E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

A REVIEW PAPER ON FORENSIC WATERMARKING

Priyanka Premnath[1], Srilatha.L.Rao[2], Kendaganna Swamy[3]
[1]Department of Biomedical Signal processing & Instrumentation ,RVCE,Bengaluru,India
[2]Department of Biomedical Signal processing & Instrumentation , RVCE, Bengaluru, India
[3]Department of Biomedical Signal processing & Instrumentation , RVCE, Bengaluru, India
1priyankapremnth@gmail.com
[2]srilatharao2006@gmail.com
[3]swamy_knsit@rediffmail.com

ABSTRACT:
Watermark is a pattern or image coverted in a paper to discourage counterfeiting of the document. Encoding such a pattern or signal into digital data like image, music, video etc is called Digital Watermark also known as Forensic watermarking. The embedding of the watermark information takes place by manipulating the content of the digital data. The hiding process should be such that the modifications of the media are imperceptible. In this paper we describe the process of Digital Watermarking, the various classifications related to it, the possible distortions and attacks, Bench mark and the types of Bench Mark, the Applications and the recent advancements in this area.

Keywords: *Bench-marking[1], Decoding[2], DCT[3], Encoding[4], Gray level[5], Robustness[6], Water-marking[7], Wavelets[8].*

I. INTRODUCTION

The rapid development in information transmission technology has necessitated the advancement in the ways of handling and protecting the multimedia data and information from unauthorised users. Digital Watermarking is one such potential method for protection of ownership rights on digital audio, image and video data. Digital watermarking is a communication method in which information is embedded directly and imperceptibly into digital data (e.g., image, video, or audio signals),called as original data or host data, to form watermarked data. This embedded information is bound to the watermarked data wherever it goes. The embedded information should still be decodable from the watermarked data, even if the watermarked data is processed, copied, or redistributed. Potential applications of digital watermarking include copyright protection, distribution tracing, authentication, and authorized access control. Thus, the information could be a user-ID, a serial number for a certain copy of a document, or authentication information. Indeed, there are a number of desirable characteristics that a watermark should exhibit. It at least should comply with the following two basic requirements for image watermark:

-The digital watermark should not be noticeable to the viewer nor should the digital watermark degrade the perceived quality of the image. It is so-called the transparency of digital watermark.

-The digital watermark is still present in the image after distortion and it can be detected by the watermark detector. Ideally, the amount of image distortion necessary to remove the watermark should degrade the desired image quality to the point of becoming commercially valueless. Possible distortions include linear or nonlinear filtering, addition of Gaussian or non-Gaussian noise, image enhancements, resampling or requantization [10][12]. In order to achieve the copyright protection and maintain the quality of the signal, the algorithm should meet few basic requirements

i. Imperceptibility: The watermark should not affect the quality of the original signal, thus it should be invisible/ inaudible to human eyes/ ears.
ii. Robustness: The watermarked data should not be removed or eliminated by unauthorized distributors.
iii. Capacity: the number of bits that can be embedded in one second of the host signal.
iv. Security: The watermark should only be detected by authorized person.
v. Watermark detection should be done without referencing the original signals.
vi. The watermark should be undetectable without prior knowledge of the embedded watermark sequence.
vii. The watermark is directly embedded in the signals, not in a header of the signal.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

II. GENERAL FRAMEWORK OF WATERMARKING

Watermarking is the process where data is hidden into an image or audio or video. The general watermarking framework is as shown in figure 1. Detection and extraction of the watermark can be done later from the carrier (cover) signal. It can contain information such as copyright, license, authorship etc[10][12].
An example of a digital watermark is a "seal" on the image to for the identification of the ownership. Any watermarking algorithm consists mainly of three parts:
- The watermark, which is unique to the owner.
- The encoder is used for embedding the watermark into the data.
- The decoder is used for extraction and verification.

