International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 02, February 2017
www.ijates.com
ijates
ISSN 2348 - 7550

A SURVEY ON DIGITAL WATERMARKING FOR HIGH SECURITY AND ITS APPLICATIONS

Dr. Ganashree T. S[1] , Mahesha AM[2]

[1]*Department of Telecommunication Engineering, Dayanandsagar College of Engg. , Bangalore, (India)*
[2]*Department of Computer Science and Engineering Visveswaraya Technological University, (India)*

ABSTRACT

Abstract--Incredible growth of internet technology has made the digital content available on hand and it is easily accessible to unauthorized users to replicate, manipulate, and distribute using the same technology. This wide use of digital content needs emphasis on safeguarding this multiple media content. So, in this paper prominence is given to categories of watermarking and its applications than on watermarking structure, mechanisms, threats on watermarked data and its evaluation process. For high security of digital content on World Wide Web it needs details on types of watermarking then applying it appropriately at the required scenario. The intention of digital watermarking is to integrate concealed information in multiple media to defend the exclusive rights of an individual's creation.

Keywords: Ghost Image, Intellectual Property Rights, PSNR, Payload, Watermarking

I Introduction

In Today's world of internet being used for all types of communication in the form of multiple media, we are very much in need of protecting our sensitive information being transmitted on the insecure channel. This information can be our legal rights on the data or multiple media we are transferring and/ or making available on World Wide Web.

Since internet is fastest medium being used for transferring data to any part of the world. It has given rise to theft of Intellectual Property (IP) rights on digital content which can be in text, audio, video, images. So watermarking process is a way for securing data from these thefts of IP rights.

Here in watermarking owners personal information is merged with his/her digital content at the time of sending the data. At receiving end this owner personal information is being used to identify the authentication of data. These watermarking process is used in multiple media like text documents, Images, audios and vedios.The refered research papers say there are many research scholars working on this watermarking process to improvise the results gained

from earlier research.[12]

This paper is sectioned as 2. Historical view of digital watermarking. 3. Categories of digital watermarking. 4. Threats for Digital watermarking. 5. Evaluation of the watermarking process 6. Applications of Digital Watermarking. 7. Conclusion

II HISTORICAL VIEW OF DIGITAL WATERMARKING

Watermarking mechanism finds its evolution from 13th century they were used to identify the manufacturer of the paper. Watermarks are used even till today as manufacturer marks. It is also used for maintaining Authentication, Integrity and Confidentiality between the sender and receiver of the watermarked data and to prevent imitations of paper currency. The main aim of watermarking is to launch information authenticity which can be ensured at the receiver based on the embedded secret information ie watermarking. Information hiding takes the advantage of human vision system.

Steganography can be seen as classical version of hiding the secret information and digital watermarking found its existence due to enormous growth of internet technology. Steganography aims for imperceptibility to human vision system by concealing information and hiding its location from the unauthorized access. Except for the sender and receiver knows the existence of information, this is being used in olden days and it is treated as *invisible watermarking*. The term "Digital Watermark" was coined by Andrew Tirkel and Charles Osborne in December 1992. The first successful embedding and extraction of a spread spectrum watermark was demonstrated in 1993 by Andrew Tirkel, Charles Osborne and Gerard Rankin. [10]. Digital watermarking is another dimension to cryptography, considering robustness as its top priority. In cryptography an unauthorized person normally knows that information is being communicated, algorithm being used and only the key size needs to be found by the unauthorized person.

Digital watermarking is a secretly embedding technique of digital content with secret information that can be extracted by the recipient. The image in which the secret data to be embedded, is called the cover image or host. The watermarking process has to be flexible against attacks and tampering keeping the content of a watermark readable in order to be recognizable when extracted by the recipient.

