A Review Paper on Digital Watermarking Techniques

Jaspreet Kaur[1], Navneet Kaur[2] and Narwant S. Grewal[3]

[1,2,3] *Guru Nanak Dev Engineering College, ECE Department, GNDEC, Ludhiana, India*

Abstract

Digital watermarking is used to hide important data in an another data so that hidden important data is only known by receiver (RX) or only known to that person who is belonging to that data and not known by any attacker that's why this technique (tech) is also known as security based tech. This article gives prescribed description of basics of digital watermarking, classification, review of different digital watermarking methods and summary of digital watermarking in terms of their different parameters in which methods used and features related to that parameters are explained in a tabular form. Watermarking could be used with Cryptography and Steganography to increase the safe level. It is also helpful to all of the research scholars to gain knowledge about different digital watermarking techniques and their implementations in different tools or software where mostly tools used are Matlab, XSG and Xilinx Vivado which are mentioned in this review.

Keywords

Reverse Contrast Mapping (RCM), Difference Expansion (DE), Frequency Domain Transforms (FDT), Xilinx System Generator (XSG), Matrix Laboratory (MATLAB).

1. Introduction

Watermark is in an image or text form printed on any paper. Video watermarking needs real time detection for compression. Sound watermarking take in internet tunes. Text watermarking is embedded in a text shape and area b/w text and line spaces. Graphic watermarking performs insertion to 2D or 3D graphics [1].Visible watermarking is seen by the observer. In Invisible Watermarking modifications to the pixel values are not observed. Dual Watermarking is that where invisible is a holdup of visible. Digital Watermarking is used for broadcast testing, thumb prints [2] [3]. Inputs (I/Ps) are watermark, secret information; public or private key for safety and watermarked output (O/P) is sent to human being and that human being creates an alteration is called as an attack. Robustness or interference attacks destroys watermark-cropping, JPG Compression, AWGN, quantization, rotation, collusion, demodulation, averaging. In Presentation attack, affine alteration, variation of aspect ratio, translation, scaling, rotation, geometric transformation comes under extraction failure. Counterfeiting attack creates fake data by manipulating the real data. Geometric hacks are image geometric transformations-row- column blanking, translation, warping, scaling, cropping, and rotation. Signal processing or non-geometric hacks-image compression, Distortion- Gaussian noise, gamma correction, filtering, brightness, sharpening, histogram equalization, averaging, collusion, printing, scanning [3]. Collusion hack is a no of licensed RXs to create an real data by averaging all watermarked data [2]. Cryptographic hacks break the privacy by computing the private key with exhaustive brute force way [10]. Protocol hacks ends the gaps in the watermarking-IBM hack (deadlock or inversion or counterfeiting hacks) inserts1or more watermarks that are not clear which the watermark of the real vender was[2], then technique applied to the hacked data to extract the

International Conference on Emerging Technologies: AI, IoT, and CPS for Science & Technology Applications, September 06–07, 2021, NITTTR Chandigarh, India

EMAIL: jaspreetldh147@gmail.com (A. 1); navneetKaur@gndec.ac.in (A. 2); ernarwant@gmail.com (A. 3)

ORCID: 0000-0003-4958-9226 (A. 1); 0000-0003-0515-2698 (A. 2); 0000-0002-8295-7118 (A. 3)

watermark from it. I/Ps are watermarked, private or public key and O/P is an original data.

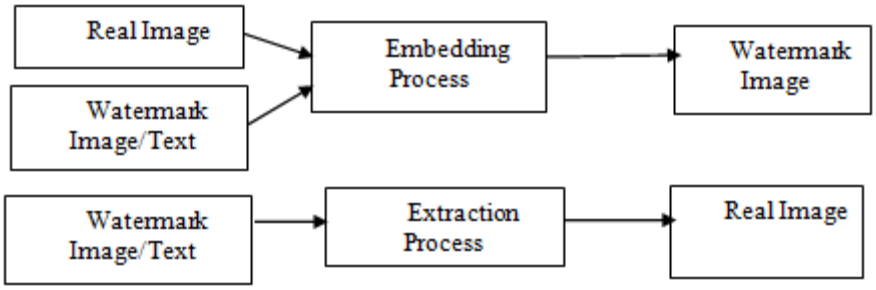

Figure 1: Watermarking Embedding and Extraction system [1].

