ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Survey of Digital Watermarking techniques for Data security

M.Hariharalakshmi[1], Dr.M.Sivajothi[2], Dr.M.Mohamed Sathik[3]

Assistant Professor, Dept. of Computer Science, Manomaniam Sundaranar University, Tirunelveli, Tamilnadu, India[1]

Associate Professor, Dept. of Computer Science, Manomaniam Sundaranar University, Tirunelveli, Tamil Nadu, India[2]

Associate Professor, Dept. of Computer Science, Manomaniam Sundaranar University, Tirunelveli, Tamil Nadu, India[3]

ABSTRACT: Digital watermarking is a technology being in progress to ensure and make easy data authentication, security and copyright protection of digital media. It became very important in various applications areas like video, audio, text, image etc., This paper incorporates the detail study of watermarking definition, concept in a detailed and the main contributions in this field such as categories of watermarking process. It starts with overview, applications, properties of watermarking, classifications, general model, approaches, various attacks and quality performance metric of watermarking.

KEYWORDS: Applications;Attacks;Audio;Quality Performance metric; Text; Video.

I. INTRODUCTION

Today Internet is the most popular priority of everyone. It is a very fast access, which transfers the data throughout the world in the form of text, audio, video or images. Internet uses data as personal or professional. So the data is protected to avoid access from unauthorized person. The unauthorized person access is copying the data from us and pretending it like created by others. We are the owner of the data but unknown persons to copy our data. In order to overcome we can use digital watermarking to secure our data from unauthorized access or copying data.

There are many methods like Cryptography, Watermarking and Steganography to transfer the data / image to the proposed user to destination without any alteration [1]. A key present in watermarking is the perceptual transparency. It refers to the details that the embedding of a signal should not be visible to humans and not affect the quality of the basic data [2]. The protection and enforcement of logical property accurately for digital media develop into an main issue [3]. In this work, we have explained the most common watermarking applications scenarios to illustrate that watermark techniques are in the eye of the storm of most of the Internet security and copyright problems. Then we summarize the most common and well known watermark methods giving readable description and explaining the advantages and we provide the description of many possible attacks against watermarks.

II.LITERATURE SURVEY

In [16] authors proposed to protect digital identity documents beside a Print Scan attack for a secured ID card confirmation system. The existing PS function enforces some alteration, such as geometric rotation & histogram distortion on the watermark position which may basis the loss of information. In [17] authors proposed a new way of classified watermark technique during image modelling called ‘alpha channel composition‘ uses gradual mask. Two images with flat mask and gradual mask are used to make watermark that modify gray values of pixel in the image. A process of watermark recovery by concern inverse transformation to the distorted images. The image is watermarked using the type of Dig marc’s Picture Mark watermarking filter that is obtainable with Adobe Photoshop and the image is distorted by related the Stir mark tool of affine transformation. In [18] authors proposed, a approach for validating the image using lossless watermarking is being planned that present high capacity host signal (information) and non-altered image by executing the elliptic curve cryptography and LSB method. The proposed LWM image authentication technique requires of four processing steps namely, i) information verification, ii) data embedding on image, iii)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

information and image healing, and iv) confirmation. These four stages are consecutively performed and thus obtained the watermarked and recovered images.

A.**Applications**

In the following, some existing application fields are explained together with the reference technologies, and case studies are presented, highlighting some of the most common real world situation. Most of the examples shown refers to the watermarking of digital images, but they are commonly applicable to other media, such as audio or video streams.

A. Copyright Protection:

The first application area to that watermarking is that the copyright protection of digital media. In the digital world it is possible for nearly anyone to duplicate or manipulate digital information while not loosing quality. This has allowed previously unseen copyright infringement problems. Digital watermarking provides an added layer of security to the content protection chain to discourage unauthorized use or duplication of content by embedding watermarks that establish original media and also the allowable uses of the content. In such a situation, devices scan the watermark throughout playback or copying of the content. If the watermark indicates that the employment is unauthorized, the playback or copying is prevented and informative message is also displayed.

Effective content protection helps content, communicate copyright possession and uses rights of their content, protect it against common threats of piracy together with television camera recording, peer -to- peer file sharing, repetition format conversion, encryption and different kinds of re-processing.