Robustness, fidelity and payload are the essential factors of a watermarking system; considering capacity of the embedded information, data becomes less robust based on increase in the capacity. As a result there is a loss and gain between these factors and these must be considered while implementing the watermarking mechanism. [3]

Today we use watermark in our daily official documents usage of MS-Word document for instance to mark the documents as confidential on the background layer of the paper which is visible and readable to our eyes. It is called as *visible watermarking.* In general there is need for us to use watermarks for securing sensitive information on insecure e-communication channels.

III CATEGORIES OF DIGITAL WATERMARKING

When it comes to watermarking of digital content which is available on the internet in the form of text, audio, video, images and any form of digitized documents are seen as digital image watermarking of this digitized images. Digital image watermarking method can be viewed in seven categories and it is represented in a tree structure form as shown in the Fig. 1 below

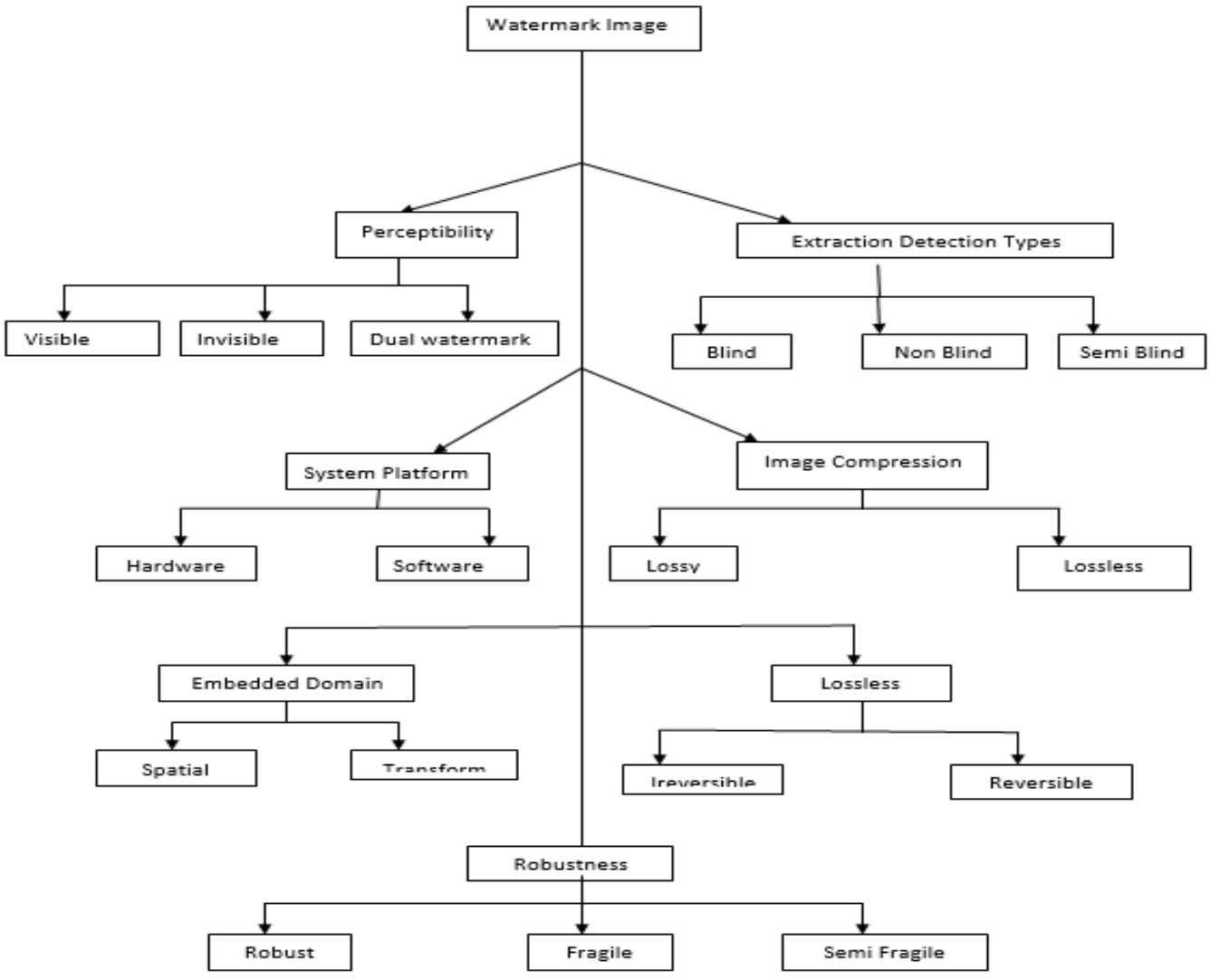

Fig. 1: Tree structure representation of categories of watermarking

There is common need to be reached when Watermarking method is implemented. Based on the needs watermarking method can be categorized into seven as shown in the fig 1.

3.1 Perceptibility

Visible and invisible watermarking based on *perceptibility* criteria. *Visible* watermarking is about visibility of marked image as owners right for protecting his/her authority on the marked image. For example in currency notes, Bond papers logos on TV channels etc.,*Invisible* watermarking is about embedding an image which is cannot be perceived by human vision system but needs specialized software to extract the watermarked image from the cover image to identify the owner of the cover image. For example text documents, images or even audio content.

Dual watermarking combination of visible and invisible watermarks, invisible watermark used as back up for visible watermark.

3.2 Extraction

Blind, semi-blind and non-blind watermarking based on the way *extraction* of watermarking is done. Blind watermarking is also called as *public* watermarking, it requires neither the cover image nor the embedded watermark, but extracts n bits of the watermark data from the watermarked image. *for example :* Piracy control is the specific application of blind watermarking which has to send different watermark to each user and distinguish and understand these different watermarks.

Semi-blind watermarking is also called as *semi private* watermarking; intention is to find whether that the watermark can be detected. Semi private watermarking does not require cover image. For example used in applications of systems of copy control ie.as in DVD where copying is not allowed), copy right protection (ownership) and fingerprinting where purpose is to recognize the original recipient of the pirated copies.