2. Classification

Capacity-The note is 0 bit to extract the existence or non-existence is named as 0 bit or existing watermarking. If a note is n-bit and is controlled in the watermark called as multiple or non-zero bit watermarking. Estimation and Benchmarking-The assessment of watermarking methods give described data for planners cameras have safety specifications adds noise to the real image.

1. Semi fragile watermarking aids little bit change to a watermarked data [1].
2. Spatial domain watermarking stores the information to the pixels value. [1].In Frequency domain, particular frequencies are changed from their real image [1].
3. In visual or private watermarking, real matter is needed [1]. In Semi blind or semi-private watermarking, the real information is not needed for extraction [1].
4. In Source-based, a dissimilar watermark linking to vendor is defined to all the distributed image copies[1].In Destination based, watermark is to track down the buyer in the state of unlicensed reselling [1]

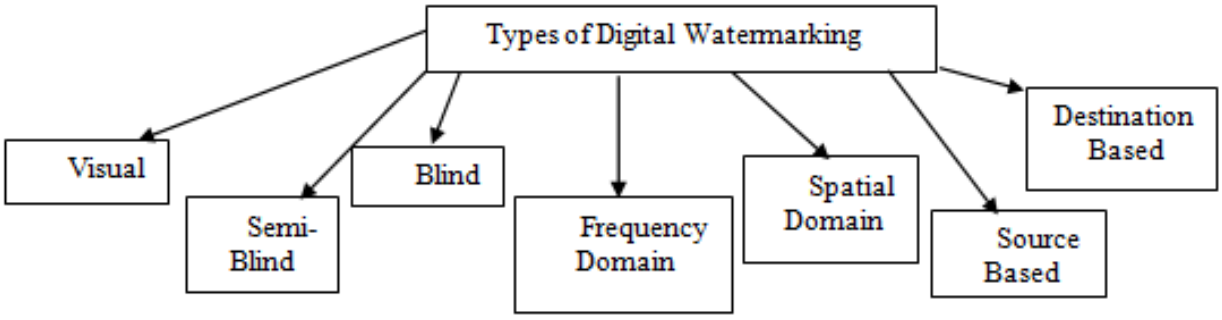

Figure 2: Classification of Digital Watermarking Techniques

3. Review on Digital Watermarking

Diverse uses where watermarking needed [1].The watermark is unaffected as it is transparent [3]. DWT is well due to zero tree wavelet image compression and max. Frequency sub bands [5]. An image has been encoded with large private key by turning pixel bits by XOR then in steganography it has been modified by LSBs of the secret and stego image, then stego image has been watermarked in the time and frequency domain.[6][7].Optical watermarking take merit so f parallel high-speed processing and multi-dimensional compared to digital methods. The techniques for inserting the optical O/P to a host image are Double Random Phase Encoding, off axis and phase shifting holography, optimized phase- only mask, Joint Transform Correlate, ghost imaging, ptychography. [9]. Diverse sorts where watermarking needed [10]. RC Miscarry out in MATLAB and O/ Pison ZEDBOARD [11].All images of gray I/P video are verified in tool. O/P video is at

OV7670 Camera with ZEDBOARD [12]. It was applied on 2 images to find its contrast enhancement by 2 peaks (i.e. the max. 2 bins) in a histogram are chosen and put it to the medical and satellite images for the superior visibility, will be shown in future [13]. The quantity of change can be organized by a factor modulation index selects the value of cover and extraction (LSB). A PN code embeds and extracts watermark, Procedure has been estimated by many test images and IQA metrics along with some hacks. FPGA and ASIC have been estimate din terms of resources used, area, speed and power but throughput is so high for video applications [14]. HLS with resource design needs only +, -, *, divider with 20 registers and 14 MUXs. SSIM RIW of MATLAB is compared with the SSIM hardware [16]. For PN watermark to a real data (mutual exclusive) parameter, then create it public. The writers integrates data integrity and a sole features of VLSI blocks stays friendly by a constraint watermarking and uses VLSI CAD problems-mapping, partitioning, graph coloring, FPGA design, and Boolean discovers a public watermarks, a public– private watermarking way agrees an IP's invention to recognize simply and publicly, old constraint watermark as secret part and public–private watermarking is of public extractability by no ruin on a watermark [17]. Later gaining a local contrast quality map and a global VS quality map then sum up a standard deviation together to gain a final quality score. An outcomes of 3 level files (LIVE, TID2008, and CSIQ) finds that project does well for visual quality and compared with IQA and is only designed for gray images [20]. A Spartan-3A DSP edition board (XC3SD3400A4FGG676C) is used and an O/P through XSG [21]. A noticeable Stochastic Resonance uses detection in very low signal- distortion [23]. A watermarking of large-size images at Huawei cloud then split a method in 2 sorts: tool work area and hardware work area, watermarks crambling is treated by CPU, and the varied skill under OpenCL style. The size for DCT and a bulk for DCT kernel are the main to reach the max. Functionality. The Stirmark tool is used to check the robustness of the watermarking [19][24].