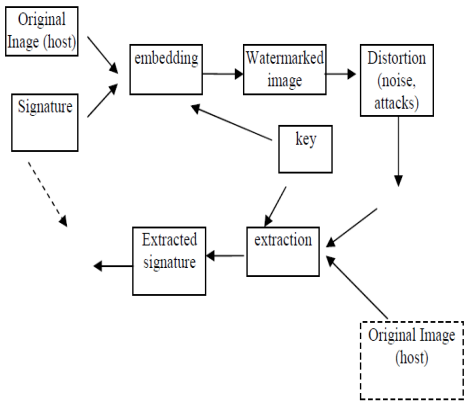

Fig 1. Digital watermarking, a general overview

III. CLASSIFICATION OF WATERMARK ALGORITHM

In this section we discuss different classification of watermarking algorithm[10].
-Firstly, According to type of document, watermarking technique can be divided into four groups: Text watermarking, Image watermarking, Audio watermarking, Video watermarking.
-Secondly based on the human perception, watermark algorithms are divided into three categories: Visible Watermarking: Translucent overlaid into an image is visible to the viewer, Invisible watermarking: Embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed, Dual watermark: Combination of visible and invisible watermark. An invisible watermark is used as a backup for the visible watermark.
- Thirdly, according to the watermarking extraction process, techniques can be divided into three type: Non-blind(In private watermarking original signal is required for detection of the watermark), Semi-blind(Sometimes it requires some extra information for detecting the watermark like a secret key or watermark bit sequence),Blind or public watermarking(watermark detection we require only secret key).

-Fourthly, Classification based according to the additional feature 'robustness'. Robust Watermark in which the watermark can survive after common signal processing operation such as filtering and lossy compression, Fragile watermark(where the watermark should be able to be detected any change in signal and also possible to identify the signal before modification),Semi-Fragile Watermark(Sensitive in nature and they can change a watermarked image).
-Finally based on Embedding processing domain, watermark technique can be divided into:
• Spatial Domain which refers to the image plane itself, where watermark data to be embedded in the pixel value. In this method some minor changes are made in pixel value intensity.
• Transform Domain: Transform domain have imperceptibility as well as satisfy the robust property. Transform domain is also called frequency domain because value of frequency can be altered from their original value.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

IV. DISTORTIONS AND ATTACKS

Distortions and Attacks are the attempt made to weaken the quality of the image and destroy it.
First of all, we have to distinguish two reasons for an attack against a watermark image:
• Hostile or malicious attacks, which are an attempt is made to weaken, remove or alter the watermark, and
• Coincidental attacks, which can occur during common image processing and are not aimed at tampering the watermark.
One categorization of the wide class of existing attacks contains four classes or attacks:
• Removal Attacks: It aims at the complete removal of the watermark information from the watermarked data without such that the security of the watermarking algorithm (e.g., without the key used for watermark embedding)is not affected. That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. It includes de-noising, quantization (e.g., for compression), re-modulation, and collusion attacks.
• Geometric Attacks: In contrast to removal attacks, geometric attacks do not actually remove the embedded water- mark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. The best known benchmarking tools are Unzign and Stirmark, they integrate a number of geometric attacks. Unzign introduces local pixel jittering and is very efficient in attacking spatial domain watermarking schemes. Global and local geometric distortions are introduced by stirmark.
• Cryptographic attacks: It aims at cracking the security methods in watermarking schemes and thus finds a new way to remove the embedded water- mark information. One such technique is brute-force search for the embedded secret information. Oracle attack comes under the same category, which can be used to create a non-water- marked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity.
• Protocol Attacks: It aims at attacking the entire concept of the watermarking application. Invertible watermarks is based on this. The idea behind is that the attacker subtracts his own water-mark from the watermarked data and claims to be the owner of the watermarked data. Thus ambiguity is created with respect to the true owner-ship of the data. It has been shown that for copyright protection applications, watermarks need to be noninvertible. The requirement of non-invertibility of the watermarking technology states that it should not be possible to extract a watermark from a non-watermarked document. A solution to this problem might be to make watermarks signal-dependent by using one-way functions. The copy attack also comes under the same category. Here, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data.

V. BENCHMARKING

Benchmarks are used to evaluate the robustness of the watermarking technique. To prevent unauthorized use of digital content, when using digital watermarking, the robustness of the watermarking should be evaluated in detail. To evaluate the robustness of watermarking, benchmark tools such as Stirmark and JEWELS have been developed. These tools can show which attacks will break embedded digital watermarks.

Existing benchmark tools:
The various benchmark tools attack digital watermarks and estimate whether digital watermark was destroyed. Stirmark and JEWELS are the two well-known benchmark tools.

• *Stirmark*: It is the most popular benchmark tool, and was developed at Cambridge University in the UK in1998. The latest edition is the fourth version, which was released in October 2007. Stirmark has attack functions that use image processing, such as adding noise, rotation, JPEG compression, and cropping. It can fine tune its parameters. For example, the quantity of noise added to an image can be set when adding noise, and the angle can be set per degree of rotation. However, all the attacks using are classed as single image attacks. Moreover, it is a program with a command line base without an image viewer, so to see the attacked image, another independent image editor is required.