Non Blind watermarking is also called as *private watermarking*, it requires original data (Cover image) for detection, *first way* is to extract the watermark from the possibly distorted data and use the original data as a clue to find where the watermark could be in distorted data. *Second way* needs copy of the embedded watermark for extraction and give in Yes or No to recognize watermark data exists and this is believed to be more robust because it exchanges very little information and access to secret information. Non blind watermarking is not research topic in today's world of internet.

3.3 Platform

Hardware and software based watermarking considering the system *platform* used for watermarking.

Hardware watermarking can be implemented but it lacks in watermarking algorithm implementation where as software implementation of watermarking algorithms operations are performed as computational process on microprocessor that extensively consumes more power and algorithm code should be stored in memory which occupies more area. and it may not perform sufficiently fast. It may be faster to implement an algorithm in software, it is due to availability of software tools for various watermarking operations, but limitation to time complexity and

space complexity of the implementation. The reasons for moving towards hardware implementation is algorithms operations are implemented in custom designed circuitry leading to advantages like increase in speed of performance and decrease in power consumption. Hence hardware watermarking scheme is more economical.[4]

3.4 Image Compression

Lossy compression watermarking and lossless compression watermarking based on *image compression* methods used. The reason for compression is easy to handle in storage and communication. According to Image Compression, compression can be categorized to two main groups lossy and lossless.

The lossy compression also called as irreversible compression is applicable only to non-sensitive data such as video watermarking because it does not lead to any major changes to the original data if some part of data is lost. Transform coding techniques like Wavelet and Cosine transforms are found to be appropriate for lossy compression watermarking. Lossless compression also called as reversible compression which does not cause a loss of data. On reversing the compressed data to its original data both are same; it is most frequently used in medical image analysis and in sensitive data watermarking. [5]

3.5 Robustness

Fragile, semi fragile and robust watermarking is based on *Robustness* criteria.

A digital watermark is known as *fragile* when it is not detectable after the smallest amount of modifications., Commonly used for maintaining integrity of the information ie tamper detection.

