integration of the two systems, taking into account a multiplicity of use cases and application circumstances. Zanwar et al. "A Review on Digital Watermarking in Video for Secure Communication", [10] anticipated a fusion digital video watermarking method based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). SVD image watermarking scheme, in which the watermark is appended to the SVs of the whole image or to an apart of it. The video frames are primary decomposed using DWT and the binary watermark is embedded in the most important components of the low frequency wavelet coefficients. The indiscernible high bit rate watermark embedded is vigorous beside different attacks that can be carried out on the watermarked video, such as filtering, contrast amendment, noise addition and geometric attacks.

#### IV. DIGITAL WATERMARKING TECHNIQUES

To make our digital data like audio, video, images and text etc. secure various techniques has been developed. It is mainly classified into two: Spatial domain and frequency domain.

##### A. Spatial Domain

The spatial domain represents the image in the form of pixels.

The spatial domain watermarking embeds the watermark by modifying the intensity and the colour value of some selected pixels [12]. The strength of the spatial domain watermarking is simplicity, very low computational complexity and less time consuming. The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks. The spatial domain techniques can be easily applied to any image. The most important method of spatial domain is LSB.

**Least Significant Bit.** *The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image. Example of least significant bit watermarking [12]:*

Image:

10010101 00111011 11001101 01010101...

Watermark:

1 0 1 0.....

Watermarked Image:

10010101 00111010 11001101 01010100.....

The main advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not degrade. The main drawback of LSB technique is its poor robustness to common signal processing operations because by using this technique watermark can easily be destroyed by any signal processing attacks. It is not vulnerable to attacks and noise but it is very much imperceptible. The steps used to embed the watermark in the original image by using the LSB [13]:

- 1) Convert RGB image to grey scale image.
- 2) Make double precision for image.
- 3) Shift most significant bits to low significant bits of watermark image.
- 4) Make least significant bits of host image zero.
- 5) Add shifted version (step 3) of watermarked image to modified (step 4) host image.

But the spatial domain has some limitation: It is simple as compared to the transform domain watermarking. The robustness is the main limitation of the spatial domain watermarking. It can survive simple operations like cropping and addition of noise.

Another restriction of spatial domain method is that they do not permit for the successive processing in order to enhance the robustness of watermark.

##### Patchwork Algorithm

Patchwork is a data hiding method developed by Bender et Alii and published on IBM Systems Journal, 1996. It is related to a pseudo-random, statistical model. Patchwork indiscernibly inserts a watermark with a scrupulous statistic using a Gaussian distribution.

A pseudo randomly assortment of two patches is carried out where the former one is A and the second is B. Patch an image data is brighten up where as that of patch B is darkened (for reason of this graphic this is exaggerated). The following are the steps involved in the Patchwork algorithm [14]: -Create a pseudo-random bit stream to opt for pairs of pixels from the cover data. -For every pair, let  $d$  be the difference among the two pixels.

-Encode a bit of information into the couple. Let  $d < 0$  signify 0 and  $d > 0$  signify 1. Given that the pixels are not ordered properly, exchange them.

-In the incident that  $d$  is larger than a predefined threshold or if is equal to 0, disregard the pair and proceed to the subsequent pair. Patchwork being statistical methods utilizes redundant pattern encoding to insert message inside an image.

-Correlation-Based Technique: In this method, a pseudorandom noise (PN) pattern says  $W(x, y)$  is appending to cover image  $I(x, y)$ .

$$I_w(x, y) = I(x, y) + k'W(x, y)$$

Where  $K$  indicates the gain factor,  $I_w$  signify watermarked image ant position  $x, y$  and  $I$  signify cover image. Now, if we enhance the gain factor then even though it enhances the robustness of watermark but the excellence of the watermarked image will decrease.

**Correlation-Based Techniques [15]:** This method adds a pseudo random noise (PN) with a pattern  $W(x, y)$  to an image. At the decoder the correlation among the random noise and the image is found out and if the value exceeds a definite threshold value the watermark is detected else it is not. Equation for the above is given as:

$$I_w(x, y) = I(x, y) + K * w(x, y) \quad (3)$$

Where  $k$  stands for a gain factor, and  $I_w$  the resultant watermarked image,  $K$  is directly propositional to robustness, that is increasing  $K$  increases the robustness of the image but degrades the quality of image. The same pseudo random noise key is used for retrieving the watermarked image by computing the correlation between the noise pattern and the watermarking image. If the correlation goes beyond a convinced threshold ( $T$ ), the watermark is detected and a single bit is set. This method can simply be extended to multiple-bit watermark by dividing the image into blocks and performing the above process autonomously on each block.

