RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
Vol. 05, Issue 01 January
www.rspsciencehub.com

Check for updates

http://dx.doi.org/10.47392/irjash.2023.002

# An Overview on Research Trends, Challenges, Applications and Future Direction in Digital Image Watermarking

*Pavan A C* [1], *M T Somashekara* [2]

[1] *Research Scholar, Department of Computer Science and Applications, Bangalore University, Bangalore, India*

[2] *Associate Professor, Department of Computer Science and Applications, Bangalore University, Bangalore, India*

Emails: shyam2712.pavan@gmail.com, somashekar_mt@hotmail.com

## Article History

*Received: 20 December 2022*
*Accepted: 22 January 2023*

## Keywords:

*Digital image Watermarking;*
*Tamper Detection;*
*Visual Imperceptibility;*
*Robustness*

## Abstract

*Digital data including photographs, audio, and video are now readily available because to the development of the Internet. The ease of access to multimedia raises concerns about ownership identification, authentication of content, security, and copyright protection. Here, we talk about the idea of digital picture watermarking with an emphasis on the method utilized for embedding and extracting the watermark from images. This paper also presents a complete classification of digital watermarking along with its fundamental properties, such as visual imperceptibility, resilience, capacity, and security. Additionally, we have covered the most recent uses of digital watermarking in the fields of healthcare, distance learning, electronic voting, and the military. The robustness is assessed by looking at how image processing assaults affect the content that is signed and the recoverability of the watermark. The thorough survey that is offered in this study, in the opinion of the authors, will aid brand-new scholars in learning more about this area. Additionally, the comparative study can spark suggestions for how to enhance the methods already outlined.*

## 1. Introduction

The ability to gather information is the key to an organization's success in the modern day. How well it can prevent other users from accessing and modifying the information produced by its operations and processes is also a cause for concern. The ease of access to digital storage devices, as well as the Internet's widespread use, has made it simple to produce and distribute digital material. This has made it imperative to create strategies for combating copyright violations (C. Kumar, A. K. Singh, and P. Kumar P. Singh and Chadha).

Digital watermarking is a widely used approach in cases where an organisation needs to prevent data from leaking into the public domain. When a business has a direct fiduciary relationship with its customers and is required to protect their information as well, it is absolutely essential (C. Kumar, A. K. Singh, and P. Kumar). Digital watermarking is a technique to offer defence against any modification or tampering (S. Kumar, B. K. Singh, and Yadav Cox et al. S. Kumar and Dutta). It protects digital content and authenticates users. Signal information is inserted into the original media content as part of the digital watermarking process. In order to identify the true owner of the digital media, the implanted information is then discovered and removed. The process of watermarking entails incorporating watermark, digital signature, or label data into the digital medium. You can extract this watermark to show the media object's legitimacy (Abraham and Paul). We can visualise a recognisable ”seal” over an image as an illustration of a watermark.

There are three basic parts of digital watermarking algorithm: -

1. Creating Watermark
2. An Encoding algorithm
3. A decoding algorithm (C. Kumar, A. K. Singh, and P. Kumar Y. Liu et al. A. K. Singh et al.).

This method can be applied for confidential communication, copyright protection, embedding fingerprints for data integrity checks, and placing authentication. Tracing illicit users so that the owner can contact regulatory authorities is another significant application of watermarking technology. It can be helpful to make sure that information about the individuals who purchase and sell digital material is recorded for each transaction. For the purpose of preventing violations of copyright, this data can be tracked further. In fact, this unauthorised dissemination of digital content requires the implementation of rigorous restrictions. The paper is organised as follows: Section 2 classifies digital watermarking according to a number of factors. The salient characteristics of digital watermarking are described in Section 3. The most recent fields of watermarking application are covered in Section 4. The many sorts of attacks are presented in Section 5. The key findings and outcomes of related research by various authors are examined in section 6, and the conclusions and potential future applications of image watermarking are presented in section 7.

## 2. Digital Watermarking Classifications

This aspect of paper describes the categorization of digital watermarking which is based on some of the criteria (Pavan and Somashekara) like robustness, perceptibility, area, and multimedia detection technique. We will also discuss the many widely used watermarking techniques in the next section.