B. Content identification and management:

Digital watermarking allows effective content identification by providing a novel digital into all or any varieties of media content in an exceedingly means that persists with the content where it should travel. Digital watermarks are simply embedded into content without intrusive with the consumer's enjoyment of it. It is invisible to humans, however simply detected and understood by computers; networks and a large vary of common digital devices. The watermark will carry such data, equivalent to the owner identity, however it should be used or anything the owner desires to convey. It can also predefine actions, together with linking to websites or alternative consumer experiences. Content identification helps:

- Consumers to search out the content they are trying to find, learn a lot of regarding it, try it out, and find wherever and the way several to get it.
- Copyright owners, brands and distributors to locate and find out about however, once and wherever content is being consumed and determine the supply of leaks once confidential content unknowingly or purposely makes its approach onto the net.

C. Content filtering:

The data carried within the digital watermark is speedily cross related with different content or actions. On the one hand, a particular action or maybe piece of content is triggered upon identification of the watermark, permitting customer interactivity. For example, whereas observance of a scene during a picture, a particular decision to action may be triggered. Similarly a particular and targeted advertisement may be triggered. Rather than a commercial showing at regular times, the commercial may be triggered consistent with what content is being watched and at specific times inside the content.

D. Document and image security:

A unique digital watermark will be simply embedded into every copy of a confidential document as they are being created and distributed. The information contained within the watermark will include who are the recipients of every copy in order that any information that is unknowingly or purposely leaked out is definitely copied back to the source. In addition, companies will be network detectors and email filters to examine for digital watermarks within documents and pictures, providing notification if an attempt is created at uploading to the net or forwarding in email outside the company. Similarly, watermarked detectors will be enclosed in numerous printers, scanners and different

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

devices to examine for watermarks in confidential documents that somebody is making an attempt to copy. During this case the watermark will trigger an action, like a don't copy or scan.
Therefore, document and image security helps to:

- Establish each copy of a confidential document and/or image with a novel digital identity;
- Trace back to the supply of leaks if sensitive materials are distributed on purpose or inadvertently;
- Filter documents being uploaded to the online or forwarded in email to quickly determine confidential materials and stop distribution;
- Prevent the repetition of confidential documents on copiers and/or scanners.

II. PROPERTIES OF WATERMARKING

There are three main Properties of digital watermarking technique

A. *Translucency or Fidelity:*

The digital watermark should not affect the quality of the cover image after it is watermarked. Watermarking should not present visible alteration because if such distortions are presented it degrades the commercial value of the image.

B. *Robustness:*

Watermarks could be removed intentionally or accidentally by simple image processing operations such as contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against such different attacks.

C. *Capacity or Data Payload*:

This property represents to how much data should be embedded as a watermark to strongly encounter during extraction. Watermark should be able to take sufficient information to denote the distinctiveness of the image. Various applications have different payload requirements.

III. APPROACHES OF ROBUST WATERMARKS

There are various types of Approaches in watermarks, some of them are discussed in this survey. [10]

A. Noise Watermark:

Noise watermark is the most normally used type of robust watermark. For the basis of security and statistical invisible, it is confirmed that the watermark is most secure, if it is in the structure of Gaussian random sequence. To compute the comparison between original and extracted sequence, the correspondence value is used to indicate the similarity.

B. Logo Watermark:

Logo is another type of robust watermark. The logo is small image pattern in type of binary form. It can be company logo used in business applications. The characteristic of logo image is computed by human perception. That is, it is particular test of proving accuracy of the digital content.

C. Message Watermark:

Message watermark is covered of text. Message watermark has the advantage of easy to use in difference with noise-type watermark or logo watermark. However, the message watermark need bit error rate approaching to zero, because any bit error will produce main defect in the final result. In most cases it is essential that information with at least 64 bit (or 8 bit ASCII character) can be accepted by multimedia.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

CLASSIFICATIOIN OF DIGITAL WATERMARKING TECHNIQUES

Watermarking techniques can be classified based on some principle as shown in the below:-

