International Journal Of Electronics Engineering (Issn: 0973-7383)
Volume 10 • Issue 2 pp. 210-216 June 2018-Dec 2018 www.csjournals.com

# Review On: Digital Watermarking

Supiksha Jain
M.TECH Scholar, CSE Dept., DCRUST Murthal, India
supikshajain04@gmail.com

**Abstract:** In today's world the art of sending & unveiling the hidden information especially in public places has received more attention so, it has to face many challenges. As sharing of sensitive information via a common communication channel has became inevitable. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. While steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Watermarking techniques have been developed to fulfil the requirement of data hiding.

**Index Terms:** Attacks, Challenges, Techniques, Watermarking>

**Introduction:** Today's generation is witness of development of digital media. Simplest example of digital media is photo captured by our cell phones. As we know internet is the fastest mode for sending digital data over world. As this technology grown up threat of piracy & copyright very obvious thought in owners mind. So, watermarking is a process to secure data from any kind of threat. Watermarking can be done in two ways invisible & dual. Invisible watermark is embedded into the data in such a way that the changes made to the pixel values are perceptually not noticed. Dual watermarking is the combination of both visible & invisible watermark. An invisible watermark is used as a backup for visible watermark.

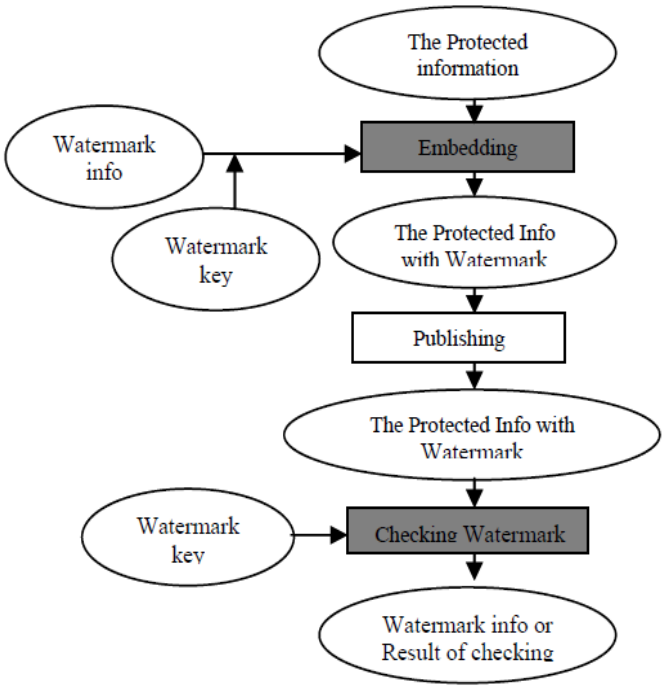



Fig 1: Fundamental Process of digital Watermarking

The authors in [15] & [16] were first to describe that in order for a watermarking technique to be robust, the watermark should be embedded in the perceptually significant portion of the data. Requirements & design of watermarking techniques are impacted by the different types of content in 2 major ways:

- imperceptibility
- robustness requirements

A Digital watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information( author, rights, etc.)

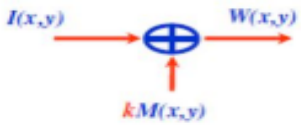
### A. Digital Watermarking: Classification

- According to working : Spatial Domain & Frequency Domain
- According to type : Text, Image, Audio , Video
- According to human : Invisible & Visible
- According to applications : source based & destination based

### A.1 According To Working:

**SPATIAL DOMAIN** : The term spatial domain refers to the aggregate of pixel composing an image. Spatial domain methods are procedures that operates directly on the pixels.

- Watermark message M(x,y)
    a. Random or pseudo random signal
    b. Binary {-1, +1} or {-1,0,+1}
    c. Other signals are used
- Watermark message is added linearly as: W(x,y) = 1(x,y)+ KM(x,y)




**FREQUENCY DOMAIN:**

- This technique is motivated by both perceptual transparency & watermark robustness.
- This technique is very effective both in terms of transparency, robustness to signal processing.