### *2.1. Based on Characteristics/Robustness*

Robust: When copyright information must be incorporated, strong watermarking is suggested. If the watermarked image survives an attack undisturbed, this shows robustness. It is resistant to numerous assaults. It is evident that a strong watermark is useful for copyright protection.

Fragile: If the data has been altered, it is simple to determine from the watermark’s condition. This watermark is the best option for integrity protection.

Semi-fragile: A semi-fragile watermark is tolerant of some degree of modification (P. Singh and Chadha S. Kumar, B. K. Singh, and Yadav Abraham and Paul).

### *2.2. Based on Perceptibility*

Perceptible: Perceptible refers to a visible watermark.

Imperceptible: Imperceptible watermark is the phrase used to describe a watermark that cannot be seen. This prevents the visibility of information that is hidden within the image. In these circumstances, a barely discernible watermark can be used to demonstrate ownership of the image (P. Singh and Chadha A. Dixit and R. Dixit).

### *2.3. Based on Domain*

Frequency: Before anything further, the image is converted to the frequency domain. Different transformation techniques, including DCT, DFT, and DWT, are used in this type of watermarking (Sherekar, Thakare, and Jain).

Spatial: The watermark is injected into the host image, and watermarking in this context modifies the value of pixels in randomly chosen areas of images. In the spatial domain, no transformation or conversion is used. Some of the well-liked spatial domain-based approaches include LSB, Patchwork method, and SSM Modulation (P. Singh and Chadha S. Kumar, B. K. Singh, and Yadav). In general, watermarking done in the frequency domain is more reliable than watermarking done in the spatial domain.

### *2.4. Spatial Domain*

Method of Least Significant Bit (LSB):

The watermark is put using this technique in the image’s pixels’ least significant bit (LSB). The best method for embedding is either of the two. One method substitutes a pseudo-noise (PN) sequence for the LSB of an image, while another method adds the PN sequencing to the LSB. Although the LSB approach is simple to implement, it sacrifices robustness against attacks.

Method of Patchwork:

Patchwork technique selects n pairings of picture points at random (x, y). Data is darkened in the y region and lightened in the x region. Although this approach may endure numerous assaults, it is not very powerful.

### 2.5. *Frequency Domain*

Discrete cosine transforms (DCT):

The methodology used in this method involves separating a picture signal into non-overlapping blocks of size 8 8 pixels. Following the completion of block-wise DCT, the coefficients to be watermarked are selected. To obtain the signed picture, an inverse of DCT is then performed to each 8x8 block.

Discrete wavelets transform (DWT):

This technique involves applying a series of low and high-pass filters on the image. The decomposition of an image into four equal subbands includes horizontal features, low frequency (LL), diagonal and vertical features (HL) in each subband (HH). Because it offers a reliable and safe watermarking method, it is a favoured algorithm (P. Singh and Chadha S. Kumar, B. K. Singh, and Yadav Sherekar, Thakare, and Jain).

### 2.6. *Based on the Process of Detection*

Blind: These watermarking techniques fall into this category, and all that is needed to remove the embedded data is the watermarked image. Applications for it include copyright protection, voting, and other things (Agarwal, A. K. Singh, and P. K. Singh).

Non-Blind: In such kind of watermarking, the procedure duplicates the watermark with the text data, the image, and the added data. Copyright protection is one area where it is used (Agarwal, A. K. Singh, and P. K. Singh).

### 2.7. *Based on Multimedia*

Words, punctuation, phrases, and other elements make up text watermarking. One of these components undergoes transformation, and the result watermark is embedded (S. Kumar, B. K. Singh, and Yadav). Large-size photographs must be watermarked, which is accomplished by image watermarking. We demand strong watermarks on photographs that should be undetectable (S. Kumar, B. K. Singh, and Yadav). Video watermarking: In this situation, getting an undetectable watermark is challenging. Graphic Watermarking: A watermark is incorporated into 2D or 3D digital graphics. It offers copyright defence.

## 3. Some of the Characteristics of Digital Watermarking

Here, few aspects of digital watermarking are mentioned:-

Robustness: The digital watermark can withstand various processing activities and attacks, according to the robustness characteristic. After that, it is regarded as robust (S. Liu, Pan, and H. Song).