**Predictive Coding Schemes image [15]:** Predictive coding scheme was proposed by Matsui and Tanaka in for gray scale 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.

**Spread Spectrum Watermarking:** Spread spectrum techniques are widely used in digital watermarking which is derived from the communication field. The basic idea of spread spectrum is to spread the data across a large frequency band. In the case of audio, it is the whole audible spectrum in the case of images; it is the whole visible spectrum. Spread spectrum is a military technology designed to handle interferences and disturbances. In most cases, signals that represent the information are modulated at low intensity diagonally the source bandwidth. Spread spectrum techniques used in communication for radar, navigation, and communication applications.

**Blind and Non-blind Techniques.** In order to distinguish the watermark information, blind and non blind procedures are used. If the revealing of the digital watermark can be done exclusive of the original data, such systems are called blind. At this point, the source article is scanned and the watermark information is extracted. In contrast, non blind methods use the original source to extort the watermark by simple comparison and correlation or interconnected procedures. On the other hand, it turns out that blind methods are more apprehensive than non blind methods [17].

**Texture mapping coding method.** In this method, a region of random texture pattern found in the image is copied to an area of the image with similar texture. Autocorrelation is then used to recover each texture region. The most significant problem with this scheme is that it is only appropriate for images that possess large areas of random texture. [18].

**Frequency Domain.** In Frequency Domain Watermarking, the watermark information is embedded in the transform domain. So this technique is also known as Transform Domain Watermarking. As discussed early, transformed domain watermarking schemes are more robust as compared to simple spatial domain watermarking schemes because information can be spread out to entire image. Though, they are complicated to implement and are computationally more luxurious. The most frequently used transforms are DCT, DFT, DWT and DHT. Each of these transforms has its own characteristics and symbolizes the image in unusual ways. In this paper they had discussed watermarking in frequency domain such as DFT, DCT, and DWT.

**Discrete Cosine Transform.** Discrete Cosine Transform (DCT) used for the signal processing. It transforms a signal from the spatial domain to the frequency domain. DCT is applied in many fields like data compression, pattern recognition and every field of image processing. DCT watermarking is more robust as compared to the spatial domain watermarking techniques. The main steps which used in DCT [19]:

- 1) Subdivision the image into non-overlapping blocks of 8x8.
- 2) Relate forward DCT to each of these blocks.
- 3) Apply some block selection criteria (e.g. HVS).
- 4) Apply coefficient selection criteria (e.g. highest).
- 5) Embedded watermark by modifying the selected Coefficient.
- 6) Apply inverse DCT transform on each block.

In DCT, for embedding the watermark information, we divide the image into different frequency bands. In Figure 4 FL denotes the lowest frequency component of the block, while FH denotes the higher frequency component and FM denotes the middle frequency component which is chosen as the embedding region. The Discrete cosine transform achieves good robustness against various signal processing attacks because of the selection of perceptually significant frequency domain coefficients.

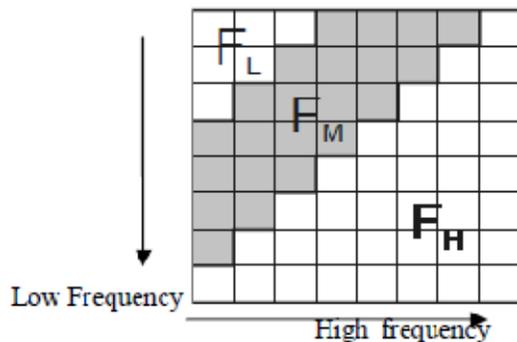


Fig. 2. Discrete Cosine Transform Region.

**Discrete Wavelet Transform.** The basic idea in the DWT for a one dimensional signal is the following. A signal is split into two parts, usually high frequencies and low frequencies. This splitting is called decomposition. [20, 21]

A step of wavelet transform decomposes an image into four parts: HH, HL, LH and LL in Figure. LL is low frequency coefficient, LH is high frequency coefficient horizontally, HL is high frequency coefficient vertically, and HH is high frequency coefficient

diagonally. Watermark should be embedded in low frequency coefficients.

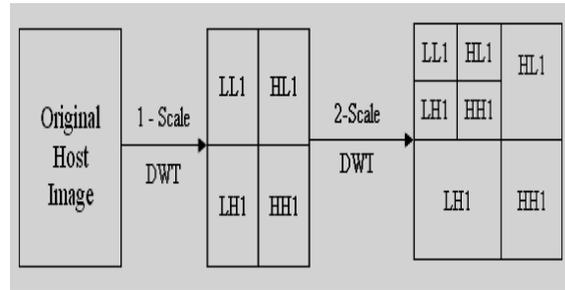


Fig. 3. Flow of DWT Process.