Semi fragile watermarking resists gentle transformations but not able to detect after rough transformations.

Robust watermarking is with respect to resisting designated class of transformations commonly used in copy protection application.

3.6 Quality

Eventually there is irreversible and reversible watermarking based on *quality* of the watermarking image.

Reversible watermarking is a mechanism that enables images to be authenticated and then restored back to the original data as before the watermarking of the original data. Irreversible watermarking ie unalterable once slight modifications are done to original data in order to conceal informative message and it is irreversible question of reliability arises on the watermarked data, and this is not always acceptable. So most of the watermarking we use and prefer to be reversible. [23]

Arsalan,malik,and khan[5] has proposed a intelligent reversible watermarking approach GA-RevWM for medical images.here intelligent is applied to improve the imperceptibility for a fixed payload. The experiment results show significant improvement in terms of imperceptibility for a desired level of payload against the existing approaches.

3.7 Embedding

There is *spatial* frequency and *transform frequency* watermarking methods based on *embedding* domain.

These are two approaches used for merging of watermarks in host image. In spatial domain approach changing pixel values of host image and used in document authentication and tamper detection. Frequently used spatial domain techniques are LSB, Spread spectrum.

In Frequency domain approach hiding the watermark image in coefficients which spread the watermark image thru the frequency spectrum, frequently used frequency domain approaches are DCT, DWT which are widely used in watermark embedding process.

When designing a watermarking process considering the characteristics of image is essential i.e. *robustness, payload, Imperceptibility.*

3.8 Common Watermarking Structure

Let us go thru the common watermarking structure that is as shown in the Fig. 2 below:

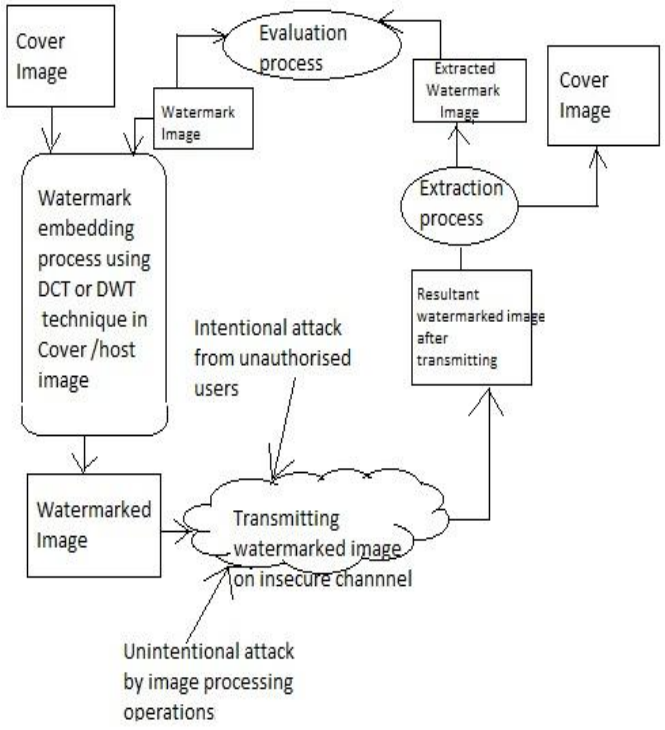

Fig. 2: Common watermarking structure

The above Fig 2. Gives a common structure of watermarking process. Square and Rectangle gives a logical end to the process, elliptical shape and rounded vertical rectangle gives process takes place and arrow marks show the flow of watermarking process.