Table 1
Summary of Digital Watermarking in terms of PSNR, SSIM, QOS, Latency, efficiency Throughput,Critical path.

Ref. ID	Features	Method used
[11]	Real-time, Min. price, High	RCM DE
[16]	Rapidity, Reduces complexity.	LSB and Reverse non-
[21]	Real-time, Min. price, High	blind method
[22]	Rapidity, high performance.	DWT DCT/IDCT DCT
[26]	Improves design efficiency,	RCM (Histogram bin
[27]	development time and cost, less	shifting).
[33]	complexity.	
	Good Robustness and performance in terms of operating speed.	
	Good performance and robustness, Reduces complexity, real-time and improves throughput and hardware efficiency.	
	Less power consumption and high performance.	
	Min. price, easy scheme, re-configurability. Real time use, less distortion, more secure, high speed	

Table 2
Summary of Digital Watermarking in terms of Robustness, efficiency, SSIM, BER.

Ref. ID	Features	Method used
[3]	Robust watermarking schemes.	DWT
[25]	Enhances Robustness, Imperceptibility and BER.	DCT Blind Watermarking IDCT and Faraday 0.18 micrometer CMOS Technology 3.35~4 CMOS Technology 40nm Cu CMOS Technology
[31]	Flexible, simple, real-time use, High speed, improves performance and robustness.	
[36]	Less power, high performance, reliability.	
[37]	Efficient in terms of area, power and performance.	

Table 3
Summary of Digital Watermarking in terms of Resolution

Ref. ID	Features	Method used
[12]	High speed, Low cost, Real-time use, high performance and consumes less power to reduce shortcomings of RCM. Highly extensible, widely shareable, secure and highest processing speed and high performance. Real-time use, consumes less power, very high throughput and max. Operating frequency, highly efficient and good robustness. Less complexity, High speed. Real-time use, Increases embedding rate and less visual distortion.	RCM for 640 x 480 Resolution image.
[24]		DCT (800 X 800) Color Image Resolution.
[30]		DWT (Adaptive Dither Modulation Technique) for 512 x 512 Resolution images.
[34]		DFWH for 256 x 256 Resolution image.
[35]		RCM for 512 x 512 and 256 x 256 Resolution images.

4. Conclusion

In the nut shell, it is concluded that digital watermarking issued to hide important data in another data so that hidden important data is only known by RX or only known to that person who is belonging to that data and not known by any attacker .This paper gives prescribed description of basics of digital watermarking, classification and review of different digital watermarking methods and summary of digital watermarking in terms of their different parameters in which methods used and features related to that parameters are explained in a tabular form. The future of Digital Watermarking is bright as a review provides data related to digital watermarking which can be helpful in gaining knowledge for further research in this field. Batch and cloud processing in image is implemented and RCM is further implemented by an interpolation technique in a future in order to meet the IQA parameters.

5. References

[1] Patel Ruchika, Bhatt Parth, a Review Paper on Digital Watermarking and its Techniques, International journal of computer applications (2015) 0975-8887 Vol. 110,No.01.

[2] Manpreet Kaur, Jindal Sonika, Behal Sunny, A Study of Digital Image Watermarking,(IJREAS) International journal of research in engineering and applied sciences (2012) 2249- 3905,Vol.02.

[3] Jabade.SVaishali, Dr. Gengaje.R Sachin, Literature Review of Wavelet Based Digital Image Watermarking Techniques, International Journal of Computer Applications (2011) 0975 – 8887 Vol. 03, No. 01.

[4] Nasereddin H.O. Hebah, Digital Watermarkinga Technology Overview,(IJRRAS), (2011)Vol. 06.

[5] Mistry Darshana,Comparison of Digital Water Marking methods,(IJCSE) International Journal on Computer Science and Engineering (2010) 2905-2909 Vol. 02, No. 09.