• *JEWELS*: It is a software package developed by Japan Electronics and Information Technology Industries Association in 2000, and has various types of attack functions that use image processing, like Stirmark does. It

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

mainly uses single image attack. The plural image attack function of JEWELS is only a single "composite". It blends two images based on few parameters. It is a program with a command line base like stirmark.

VI. APPLICATIONS OF WATERMARK IN SEVERAL FIELDS/LATEST ADVANCEMENTS:

i. ***The watermarking of synchronous sequential circuits***: State diagrams are basically used to give an abstract description of the behaviour of a system. The classic form of state diagram for a finite state machine is a directed graph which is called the state transition Graph. Authorship of designs can be identified by imposing a digital watermark on the state transition graph (STG) of the circuit. The methodology is also applicable to sequential designs that are made available as firm intellectual property, the designation commonly used to characterize designs specified as structural hardware description languages or circuit net lists. By manipulating the STG of the design in such a way as to make it exhibit a chosen property that is extremely rare in non-watermarked circuits, watermark can be embedded here. While, at the same time, not changing the functionality of the circuit.

This manipulation can be performed without computing this graph in either implicit or explicit form. Instead, the digital water- mark is obtained by direct manipulation of the circuit description. There is evidence that it is not possible to remove watermark with any known algorithms for circuit manipulation and is immune to a variety of other attacks. There are many ways to create a change in the STG that embeds a specific watermark. In general, any change in the STG that can be used as a watermark in this framework should have the following characteristics.

- By performing a direct manipulation of the circuit, a watermark can be embedded.

- The sequence of states traversed by the sequence of inputs specified by the watermark exhibits a specific property that:

- can be checked efficiently if the sequence of inputs that represents the signature is known;
- cannot be easily removed by methods that manipulate the circuit net list.
- is rarely present in non -watermarked designs;
- is hard to detect if the sequence of inputs that represents the signature is not known;

- The change has a limited impact on the size and speed of the circuit.

The choice of the specific STG manipulation to perform is an important one since if affects the quality of the watermark, the difficulty of removal, and the impact on circuit quality[1].

ii. ***Security of cloud****:* Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools
of storage which are generally hosted by third parties. By calculating the expectation value, entropy and hyper entropy, using the cloud generator, clouds are created. The discrete cosine transform embeds the watermark in a standard image by adjusting the block DCT coefficient of the image then by blocking the selected image according to 8x8 pixels then dividing the selected image into non overlapped sub image blocks. Data can be easily stores in the cloud, and accessing cloud applications without the local hardware and software management is possible the help of cloud storage. Conversely the profit are clear, such a service is also strengthens user's physical control of their outsourced data, which unavoidably poses new security risk towards the correctness of the data in cloud. Third party outflow of the data is the major problem in the cloud data storage. In this, Simple substitution for the text encryption and LSB hiding for the image embedment is done.

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

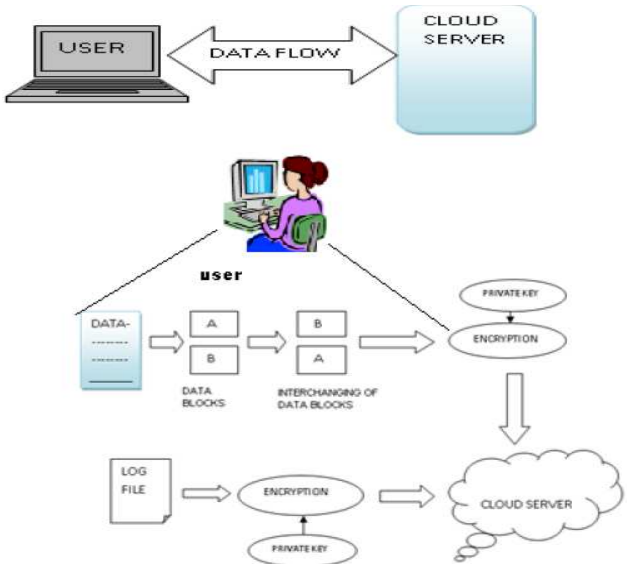

Fig 2: Watermarking in cloud computing [7]