## A.2 ACCORDING TO TYPE:

**TEXT:** Text watermarking is one of the easiest wat to hide information in such a way the format get change & unreadable for the user. But one of the problems wih it is that the changed format is visible for other who sees it. Also the capacity of data to be hidden is limited. There are various watermarking techniques are available like DES, AES, BLOWFISH, etc. which provide some sort of security to the data in terms of key matters. But still it proves to be insecure. If hacker sees this data then can try brute force attack on it to get the hidden data.[17]

**IMAGE:** Images are used to hide data inside it. Images can hide a lot more information compare to text watermarking. Image use watermarking techniques to hide data inside the pixels of the images. Image watermarking involve various techniques based on their spatial information, their frequency information & sometime using hybrid information. Example of spatial image watermarking process is checksum, basic m- sequence etc.

LSB watermarking is one of the most important technique to hide the data in last bits.

**AUDIO:**

1. Least Significant Bit Coding:

This simple approach in watermarking audio sequences is to embed watermark data by altering certain LSBs of the digital audio stream with low amplitude [4].

2. Phase coding:

The basic idea is to split the orignal audio stream into blocks & embed the whole watermark data sequence into the phase spectrum of the first block [4].

3. Quantization method:

A scalar quantization scheme quantizes a simple value x & assign new value to the simple x based on the quantized simple value. In other words, the watermarked sample value y is represented as follows:

$Y=q(x,D) + D / 4$ if $b =1$,

$Y=q(x,D) – D / 4$ otherwise[4]

**VIDEO:** Apparently any image watermarking technique can be extended to watermark videos, but in reality video watermarking techniques need to meet other challenges than that in image watermarking schemes such as large volume of inherently redundant data

between frames, the unbalance between the motion & motionless regions, real time requirements in the video broadcasting etc. Watermarked video sequences are very much susceptible to pirate attacks such as frame averaging, frame swapping, statistical analysis, digital- analog (AD/DA) conversion , & lossy compressions[5].

### A.3 ACCORDING TO HUMAN:

**INVISIBLE:** In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden).

**VISIBLE:** In visible watermarking, the information is visible in the picture or video. The information is text or a logo which identifies the owner of the media.

### A.4 ACCORDING TO APPLICATIONS:

**SOURCE BASED WATERMARKING:** This technique is used when owner of a document wants to distribute the document to multiple destinations with the same authentication purpose. With this method one can identify whether the received document is tempered or not.

**DESTINATION BASED WATERMARKING:** The purpose of this kind of technique is same as source based scheme but here each receiver gets unique watermark information that is embedded behind the document. Only the receiver can open the document. This method can prevent illegal reselling of the document.[18]

## B. APPLICATIONS OF DIGITAL WATERMARKING [19]

- **Copyright protection:** Digital watermarking can be used to identify & protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.
- **Copy protection:** Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks & prevent unauthorized replication of the content.
- **Digital right management:** Digital right management (DRM) can be defined as “the description, identification, trading, protecting, monitoring, and tracking of all forms of usages over tangile & intangible assets”. It concerns the management of digital rights & the enforcement of rights digitally.
- **Tamper proofing:** Digital watermarks which are fragile in nature, can be used for tamper proofing. Digital content can be embedded with fragile watermarks that get

destroyed whenever any sort of modification is made to the content. Such watermarks can be used to authenticate the content.

- **Broadcast monitoring:** Over the last few years, the number of television & radio channels delivering content has notably expanded
- **Fingerprinting:** Fingerprints are the characterstics of an object that tend to distinguish it from other small objects. As in the applications of copyright protection, the watermark for finger printing is used to trace authorized users who violate the license agreement & distribute the copyrighted material illegally.
- **Access control:** Different payment entitles the users to have different privilege on the object. It is desirable in some systems to have a copy & usage control or limit the number of times of copying. A robust watermark can be used for such purpose.
- **Media forensics:** Forensic watermark applications enhance a content owner's ability to detect & respond to misuse of assets. Forensic watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner & the people or companies with which it shares its contents.
- **Improved auditing:** Media content of all types- television, music, movies, etc. – continues to proliferate & makes its way onto many new consumer devices as well as many sites across the internet. Digital watermarking applications for auditing give all members within the value chain the ability to verify usage to support highly accurate billing & contract enforcement.