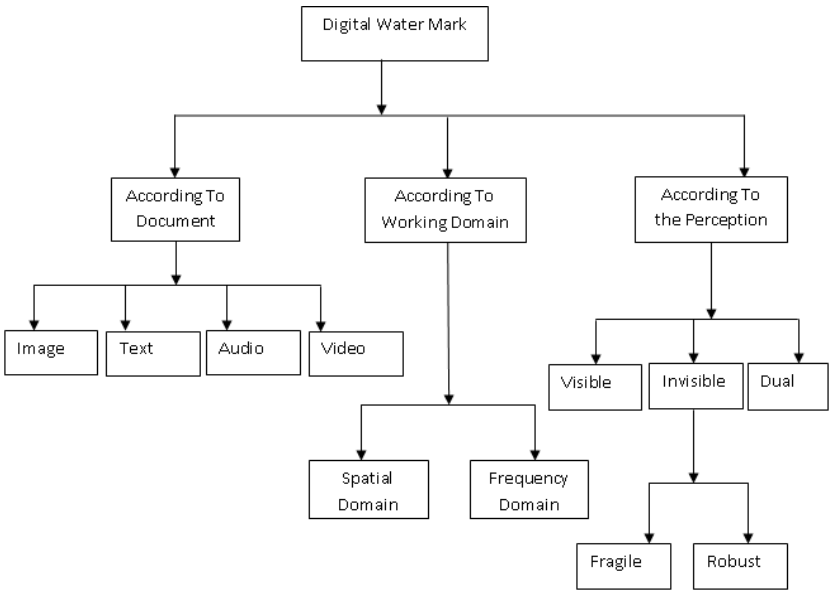

Fig 1: Classification of Digital Watermarking [5]

A. *According to Document:*

There are arranged into four categories [7]

- *Image watermarking:*

  This is used to conceal the particular information into the image and to identify and extract that particular information for the author's ownership.

- *Video watermarking:*

  This inserts watermark into the video stream to organize video applications. It is the expansion of image watermarking. This method forces actual time quality extraction and robustness for compression.

- *Audio watermarking:*

  This inserts watermark to the audio signals such as MP3 or internet music to embed and it is used to identify the copyright.

- *Text watermarking:*

  This includes watermark to the PDF, DOC and other text file to avoid the changes made to the text. The watermark is appended in the font shape and the space between characters and line spaces.

B. *According to working domain:*

- *Spatial domain:*
  - Initially watermarking schemes were presented in the spatial domain, where copyrighted information is added by changing pixel values of cover image. Least Significant Bit insertion is one of the models of this category. But such algorithms have low payload, they can be easily revealed and quality of image after embedding the copyright information and extracted watermark is not satisfied as pixel strengths are directly altered in these algorithms [10][11].
  - Patchwork is a data hiding technique, it is based on a pseudo random, statistical model. Patchwork imperceptibly includes a watermark with a specific statistic using a Gaussian distribution. A pseudo

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

randomly choice of two patches is passed out where the first one is A and the second is B. Patch A image data is make brighter where as that of patch B is darkened (for goal of this design this is magnified). Patchwork being statistical methods uses unwanted pattern encoding to include message within an image .

- *Frequency Domain :*

This technique is also called transform domain. Principles of particular frequencies are distorted from their host. There are some general transform domain methods used, such as DCT, DWT, and DFT.

The Discrete Cosine Transform:

One of the most usually transform domains for watermarking of quiet digital images is the Discrete Cosine Transform domain[6]. DCT denotes the entire image as coefficients of separate frequencies of cosines. The DCT of the image is computed by taking 8x8 blocks of the image, which are then distorted individually. The 2D DCT of an image provides the result matrix such that top left corner denotes lowest frequency coefficient while the bottom right corner is the highest frequency coefficient.

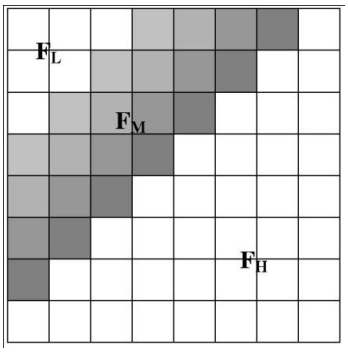

Fig 2: Various Frequency Bands

In above figure represents separate frequency bands of 8x8 block of DCT [4]. FM denotes the mid band frequencies of 8x8 block, FL represents lowest frequency components and FH denotes higher frequency components. Any of the bands can be used as embedding area. But if watermark is inserted to the FL band then it will produce more visual effect. If FH is taken as embedding band then it cannot holdup the image processing operations like compression. So only FM is preferred as the embedding region as to provide more challenge to lossy compression techniques, without doing significant variation in the concealed image.

Discrete Wavelet Transform:

Wavelet Transform is a recent technique commonly used in digital image processing, compression, watermarking etc. The wavelet transform provides the time-frequency description of a given signal. The transforms starts on small waves, called wavelet, of varying frequency and limited duration. The wavelet transform decomposes the image into three spatial orders such as horizontal, vertical and diagonal. Hence wavelets return the anisotropic properties of HVS more precisely.