3.9 Working of Watermarking mechanism Discrete Cosine Transform and Discrete Wavelet Transform

Working of Discrete Cosine Transform (DCT): Digital image watermarking using DCT is most popular transform domain. DCT behaves as tool to decorrealte the input signal in a data independent manner. [13]

In order to embed the watermark DCT allows cover image to be decomposed into different frequency bands like high, middle and low bands. So it is easier to choose the suitable band in which we are going to embed watermark. Usually watermark is embedded in middle band and it does not spread out to low frequency band. It does not overexpose them to remove through image compression and noise attacks where high frequency components are chosen. [6].There are diverse methods of DCT based watermarking technique one of the technique chooses middle band frequency region to provide additional imperceptibility to lossy compression techniques and avoiding major modifications to the cover image. [13][10]

Let us consider a cover image with size SxS then DCT is performed for each block of the selected band for a given piece of an image (ie block of size SxS) function f (i, j) over two integer variables *i* and *j* , the DCT transforms it into a new function F(u,v) with integer u and v running over the same range as *i* and *j*. DCT defined and expressed as :

$$F_{(u,v)} = \sum_{i=0}^{S-1}\sum_{j=0}^{S-1} C_{(u)}C_{(v)}f_{(i,j)} \cos\left[\frac{\pi(2i+1)u}{2S}\right]\left[\frac{\pi(2j+1)v}{2S}\right] \quad \text{..... (1)}$$

$$f_{(i,j)} = \sum_{i=0}^{S-1}\sum_{i=0}^{S-1} C_{(u)}C_{(v)}\,F_{(u,v)} \cos\left[\frac{\pi(2i+1)u}{2S}\right]\left[\frac{\pi(2j+1)v}{2S}\right] \quad \text{..... (2)}$$

$$C_{(u)}C_{(v)} = \begin{cases} \sqrt{1/S}, u, v = 0 \\ \sqrt{2/S}, u, v = 1,2 \ldots S-1 \end{cases}$$

As said earlier it is popularly used for [11] Digital Image Watermarking implementation for the reasons like a) till date most common image compression technique are JPEG based on DCT b) results on incorporation of characteristics of Human Vision System are already available for DCT, these results influence their use in designing imperceptible data hiding schemes.

Working of Discrete Wavelet Transform (DWT): Is another method of *decomposition* that has gained a immense transaction of recognition in current years is the wavelet transform. There are two types of wavelet transforms: the *Continuous Wavelet Transform (CWT)* and *Discrete Wavelet Transform.* CWT applied to large class of functions. DWT applied on discrete samples of the input signal.[13]

DWT technique can be seen similar to human vision system behavior. DWT uses this behavior to embed the

watermark data in less sensitive area to Human Vision System (HVS). [8]

DWT is a best example technique under transform domain watermarking technique here [8] it modifies the quantized coefficients of cover image.DWT acts as tool for decomposing images into four components namely LL1, HL1, LH1 and HH1 as shown in Fig. 3 below:

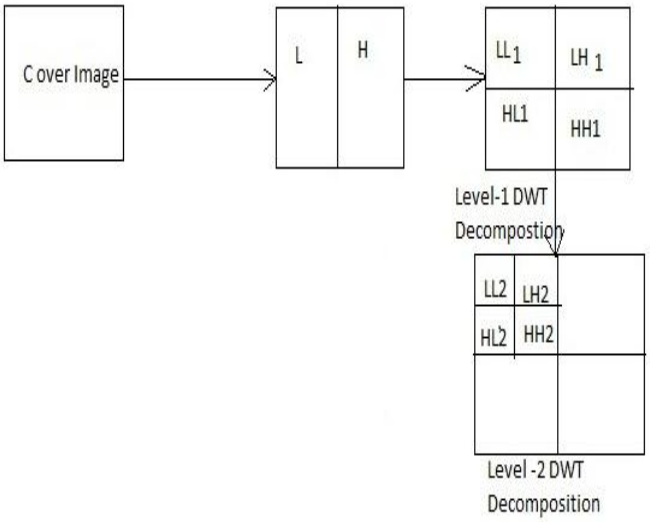

Fig 3: Two Level DWT Decomposition

We call these four components as sub bands also named as

LL1 (low, low) approximate

LH 1(low, high) vertical

HL 1(high, low) horizontal

HH 1(high, high) diagonal

From the review of research papers it is known fact that maximum energy is found LL sub band(low frequency)so any changes to coefficients of these LL sub band will lead to image loss[6]. So we should not embed watermark in LL subband.It is better to embed watermark data in high frequency band.