Recent advancement is the Steganography technique of encrypting scheme based on Digital Watermarking Algorithms the two different network entities can be identified as follows:
User: an entity, who has data to be stored and computation, can be either enterprise or individual customers.
Cloud server(CS): an entity, which managed by the cloud service provider(CSP) to provide data storage service and has significant storage space and computation resources.
• Encryption of the data can be done by cloud storage and decrypt the data using the cloud apps that well work with the proposed algorithm.
• Initially, data's are split into number of data blocks and then data blocks are interchanged for the security then converted into binary format and then data encryption is done by the digital marking algorithm. The algorithm attempts to combine image watermarking and text encryption together into one. The key which is generated by the user plays an important role. It is impossible to hack the information unless the secret key is known. Along with the textual information, logos or symbol can be embedded. The size of the secret image should be less than the host image. Text and Image(s) is embedded based on starting from pixel positions as determined by the user's key. Using simple bit manipulation, the secret image can be embedded into the host. The secret image can be the logo of the business. The n least significant bits of the original image are masked, hidden and substituted by the n most significant bits of the watermark image for LSB hiding algorithm. Smaller the value of n, lesser is the weakening in the quality of the image[7][9].

iii. ***Perceptual digital watermark of images using wavelet transform:*** In this method, Watermarks are embedded in the wavelet coefficients and the main criteria is that the amplitude is controlled by the wavelet coefficient. So that it should not exceed the Just Noticeable Difference of the wavelet coefficients. Watermark noise in wavelet coefficients is of the same order as that of visually significance of wavelet coefficients. In this method, transparency and the robustness of digital watermark in the image are guaranteed[3].

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

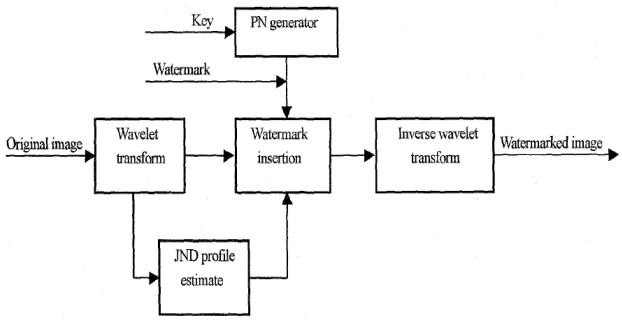

Fig 3: Block Diagram of Perceptually Based Watermarking technique [3]

iv. ***Image Verification for Digital Rights Management Using Fragile Watermarks Based on a Human Visual Model:*** It is a method for embedding perceptually based fragile watermarks in digital images. It is mainly designed for the purpose of image verification and tamper proofing for digital rights management applications. The human visual model is employed to guarantee that modifications in images are imperceptible. According to the human visual model, set of quantized contrast functions which are quantized are created first. Next ,the required image is divided into smaller subimages of 3 x 3 dimensions. A set of gray levels with the same contrast as that of the central pixel is obtained for each subimage, from the quantized contrast functions. The gray value of the central pixel of each subimage is replaced by the chosen watermark value. Thus, imperceptibility is guaranteed. Set of random keys is generated using a pseudorandom mechanism which gives a set of random watermark values. Thus, high security is attained. The original image is not used during the verification process of watermarking. This method is used as a visual inspection tool for detection and localization for any image modification or alteration .This approach is feasible[11].

v. ***Fractional Fourier Transformation Domain Image watermarking:*** The most widely used as tool in signal processing, quantum mechanics and quantum optics, pattern recognition , study of time frequency distribution is FRFT. The main criteria is the rotation of angle α in the time frequency plane. In this method the signal is broken down into small fragments which are complex exponentials with linearly varying instantaneous frequencies, by varying the value of α from a range of 0 to π/2.
It is the most commonly used method for inserting the watermarked signals in either spatial or frequency domain. In FFFT more watermarks are created when compared to FT or DCT domain. Various angles are for watermark embedding. This is robust on some important attacks like geometrical transform, filtering etc that could be performed by a pirate. The original image cannot be extracted without knowing the transformation angle used. This prevents piracy [2].