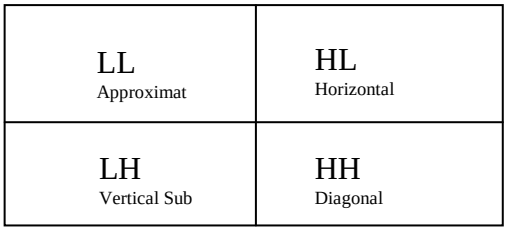

Fig 3 : One level Discrete Wavelet Transform – Decomposition [8]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is less significant for other bands (HH, LH, and HL)[5]. A 2D transform can be achieved by two separate one-dimensional transforms. First, the image is divided along the x-dimension using low pass and high pass analysis filters and reduced by two. Low pass filtered coefficients are collected on the left part of the matrix and high pass filtered coefficients are composed on the right. It is reduced the total size of the transformed image is same as the original image. Then, it is respected by filtering the sub-image beside the y-dimension and reduced by two. Finally, we have split the image into four bands represented by LL, HL, LH and HH as shown in above figure.

Discrete Fourier Transform:

Fourier Transform (FT) is a process that transforms a continuous event into its frequency components. The correspondent transform for discrete valued function requires the Discrete Fourier Transform (DFT). In digital image processing, the regular functions that are not periodic can be expressed as the basic of sine and/or cosine multiplied by a evaluating function. This weighing function construct up the coefficients of the Fourier Transform of the signal. It has robustness beside to geometric attacks like rotation, scaling, cropping, translation etc. DFT shows translation in variance. Spatial shifts in the image changes the phase submission of the image but not the significance representation, or circular shifts in the spatial domain don't concern the magnitude of the Fourier transform. Fourier Transform agrees to analysis and processing of the signal in its frequency domain by means of analyzing and transforming these coefficients.

C. *According to Human Perception:*

- *Visible watermarking:*

  Visible watermarking was the first and most fundamental way of watermarking. Visible watermarks are one, which are embedded in visual content in such a way that they are visible when the content is viewed. In this method the concealed object is taken and the watermark is added on it. This makes the watermark visible on the concealed object.

- *Invisible Watermarking:*

  In invisible watermarking, secret data is added as digital data to audio, picture or video but it cannot be identified. An invisible watermark is a concealed image, which cannot be seen, but which can be detected algorithmically. The watermark, generally a personal Identification Number, is digitally embedded within the image. While these watermarks can be defeated, they propose confirmation of your ownership if they always turn up in a publication without your authorization. Invisible watermark is used as verification of ownership and to detect misappropriated images. An invisible watermark is used as a backup for the visible watermark

- *Dual watermarking:*

  This technique is a pattern of visible and invisible watermark. It contains both visible and invisible watermark inside the conceal.

- *Robust Watermarking:*

  Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark. The term robust watermark describes those watermarks that can be detected within an object after significant levels of tampering of all kinds. The detection process of watermark can give just the probability of availability of watermark if the tampering level is too high. However, when an object is tampered with, it is automatically modified from the original, and in that sense its quality is degraded. This degradation can either be detected or not by the human sensors. Therefore, we can define some limits for the maximum required robustness of the embedded watermark. In robust watermarking applications, the extraction algorithm should be able to accurately produce the watermark, even if the modifications were strong.

- *Fragile Watermarking:*

  Fragile watermarking is a technique in which watermark gets damaged when watermarked content is modified or manipulated with. A watermark that potentially displays selective robustness, generally called fragile watermark [14], is required for tamper-proofing purposes. In short, fragile watermarking involves embedding information into a file which is damaged if the file is modified. This method is inappropriate for footage the copyright holder of the file

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been damaged with, such as using a file as proof in a court of law, since any damaging would have removed the watermark. Fragile watermarking techniques tend to be easier to implement than robust methods. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal.