Merits of DWT: DCT decompose image into blocks where as DWT does not decompose into blocks for processing. Perceptually DWT images are less evident [12] when compared to DCT.

DWT will affect the image specifically.DWT allows to watermark on the region which is less sensitive to HVS.

3.10 From our perspective spatial and frequency domain differences can be viewed as*:*

Spatial watermarking applies watermark to a specific color band so that watermark only visible when the colors are separated. Frequency watermarking applies a watermark to a specific frequency so that watermark only visible when that frequency is separated out.

IV THREATS FOR DIGITAL WATERMARKING

To measure performance of digital watermarking system three factors are considered robustness, invisibility and capacity. *Robustness* must restrict itself to any kind of attacks like rescaling, compression, cropping, rotation, noise is some of the attacks (but not all of the types are surveyed in this paper) *Invisibility* watermarked image should look indistinguishable from the original image even on highest quality equipment. *Capacity* based on the survey of many research papers capacity of watermarking scheme varies from small fraction of host image size to multiple times the size of host image. [8]

Chunlin Song, Sud Sudirman, and Madjid Merabti [8] proposed a region adaptive approach for watermarking technique to further improve upon invisibility and robustness but limitation of this technique is due to limited number of suitable regions for storing watermark, storing capacity can be low due to limited number of suitable regions.

In watermarking technology *attack* is any processing that may deteriorate the detection of watermark or communication of information concealed by the watermark.

Aim of watermark attacks is *w*atermarking mechanisms is successful or not is mainly dependent on its robustness property being able to with stand different attacks. These watermark attack intention is to remove or display any watermark in the cover image hence it is necessary to analyze how these watermarking attacks work on watermarked image so that it helps us to design best watermarking mechanism.

4.1 Categories of attacks

In one of the reviewed paper has classified watermarks attacks into 4 different categories namely *Removal, geometric, cryptography, protocol attacks.* Initially, It can also be classified broadly as Intentional and Unintentional attacks. *Unintentional attack* n watermarked image, watermark data is likely to undergo one or the other kind of image processing operations before it reaches the receiver. Processing can be lossy compression, signal enhancement etc.*Intentional attack:* other types of processing are done intentionally to disturb the watermark reception.

4.1.1 Removal attack

Is straight forward approach which destroys the existence of cover image completely without identifying watermark or trying to know the technique used for watermarking.

4.1.2 Geometric attack

Geometric attack can be treated as distortion attack, because the detection of watermark is impossible in the watermarked image. But can be recovered with the help of more intelligent watermark detection mechanism. Like zooming, rotation, cropping between recovered image and cover image.

4.1.3 Cryptography attack

Cryptography is going to break the security of watermarking technique and finds a way to remove the watermark information from watermarked image or insert deceptive watermarks. Brute-force search is an example here to

search for the watermark information. Practically use of These attacks are limited due to their high computational complexity.

4.1.4 Protocol attack

It is an attack on the entire concept of the watermarking application by disabling the authority of watermarked image. This makes an attempt to mislead the detection of watermark by embedding several additional false watermark data to disable the ownership of the watermarks.

V EVALUATION OF WATERMARKING PROCESS

Evaluation is very much essential and important part of any watermarking techniques. Here we estimate the quality parameters of the Digital Image watermarking process like PSNR (Peak Signal to Noise Ratio) and NC (Normalized Correlation)

PSNR measure quality from HVS perspective where it determines efficiency of watermarking with respect to noise,Where it degrades the quality of image.

From HVS perspective quality of watermarked image and attacked image are measured using

PSNR = 10 log (P^2/MSE)

Where p= max value in host image. If PSNR value is high it shows that watermarked image is perceptible ie not visible to Human Vision System.