Imperceptibility: The feature of imperceptibility states that a watermarked image should not be perceptible to the human eye. The embedded watermark shouldn’t be visible. Only specialist procedures can detect it. The act of embedding a watermark should be done in a way that preserves the integrity of the material and ensures that the viewer cannot see the watermark (S. Liu, Pan, and H. Song).

Security: According to the security function, the embedded digital watermark cannot be deleted, even in the event of targeted attacks. According to watermark security, it should be difficult to change or remove a watermark without doing any harm to the host signal. Data ownership, protection, and confidentiality can all be achieved by watermarking security (P. Singh and Chadha). Data payload or capacity refers to the volume of information included within a watermarked image (S. Kumar, B. K. Singh, and Yadav).

Verifiability: Using the watermark, we ought to be able to obtain some proof of who owns copyright-protected data. This assists in determining the legitimacy of any digital data and even in restricting unauthorised copying of it (Su, Yuan, and D. Liu).

## 4. Few Recent Watermarking Applications

As we are all aware, photos are freely available on the internet and may be simply distributed. Commercial usage of these photos is permitted. Data must therefore be protected by copyright, and digital watermarking is highly helpful in this regard. To determine who owns the copyright, a digital watermark will be inserted (P. Singh and Chadha Agarwal, A. K. Singh, and P. K. Singh). Digital watermarking using a fingerprint may be suggested as a way to embed some individuality. It should be tough to modify the fingerprint. The data entered is associated with the customer. This fingerprinting reveal which authorised consumers are participating in the distribution of copyright data in violation of the contract (P. Singh and Chadha Sherekar, Thakare, and

Jain). Digital watermarking can be used to stop the unauthorised reproduction of digital data. Devices that perform replication are able to recognise these watermarks, report instances of copying, and so prevent unauthorised copying (S. Kumar, B. K. Singh, and Yadav A. Dixit and R. Dixit).

Broadcast Monitoring: It has been increasingly easier and more common to access and find media content throughout time. The information is also accessible online. In these circumstances, it is crucial for content owners and copyright holders to be aware of the actual content distributor. Here, digital watermarking is crucial (S. Kumar, B. K. Singh, and Yadav A. Dixit and R. Dixit).

Medical Application: Visible watermarking can be used to embed the patient's name in the reports from an MRI, CT, or X-ray scan. These medical reports determine how the patient will be treated. Thus, visible watermarking is a technique that can be utilised to prevent report mixing (Agarwal, A. K. Singh, and P. K. Singh).

Electronic voting system: From large cities to tiny communities, the Internet is now widely used throughout the nation. Elections are carried out with the assistance of electronic voting while taking security into account (Agarwal, A. K. Singh, and P. K. Singh).

Remote Education: In small settlements, a teacher shortage is a major issue. Distance learning requires the use of smart technology. In this instance, watermarking contributes to the reliable transmission of educational content via the internet (Agarwal, A. K. Singh, and P. K. Singh Sherekar, Thakare, and Jain).

## 5. Attacks on Watermarking

The assault resistance of a watermarking technology is a constant criterion for evaluation. Operations on any watermark are conducted to disable the watermark that has been implanted or make it more challenging for users to locate the watermark. Any assault aims to undermine the security that digital content receives from a watermark. Watermarking attacks fall into four categories: protocol attack, cryptographic attack, geometry attack and removal attack (Sanjay and Dutta C. Song et al. Voloshynovskiy et al.).

**Geometry Attack:** This type of processing applies to the watermark image and modifies its geometry by rotation, cropping, and other techniques. Additional categories for these include cropping, scaling, translation, and rotation (Abraham and Paul).

**Assault for Data Removal:** This attack seeks to delete the added information from the digital image. If it is unable to, they nonetheless attempt to destroy the contained data (Su, Yuan, and D. Liu). Assaults that fall within this category, known as protocol attacks, do not harm embedded data. There are two different kinds of Protocol assaults: Invertible and Copy attacks. A watermark should therefore be non-invertible and uncopyable. The watermark can be reverse if the attacker deletes their particular watermark from the host image. The attacker then impersonates the data's owner. This demonstrates that non-invertible watermarks are necessary for copyright protection (Vaidya and Pvssr Su, Yuan, and D. Liu).