IV. GENERAL MODEL OF DIGITAL IMAGE WATERMARKING

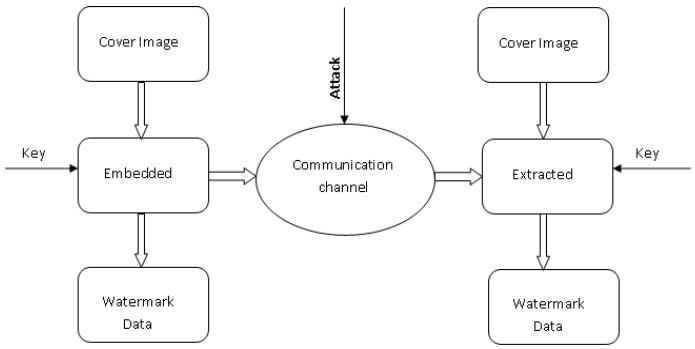

Fig 4: Illustration of Digital Watermarking

The digital water marking system basically consists of a watermark embedded and a watermark extracted. By using watermark embedded, watermark is inserted onto the conceal signal and using watermark extracted identify the occurrence of watermark signal. An entity called watermark key is used during the procedure of embedding and detecting watermarks.

V. WATERMARKING ATTACKS

There are various possible intentional or unintentional attacks that a watermarked object is likely to subject to. The availability of wide range of image processing software's made it possible to perform attacks on the robustness of the watermarking systems. The aim of these attacks is to prevent the watermark from performing its intended purpose[9]. A brief introduction to various types of watermarking attacks is as under,

A. *Removal Attack:* Removal attacks suggest to remove the watermark data from the watermarked object. Such attacks use the detail that the watermark is usually an additive noise signal present in the host signal.

B. *Interference attack:* Interference attacks are those which add extra noise to the watermarked object. Lossy compression, continuation, consent, denoising, remodulation, averaging, and noise storm are certain examples of this type of attacks.

C. *Geometric attack:* All manipulations that concern the geometry of the image such as flipping, rotation, cropping, etc. should be visible. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

D. *Low pass filtering attack:* A low pass filtering is done over the watermarked image and it results in a variation map composed of noise.

E. *Forgery attack:* The forgery attacks that result in object insertion and deletion, scene background transforms are identical to substitution.

F. *Security Attack:* In particular, if the watermarking algorithm is identified, an attacker can further try to present modifications to make the watermark invalid or to estimate and modify the watermark. In this case, we converse about an attack on security. The watermarking algorithm is measured secure if the embedded information cannot be damaged, detected or forged.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

VI. ANALYSIS & QUALITY PERFORMANCE MEASURES

A. Peak Signal to Noise Ratio (PSNR):

PSNR is the ratio between the most feasible power of a signal and the power of damage noise that change the reliability of its representation. Because many signals have a extremely wide dynamic range, PSNR is usually specific in terms of the logarithmic decibel (dB) scale. The PSNR can be computed as follows

$$PSNR = 10\ X \log 10 \frac{255\ x\ 255}{\frac{1}{H\ X\ W}\sum_{X=0}^{H-1}\sum_{y=0}^{W-1}[f(x,y)-g(x,y)]^2} dB \quad (1)$$

where H and W area part of the height and width of the image, severally; and f(x,y) and g(x,y) area section the gray levels situated at coordinate (x,y) of the first image and attacked image, respectively.

B. Mean Square Error(MSE):

It is considered as average squared difference between the original image and distorted image. It is calculated by the formula given below

$$\text{MSE} = \frac{1}{\text{n}} \sum_{\text{i}=1}^{\text{n}} (\hat{\text{Y}}_{\text{i}} - \text{Y}_{\text{i}})^2 \quad (2)$$

where, Yˆ is the distorted image and the Y is the original image[13].

C. Root Mean Square Error(RMSE):

The Root Mean square Error (RMSE) may be a frequently used exists of the distinction between distorted image values and also the original image values.

$$\text{RMSE} = \sqrt{\frac{\sum_{\text{i}=1}^{\text{n}} (\hat{\text{Y}}_{\text{i}} - \text{Y}_{\text{i}})^2}{\text{n}}} \quad (3)$$

Where $\hat{\text{Y}}$ is distorted image and Y is original image.

D. Structural Similarity Index Module (SSIM) [15]:

The structural similarity index may be a technique for menstruation the similarity between the distorted image and also the original image.

$$SSIM\ (y, \hat{y}) = \frac{\left(2\mu_y\mu_{\hat{y}} + c_1\right)(2\sigma_{y\hat{y}} + c_2)}{\left(\mu_y^2 + \mu_{\hat{y}}^2 + c_1\right)(\sigma_y^2 + \sigma_{\hat{y}}^2 + c_2)} \quad (4)$$

where, $\hat{\text{Y}}$ is that the distorted image, the Y is that the original image, μ is that the mean and also σ is that the variance.