Mean Square Error (MSE) measures the average of the squares of the errors between Cover image and watermarked image. Mean Square Error is expressed as:

$$MSE = 1 \div MN \sum_{i}^{M} \sum_{j}^{N} (Wij - Hij)^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

M, N is pixel values in host image

$W_{i,j=}$ is pixel values in watermarked image

$H_{i,j=}$ is pixel values in host image

NC is computed using original watermark Wi and extracted watermark W'i to justify the existence of watermark and it is expressed as :

$$NC(w, w') = \frac{1}{N_w} \sum_{i=0}^{N_w} w_i \times w'_i. \quad \ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Nw being number of blocks

VI APPLICATIONS OF WATERMARKING

Digital watermarks are practically valuable in many areas like

6.1 Copyright protection

In case of photographers, photographers have always needed to take steps to protect their work. these watermark options give photographers several ways to prevent and prosecute illicit uses of their images.

6.2 Fingerprinting

It's a process of associating [12] unique information about each distributed copy of digital content which allows owners of digital content to establish and scrutinize reproduced data that are illicitly accessed. Fingerprint (is image information) is embedded in every copy of original data using watermarking process because it is invisible and inseparable from the content.

6.3 Medical

Watermarking can be used to hide the patient information and extract back by owner using certain keys.

Its about medical information security thru watermarking. Mandatory characteristics of security we know Confidentiality, Availability and Reliability. In medical information system these characteristics can be reached thru security services like Integrity, Availability, Authentication and non repudiation. Using technique of visible watermarking patient names are printed on X-rays, MRI scans etc.

6. 4 Transaction Tracking

Visible watermarking is regularly used in this application but invisible watermarks can also be used for better solution. Watermarks record the receiver's information in each authorized sale or allocation of the work. If work is misrepresented (disclosed to press or unlawfully circulated) there is way for title-holder to find out who is the collaborator.

6.5 Broadcast monitoring

Media contents like music,songs,advertisement and other custom audio and video or online channels all the time knowing where,when,how and why they are broadcasted.

For instance to monitor the TV, radio broadcasting watermarks are used to prevent airtime booking. It can be monitored active and passive.*Passive* monitoring uses computers with a database of known contents.*Active* monitoring identification of information can be directly decoded.[16]

6.6 Information management system

With information management processes, it is difficult to protect the created pdf files from alteration or misuse once it is sent and distributed to others. There are different levels of security for important documents like passport, monetary objects, the content within a pdf is also treated with same importance major concern for pdf is security against alteration and misuse. In order to provide security to pdf along with security like copying, printing to retain the distinction within hard copies once documents are printed and in case of pdf content is sensitive or not, in all these possibilities adding watermark to pdf acts as a good control of categorization of pdf document. Stamping watermarks on created pdf by pdf creator is done along with pdf creator services.

Watermarks can be textual or image placed foreground or background content of the pdf pages.

6.7 Intellectual Property Rights (IPR) Protection

Under IPR we find Trade Secret, Patents and Copyright constraints for the illicit users of documents. Major task here is demonstration of the ownership in legal disputes, fingerprinting and copy control. It is mainly the responsibility of Government to protect even if we design advanced model for IPR protection.[10]

6.8 Invisible marking on documents

Purpose of using digital watermarks on white papers in the form of blot is to authenticate the creator and content or to engage the document. For example official documents like contracts used by ,lawyers embed the name of the lawyer, in future, when argument arises digital watermark is read and creator of the document is authenticated. This concept of marking on document is a patented technology and is known as Cryptoglyph.[10]

6.9 ID Card Security

Information in a ID is embedded into the photo on that ID Card, on extraction and comparing with the information written on ID card, it can be verified. Here information in ID card is the watermark embedded and extracted. If the ID card is stolen and photo is replaced by another photo of the same person which does not contains any kind of watermark, this leading to failure in extracting the watermark will cancel the IDCard