vi. ***DCT Image Watermarking:*** The discrete cosine transform is the representation of an image as a sum of sinusoids of varying magnitudes and frequencies. It operates only on real terms and uses only cosine terms. It is highly orthogonal and is a good decorrelator. It has a unique property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT. It's referred as 'Energy compaction Property'. The signal information is embedded in the lower frequency coefficients. Due to its energy compaction property, many DCT based Digital image watermarking algorithms are developed. A very Common problem associated with DCT watermarking is block based scaling of watermark image changes scaling factors block by block and results in visual discontinuity. A visible watermarking technique is that which modifies the DCT coefficients of the host image, for a embedding factor α =10 visible watermarking is achieved and also using α =0.09 for invisible watermarking. It also make the watermark more robust[3].

vii. ***Digital Watermarking of still images with gray level digital watermarking:*** This is the method used for embedding the digital watermark image in video. By using the multi-resolution signal (two-dimensional and three-dimensional)decomposing technique , the decomposed watermark images with different resolution are embedded in the corresponding resolution of the decomposed video. The watermark information is coded by error correction coding of Hamming code in the algorithm such

E-ISSN: 2321–9637
Volume 1, Issue 5, December 2013
International Journal of Research in Advent Technology
Available Online at: http://www.ijrat.org

that robustness is ensured. It shows that the robustness is strong enough against the attacks of frame dropping, averaging and lossy compression[4].

viii. ***Reversible Watermarking:*** There is a need to restore the original image after extracting the watermark. Reversible watermarking helps in restoring the image without distortion and the weakening of the quality of the image after the extraction of the watermark. In the fields of law enforcement, medical and military image system, it is important to restore the original image without any distortions..Therefore when the watermark has to be removed to completely restore the original image, reversible watermarking can be used. . There are five basic techniques of reversible watermarking; few of them are listed here i) Difference Expansion ii) Histogram bin Shifting iii) Data hiding using Integer Wavelet Transform iv) Contrast Mapping and v) Integer Discrete Cosine Transform. It has fetched enormous attention [6].

ix. ***The other applications are:***

i. Content identification and management
ii. Content protection for audio and video content
iii. Forensics and piracy deterrence
iv. Content filtering (includes blocking and triggering of actions)
v. Communication of ownership and copyrights
vi. Document and image security
vii. Authentication of content and objects (includes government IDs)
viii. Broadcast monitoring
ix. Locating content online
x. Rich media enhancement for mobile phones
xi. Audience measurement
xii. Improved auditing

VII. CONCLUSION:

A digital watermarking is a type of marking mechanism ,in which a watermark is embedded into a noise-tolerant signal such as audio , image or any digital data. It is typically used to identify ownership of the copyright of such signal. Hence the authenticity of the data and also the owner of the is protected It is the process of hiding digital information in a carrier signal, the hidden information should, but does not need to contain a relation to the carrier signal. There has been many enhancements in this field to protect the digital data from any kind of intrusion to discourage counterfeiting.

In this paper we describe about the Digital watermarking process, the classification of the watermarking based on various criteria ,Distortions and attacks on the watermarks, Benchmarking-Types of Benchmarking and the Recent advancements in the field of Digital Watermarking along with the latest approach towards it.

REFERENCES

[1] Oliveira.A (2001): Techniques for the Creation of Digital Watermarks in Sequential Circuit Designs.
[2] Podilchuk and Zeng(1998): Image-Adaptive Watermarking Using Visual Models
[3] Wei and Qin and Fu2 'School of Sciences, Nanjing University of Science and Technology Nanjing 210094, P.R. China : Perceptual Digital Watermark of Images using Wavelet Transform
[4] Xia-mu Niu, Zhe-ming and Sheng-hoSiin: Digital Watermarking of Still Images
[5] Barn M, Podilchuk C and Delp E: Watermark Embedding: Hiding a Signal Within a Cover Image.
[6] Narawade N and Dr.Kanphade R: Reversible Watermarking:A complete Review
[7] Singh .N Matele. S and Shailendra Singh : An Efficient Approach for Security of Cloud Using Watermarking Technique
[8] Kosuke KAMIYA Takuma MORI Keiichi IWAMURA: Development of Benchmark Tool for Digital Watermarking
[9] Varadharajan and Karthikeyan.D and Senthilkumar: Towards Secure and Storage Services in Cloud Computing using Watermarking without Third party
[10] Rewani R and Mahendra K Pundir A K S: Digital Image Watermarking: A Survey
[11] Da-Chun Wu and Wen-Hsiang Tsai: Image Verification for Digital Rights Management Using Fragile Watermarks Based on a Human Visual Model
[12] Ms Rao M.S ,Jyothsna A N, PinakaPani.R: Digital Watermarking: Applications,Techniques, and attacks.