Furthermore, DWT image and video coding, such as embedded zero-tree wavelet (EZW) coding, are included in the upcoming image and video compression standards, such as JPEG2000. Thus DWT decomposition can be exploited to make a real-time watermark application. [21].

**Discrete Fourier Transform (DFT).** Transforms a unbroken function into its frequency components [22]. It makes available robustness alongside geometric attacks like scaling, cropping, rotation and translation etc. DFT of an original image is normally complex valued, which fallout in the magnitude and phase demonstration of an image. DFT demonstrates translation invariance. Spatial shifts in the image influences the phase representation of the image but not the magnitude demonstration, or circular shifts in the spatial domain don't persuade the magnitude of the Fourier transform. DFT is resistant to cropping because consequence of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, these are normalized coordinates, there is no synchronization are needed.

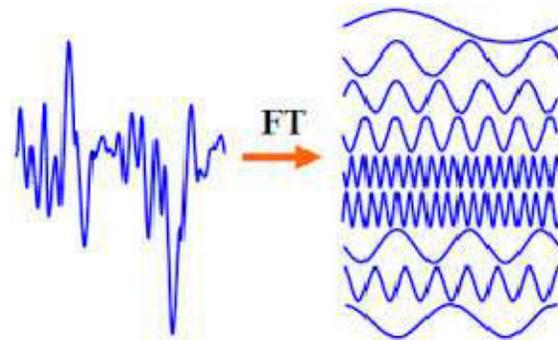


Fig. 4. The action of the Fourier Transform.

**Table 1: Digital watermarking approach merits and demerits.**

Techniques	Merits	Demerits
LSB	-It can be implemented easily - High perceptual Transparency	- Vulnerable to noise -Vulnerable to cropping, scaling
Patchwork Algo	Robustness is high	It is not able to hide large amount of information.
Correlation Based	Robustness increases due to increase in gain factor	Due to high gain factor quality of image degraded
Spread Spectrum	The computation cost is very and its storage capacity is also high	It is less robust and does not allow subsequent processing
DCT	The watermark is embedded into the coefficients of the nucleus frequency, consequently the visibility of image will not get affected and the watermark will not be detached by some kind of attack	Block wise DCT demolishes the invariance properties of the system. 2. Specific higher frequency components tend to be suppressed during the quantization process
DFT	DFT is rotation, scaling and translation (RST) invariant. Therefore it can be used to recover from geometric distortions	- Complex Implementation - Cost of computing may be higher.
DWT	- Consents to excellent localization both in time and spatial frequency domain - Higher compression ratio which is applicable to human observation	- Cost of computing may be higher. - Longer compression time. - Noise close to edges of images or video frames

## CONCLUSION

Digital watermarking is a technique to protect & make the digital more secure. In this paper, we provides the overview of watermarking with their classification, also discusses different watermarking approaches with their merits and demerits. We also discuss the area of application of digital watermarking. In this we try to discuss complete information of information hiding mechanism called watermarking with literature study. In future work, develop such technique which has less computation cost, less complex in design and provide much security to our digital data.