E. Bit Error Rate(BER):

It is the ratio that computes how many bits received in error over the number of the total bits received.

$$BER = \frac{\text{C}}{(\text{H} * \text{W})} \quad (5)$$

Where, H and W are height and width of the watermarked image, C is the count number initialized to zero and increment by one [12].

VII. CONCLUSION

This paper presented is a complete outline of Digital image watermarking techniques. A number of modern digital watermarking techniques are presented to support copy right protection for internet users. These techniques are classified into several categories depending upon the domain, document and perception in which the hidden data is inserted and to be extracted. This survey on different digital watermarking techniques shows altered robustness level on discrete attacks. In this paper we tried to give the whole information about the digital watermarking which will help the new researchers to get the maximum awareness in this domain.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

REFERENCES

1. Puneet, K., Sharma, R., and Rajni, "Analysis of Image Watermarking using Least Significant Bit Algorithm" International Journal of Information Sciences and Techniques (ijist) Vol.2, pp.95-101, July 2012.
2. Wang, J., Healy, R., Timonel , J., "Perceptually Transparent Audio Watermarking of Real audio based on the cspe Algorithm", symposium on Computers and Communications, 2010.
3. Christine, I., Podilchuk., Edward J.Delp, "Digital Watermarking: Algorithms and applications", IEEE signal processing Magazine, July 2001.
4. Monkia Patel, Priti Srinivas Sajja, "Digital Watermarking Based on different Techniques", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Vol. 3,No.10, October 2013.
5. Chirag Sharma, Deepak Prashar, "DWT based robust technique of watermarking applied on Digital images", International Journal Soft Computing and Engineering (IJSCE), Vol.2,No.2, May 2012.
6. Falkowski, B.J., Lim, L.S., "Image Watermarking using Handmard Transforms", in IEEE Electronics Letters, United Kingdom, Vol.36, No.3,pp.211-213, February 2000.
7. Mohan Durvey, Devshri Satyarthi, "A review paper on digital Watermarking", International Journal of Emerging Trends & Technology in Computer Science(IJETTCS), Vol.3,No.4, August 2014.
8. Meenu Singh, Abhishek Singhal and Ankur Chaudhary, "Digital Watermarking Technique", Internal Journal of Computer Science and Telecommunications(IJCST), Vol.4,No.6, June 2013.
9. Prabhishek Singh, Chadha R.S., "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Vo.2, No.9, March 2013.
10. Dr. Vipula Singh, "Digital Watermarking: A Tutorial', Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), January Edition, 2011
11. www.igi-global.com/chapter/literature-review-selected-watermarking-schemes.pdf
12. Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, "A Novel Technique for Digital Image Watermarking in Spatial Domain", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing,2012.
13. Gursharanjeet Singh Kalra, Rajneesh Talwar, Harsh Sadawarti, "Comparative Analysis of Blind Digital Image Watermarking Utilising Dual Encryption Technique in Frequency Domains", World Journal of Computer Application and Technology (wjcat),DOI:1013189,2013.
14. Pragya Jain Anand S.Rajawat, "Fragile Watermarking for Image Authentication", International Journal of Electronics and Computer Science Engineering (IJECSE), ISSN – 2277-1956.
15. Ankita Sharma, Sarika Khandelwal, "A Brief Introduction to Digital Watermarking", International Journal of Computer Science and Information Technology", Vol.6,No.3,2015.
16. Peyman Rahmati, and Andy Adler, and Thomas Tran. ―Watermarking in E-commerce‖, (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 4, No. 6, 2013
17. Neil F. Johnson, Zoran Duric, and Sushil Jajodia. ―A Role for Digital Watermarking in Electronic Commerce‖, http://citeseerx.ist.psu.edu/viewdoc/download?doi= 10.1.1.449.6184&rep=rep1&type=pdf
18. Arathi Chitla, M. Chandra Mohan,‖ Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography (ECC)‖, International Journal of Computer Applications (0975 – 8887) Volume 57– No.6, November 2012

BIOGRAPHY

M.Hariharalakshmi is an Assistant Professor and Research Scholar in the Computer Science Department, College of Sri Parasakthi for Women, Courtallam, Tamilnadu, Manomaniam Sundaranar University. She received Master of Computer Application (MCA) degree in 2008 from National Engineering College, Kovilpatti, Anna University, Tamil Nadu, and India. Her research interests are Image Processing, Computer Graphics etc.