In case of passports today to avoid duplications of passports in various places Indian passports are using additional ghost image which makes passport more secure and tamper proof. A ghost image is similar to watermark image of Mahatma Gandhi in Indian currency notes along with ghost photograph, the personal details of the passport holder will be embedded in the passport to make it difficult to duplicate or tamper with it. [15]

VII CONCLUSION

In this paper we presented prominent impression on categories of digital watermarking and its application areas. Secondly, presented common watermarking system with diagrammatic representation gives basic idea about watermarking process, watermarking techniques not much detailed other than just giving direction about using the popular one. Possible threats for watermark basically discussed from intentional and unintentional perspective and its impact measured in evaluation process of watermarking using PSNR for measuring quality of image with respect to human vision system on original image and watermarked image and NC evaluates the original and extracted watermark. A theoretical discussion on categories of digital watermarking and its application are essential for high security of watermarking the digital content from the designing perspective of optimized watermarking mechanisms. Applications are described with respect to real time scenarios in ID card security, information management system, and invisible marking on paper. Area which needs further research is watermarking techniques and its optimization approaches. research papers [11][12] makes us to think of using the popular watermarking techniques any one of the nature inspired algorithms to optimize the result towards improvising the robustness against attacks.

REFERENCES

Journal Papers:

[1] Lalit Kumar Saini, Vishal Shrivastava,"A survey of digital watermarking Techniques and its applications",Vol.2 Issue 3, May –june 2014,pp. 70-73

[2] A.Z.Tirkel, G.A. Rankin, R.M. Van Schyndel, W.J.Ho, N.R.A.Mee, C.F.Osborne. "Electronic Water Mark". DICTA 93, Macquarie University. p.666-673

[3] G. Coatrieux,L Lecomu,Members IEEE, Ch. Roux, Fellow,IEEE,B. Shankar ,Member IEEE A Review of Image watermarking Applications in Healthcare.

[4] Swathi S ,Shobhana S and Lakshmi HR," Hardware Implementation of Watermarking –Importance and Survey",Vol.5,Special issue 10, ,pp 82-87, May 2016,IJIRSET

[5] Muhammad Arsalan, Sana Ambreen Malik, Asifullah Khan, "Intelligent reversible watermarking in integer wavelet domain for medical images", The Journal of Systems and Software, vol. 85, pp. 883-894, 2012.

[6] Meenu singh,Abhishek Singal and Ankur Chaudhry, "Digital Image Watermarking Techniques: A Survey", Vol . 4 , Issue 6,June 2013,pp 51-55

[7] Santi P. Maity, Malay K. Kundu, "Perceptually adaptive spread transform image watermarking scheme using Hadamard transform", Vol. 181, pp. 450-465, 2011

[8] Chunli Song,Sud Sudirman,Madjid Merabti," A robust region adaptive dual image Watermarking technique", ,pp. 549-568,URL: www.elsevier.coom/locate/jvci, 2012

[9] Sanjeet kumar, Sanjeev indora," Digital Image Watermarking Based on Wavelet Techniques: A Review" Vol. 5,Issue 4,April 2016, pp 20-26, Academic Science, IJIACS

[10] Sunesh,Harish Kumar, "Watermark Attacks and Applications in Watermarking" , pp- 8-10, IJCA-RTMC,2011

[11] Yuh-Rau Wang, Wei-Hung Lin, Ling Yang, "An intelligent watermarking method based on particle swarm optimization", Expert Systems with Applications, vol.38, pp. 8024-8029, 2011

[12] Veysel Aslantas "A singular value decomposition based image watermarking using genetic algorithm."pp 386-394,2008

Books:

[13] Ze Nian Li and Mark S Drew, fundamentals of multimedia (Upper Saddle River NJ: Prentice Hall 2004).

URL's:

[14] https://en.wikipedia.org/wiki/Digital_watermarking
[15] https://en.wikipedia.org/wiki/Indian_passport.
[16] https://www.acrcloud.com/broadcast-monitoring