## REFERENCES

- [1]. Shukla, S.S.P. ; Singh, S.P. ; Shah, K. ; Kumar, A. "Enhancing security & integrity of data using watermarking & digital signature", Recent Advances in Information Technology (RAIT), 2012 1st International Conference on , 15-17 March 2012 Page(s):28 - 32 Print ISBN: 978-1-4577-0694-3, *In proceeding of IEEEExplore*.
- [2]. Arun, Kabi, K.K. ; Saha, B.J. ; Pradhan, C. "Enhanced digital watermarking scheme using fractal images in wavelets", *Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on 11-13 July 2014*, Page(s):1 - 6 Print ISBN:978-1-4799-2695-4.
- [3]. Sharifara A., Rahim, M.S.M. and Bashardoost, M. "A Novel Approach to Enhance Robustness in Digital Image Watermarking Using Multiple Bit-Planes of Intermediate Significant Bits", *Informatics and Creative Multimedia (ICICM), 2013 International Conference on 4-6 Sept. 2013. Published in IEEEExplore*, Page(s):22 – 27.
- [4]. Zaz, Y. ; FPO-Ibn Zohr Univ., Ouarzazate, Morocco ; Fadil, L.E. "Enhanced EPR data protection using cryptography and digital watermarking", *Multimedia Computing and Systems (ICMCS), 2011 International Conference on 7-9 April 2011, published in IEEEExplore*. Page(s):1 - Print ISBN: 978-1-61284-730-6.
- [5]. Samee, M.K. , Gotze, J. "Increased Robustness and Security of Digital Watermarking Using DS-CDMA", *Signal Processing and Information Technology, 2007 IEEE International Symposium on 15-18 Dec. 2007*, Page(s):185 - 189 E-ISBN :978-1-4244-1835-0.
- [6]. Jaishri Guru Hemant Dhamecha Brajesh Patel, "Fusion of DWT and SVD digital watermarking Techniques for robustness", *International Journal of Advanced Research in Computer Science and Software Engineering*. Volume 4, Issue 9, September 2014 ISSN: 2277 128X
- [7]. Seema, K.N., Jebaraj, S. "Secure data collection in clustered WSNs using digital signature", *Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference on 8-8 July 2014* Page(s): 543 - 546 Print ISBN: 978-1-4799-7986-8.
- [8]. Shubhangi D.C, Manikamma Malipatil, "Authentication Watermarking for Transmission of Hidden Data using Biometrics Technique", *International Journal of Emerging Technology and Advanced Engineering* ISSN 2250-2459, Volume 2, Issue 5, May 2012.
- [9]. Giakoumaki, A., Perakis, K. ; Tagaris, A. ; Koutsouris, D. "Digital Watermarking in Telemedicine Applications - Towards Enhanced Data Security and Accessibility", *Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE*, Aug. 30 2006-Sept. 3 2006 Page(s): 6328 - 6331 ISSN: 1557-170X.
- [10]. Mahesh S. Zanwar1 and S. V. Rode, "A Review on Digital Watermarking in Video for Secure Communication", *International Journal of Emerging Technology and Advanced Engineering* Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 12, December 2014).
- [11]. G. Sen Gupta, S.C. Mukhopadhyay, Michael Sutherland and Serge Demidenko, *Wireless Sensor Network for Selective Activity Monitoring in a home for the Elderly*, Proceedings of 2007 IEEE IMTC conference, Warsaw, Poland, (6 pages).
- [12]. N. Chandrakar and J. Baggaa, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", *International Journal of computer Application Technology and Research*, vol. 2, no. 2, (2013), pp. 126-130.
- [13]. D. Mistry, "Comparison of Digital Watermarking Methods" (*IJCSE*) *International Journal on Computer Science and Engineering*, vol. 02, no. 09, (2010), pp. 2805-2909.
- [14]. Prabhishek Singh, "A Survey of Digital Watermarking Techniques, Applications and Attacks", *International Journal of Engineering and Innovative Technology (IJEIT)* Volume 2, Issue 9, March 2013.
- [15]. S Sahar Afshan Andrabi, Sheenam "A Review: Information Hiding Using Watermarking Techniques", *SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – EFES* April 2015, ISSN: 2348 – 8387, Page 72-78.
- [16]. Jaishri Guru, Hemant Damecha, "Digital Watermarking Classification: A Survey", *International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014*, ISSN: 2347-8578. Page 8-13.
- [17]. Ensaf Hussein, Mohamed A. Belal, "Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey", *International Journal of Engineering Research & Technology (IJERT)*, Vol. 1 Issue 7, September – 2012, ISSN: 2278-0181
- [18]. Y. Zhang, "Digital Watermarking Technology: A Review", 2009 *ETP International conference on Future Computer and Communication*.
- [19]. V. M. Potdar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques", 2005 *3rd IEEE International Conference on Industrial Informatics (INDIN)*.
- [20]. V. Santhi, A. Thangavelu, "DC Coefficients based Watermarking Techniques for Color Images Using Singular Value Decomposition", *International Journal of Computer and Electrical Engineering*, Vol. 3, No.1, February 2011.

- [21]. B. Gunjal, R. Manthalkar, "An Overview of Transform Domain Robust Digital Image Watermarking Algorithms", *Journal of Emerging Trends in Computing and Information science*, Volume 2, No.1 2011.
- [22]. Jalpa M. Patel, "A brief survey on digital image watermarking techniques", *International Journal For Technological Research In Engineering* Volume 1, Issue 7, March-2014.
- [23]. Vipula Singh, "Digital Watermarking: A Tutorial", Geethanjali College of Engineering and Technology, Hyderabad India (2011).
- [24]. Anupma Yadav, Anju Yadav, "Comparison of SVD-Watermarking and LSB-Watermarking Techniques", *International Journal of Computer Science and Mobile Computing*, Vol. 3 Issue.5, May- 2014, pg. 495-499.
- [25]. Vaishali S. Jabade and Sachin R. Gengaje, "Literature Review of Wavelet Based Digital Image Watermarking Techniques". *International Journal of Computer Applications*, vol. 31, no. 1, pp. 28- 34, October 2011.