## C. CHALLENGES & LIMITATIONS OF DIGITAL WATERMARKING:

There are various technical challenges in watermarking research. The robustness & imperceptibility trade-off makes the research quite interesting. To attain imperceptibility, the watermark should be added to the high frequency components of the orignal signal. On the other hand, for robustness the watermark can be added to the low frequency components of the orignal signals are used as the host for watermark insertion. In this section, we discuss the various technical issues related to watermarking, such as properties of the human visual system & spread – spectrum communication, which are commonly exploited for making watermarking schemes successful. [13]

## References:

[1].Lalit kumar Saini, Vishal Shrivastava- A Survey of Digital Watermarking Techniques and its Applications, Volume 2, Issue 3, May-Jun 2014.

[2]. Prof. Vishal Shinde, Yogesh Ojha, Mitesh Bhanushali, Vaibahv More,- Image Processing Using Watermarking (Text, Image, Audio, Video), March 2016.

[3]. Pooja Yadav, Nishchol Mishra, and Sanjeev Sharma," A Secure Video Steganography with Encryption Based on LSB Technique ", 2013 IEEE International Conference on Computational Intelligence and Computing Research.

[4]. L. Robert, T.Shanmugapriya, "A Study on Digital Watermarking Techniques," International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[5].Vijay Kumar Sharma, Vishal Shrivastava, "A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1.

[6]. Mritha Ramalingam and Nor Ashidi Mat Isa, "A steganography approach for sequential data Encoding and decoding in video images", 2014 International Conference on Computer, Control, Informatics and Its Applications.

[7]. G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'‖A Review of digital image watermarking in health care.

[8]. Edin Muharemagic and Borko Furht —A Survey of watermarking techniques and application 2001.

[9]. HARLEEN KAUR- STUDY ON AUDIO AND VIDEO WATERMARKING, Volume-2, Issue-1, 2013

[10]. M. Fallahpour and D. Megias, "High capacity audio watermarking using the high frequency band of the wavelet domain," Journal Multimedia Tools and Applications, April 2011, Volume 52, Issue 2-3, pp 485-498

[11]. Fred Hatfull, "Watermarking Audio Data: A Survey And Comparison of Techniques for Audio Steganography," CASE WESTERN RESERVE UNIVERSITY, 2011, http://fredhatfull.com/media/talks/watermarking_audio/Watermarking%20Audio%20Data.pdf

[12]. Rini T Paul, "Review of Robust Video Watermarking Techniques," IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011

[13]. Manpreet kaur, Sonia Jindal, Sunny behal, —A Study of Digital image watermarking, Volume2, Issue 2, Feb 2012.

[14]. Abdelfatah A. Tamimi, Ayman M. Abdalla, Omaima Al-Allaf, "Hiding an Image inside another Image using Variable-Rate Steganography", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 10, 2013

[15]. Vijay Kumar Sharma, Vishal Shrivastava, "A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection", Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1.

[16]. Mahmoud El-Gayyari, —Watermarking Techniques Spatial Domain Digital Rights Seminar ©‖, Media Informatics University of Bonn Germany.

[17]. Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, —A Novel Technique for Digital Image Watermarking in Spatial Domain‖, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[18]. G. Bouridane. A, M. K. Ibrahim, ―Digital Image Watermarking Using Balanced Multi wavelets‖, IEEE Transaction on Signal Processing 54(4), (2006), pp. 1519-1536.

[19]. Prabhishek singh, R S Chadna,- A Survey of Digital Watermarking Techniques, Applications & Attacks, Volume 2, Issue 9, March 2013

[20]. Amit Kumar Singh, Nomit Sharma, Mayank Dave, Anand Mohan, ―A Novel Technique for Digital Image Watermarking in Spatial Domain‖, 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.