[6] Yousuf Farah Qasim, Din Roshidi, Review on secured data capabilities of cryptography, steganography, and watermarking domain, Indonesian Journal of Electrical engineering and computer science (2019) 2502-4752, Vol. 17, No.02.

[7] Mirza AbdurRazzaq Mirza Adnan BaigRiaz Ahmed Shaikh Ashfaque Ahmed Memon, Digital Image Security: Fusion of Encryption, Steganography and Watermarking, (IJACSA) International journal of advanced computer science and applications (2017) Vol. 08, No.05.

[8] Jain Deepika (2021), Digital Watermarking Technology – A Review, Gorteria Journal (2021) 0017-2294 Vol.34.

[9] Jiao Shuming, Zhoua Changyuan, ShibYishi, ZouaWenbin,LiaXia,Review on optical image hiding and watermarking techniques, Optics and laser technology109 (2018)370-380.

[10] Ensaf Hussein Mohamed A.Belal, Digital Watermarking Techniques,Applications and Attacks Applied to Digital Media: A Survey, (IJERT) International journal of Engineering Research and Technology (2012) 2278-0181, Vol.01.

[11] Das Subhajit, Kumar Arun, Sunaniya, Maity Reshmi , and Maity Niladri Pratap, Parallel hardware implementation of an efficient embedding bitrate control based contrast mapping algorithm for reversible invisible watermarking, IEEE (2020) 69072-69095, Vol.08.

[12] Das Subhajit , Kumar Arun, Sunaniya , MaityReshmi , Maity Niladri Pratap , Efficient FPGA implementation of corrected reversible contrast mapping algorithm for video watermarking, Elsevier Journal(2020).

[13] Hao-Tian Wu, Jean-Luc Dugelay and Yun-Qing Shi, Reversible Image Data Hiding with Contrast Enhancement, IEEE Signal processing letters (2015) 81-85, Vol. 22, No.1.

[14] Shivdeep, Ghosh Sudip, Rahaman Hafizur, A New Digital Colour Image Watermarking Algorithm with its FPGA and ASIC Implementation, IEEE, (2020)978-1-7281-6564-6/20/.

[15] Das Subhajit, Singh Pragati , Koley Chaitali, Hardware implementation of adaptive feedback based reversible image watermarking for image processing application, Springer-Verlag GmbH Germany, part of Springer Nature (2018).

[16] Das Subhajit ,MaityReshmi, Maity N. P, VLSI-Based Pipeline Architecture for Reversible Image Watermarking by Difference Expansion with High-Level Synthesis Approach, Springer Science+ Business Media(2017).

[17] Qu Gang, Publicly Detectable Watermarking for Intellectual Property Authentication in VLSI Design, IEEE transactions on computer aided design Of Integrated circuits and systems (2002) 1363- 1368,Vol. 21,No.11.

[18] Zhang Jiliang and Liu Lele, Publicly Verifiable Watermarking for Intellectual Property Protection in FPGA Design, IEEE transactionson Very Large Scale Integration Systems (VLSI)(2017).

[19] Cao Yanpeng, Yu Feng and Tang Yongming, a Digital Watermarking Encryption Technique Based on FPGA Cloud Accelerator, IEEE, (2019) Vol.XX.

[20] JA Huizhen, Zhang Lu, and Wang Tonghan, Contrast and Visual Saliency Similarity-Induced Index for Assessing Image Quality, IEEE (2018) 65885-65893, Vol. 06.

[21] Sinha Roy Subhrajit&Basu Abhishek & Chattopadhyay Avik& Das TirthaSankar,

Implementation of image copyright protection tool using hardware-software co-simulation, Springer Science + Business Media, LLC, part of Springer Nature(2020).

[22] Hajjaji Mohamed Ali ,Gafsi Mohamed, Abdelali Abdessalem Ben, and Mtibaal Abdellatif, FPGA Implementation of Digital Images Watermarking System Based on Discrete Haar Wavelet Transform, Hindawi Security and communication Networks, (2019)17 pages, Vol.2019.

[23] Lanfranco.S. Mazzini .L. H., Dominguez. A. E and Naguil .J. L., Watermark Detector Based on Stochastic Resonance Phenomenon, IEEE latin America transactions (2013)396-401.

[24] Cao Yanpeng, Yu Feng and Tang Yongming (2019), a Digital Watermarking Encryption Technique Based on FPGA Cloud Accelerator, IEEE, Vol.XX