**Copy Attack:** This type of attack Protocols also exists. The watermark is not removed in this either. The attacker instead makes an estimate of the watermark using host data. Then it is copied to additional data (Vaidya and Pvssr). Attacks that compromise the security of watermarking methods fall under the category of cryptographic attacks. With this, they can either extract the watermark data that was added or add a shady watermark. This includes the Brute-force and Oracle assaults (Su, Yuan, and D. Liu). In order to give a thorough analysis of picture watermarking, we assembled a collection of a few publications, some of which served to establish the history of digital watermarking and others of which were considered to be pertinent to the topic. Table 1 lists the watermarking plans put out by different research teams over the past few years after conducting a comparative analysis.

The table includes a review and evaluation of earlier work on digital watermarking methods. Some of the common strategies that have been previously investigated include the spatial domain and frequency domain techniques. Furthermore, it has been discovered that image pixels digital watermarking is less trustworthy and hence less common. The watermarked image's performance is assessed using its capacity, security, imperceptibility, and robustness. These were the most preferred criteria because they included the watermarked image's visual imperceptibility and the watermarking's durability. In fact, future work has the potential to combine techniques

**TABLE 1.** Summary of various Watermarking Schemes

| Research group | Title | Technique used | Input | Visual Imperceptibility | Robustness |
|---|---|---|---|---|---|
| Abraham and Paul [6] | ”An imperceptible spatial domain color image watermarking scheme” | Spatial domain Simple Image Region Detector (SIRD): Estimation of most suitable portion within the block of an image. | Cover image Colored image of Size: 512 X 512 X 3 pixels Watermark Size: 64 X 64 pixels | PSNR = 47.6 dB SSIM = 0.9904 | NCC = Range [0.9917 - 1] BER= Range [0.7500-0] Attacks considered: Salt and Pepper, Poisson, Speckle, average filtering, Gaussian LPF, Sharpening, JPEG Compression, Cropping, Resizing |
| Liu et al. [15] | ”Digital image watermarking method based on DCT and fractal encoding” | Fractal encoding and DCT method are combined for double encryption for embedding purpose. | Cover image Size: 1024 X 1024 pixels Watermark Size: 256 X 256 pixels | PSNR Range=[41-45 ] dB | Attacks Considered: white noise attack, Gaussian filter attack, JPEG compression attack. |
| Moosaza deh and Ekbatanif ard [17] | ”A new DCT-based robust image watermarking method using teachinglearning-Based optimization” | Image watermarking scheme based on DCT Teaching-Learning- Based Optimization (TLBO): Automatic detection of embedding parameters and suitable position for inserting the watermark. | Cover image Size: 512 X 512 pixels Watermark Size: 32 X 32 pixels | PSNR= Range[39.95-40.73] | NCC = Range [0.7871-0.9901] Attacks considered : Salt & pepper noise, Uniform noise, Poisson noise, Gaussian noise, Scaling, Rotation, Cropping, Sharpening, Motion Filter, Disk filter, Wiener, Median filter, Gaussian Filter, JPEG compression |
| Ambadek ar et al.[24] | ”Digital Image Watermarking Through Encryption and DWT for Copyright Protection” | DWT and encryption-based watermarking. | Cover Image Size: 228 x 228 Pixels Watermark Size: grayscale image 90 x 90 pixels | PSNR=54.96 dB | NCC=0.9749 Attacks Considered : Noise, Geometric, Compression |

and employ them in hybrid form to not only improve the durability of the watermarked image but also to mitigate the shortcomings of each methodology taken independently.

## 6. Conclusion

This article provides a general overview of digital image watermarking systems in addition to providing comprehensive classification and characteristics. The several application fields, including healthcare, distance learning, military, and electronic voting systems, have been discussed. Due to the widespread transmission of digital data, it's seen that data security has elevated to the top of the priority list. Digital watermarking is therefore employed for giving approved data or protecting sensitive data. Robustness, imperceptibility, security, and capacity are used to assess how well the watermarked photos operate. PSNR and bit-error ratio are used to examine them. It was found that the favoured criterion was robustness. For the purposes of content authentication and ownership evidence, invisible watermarking is used. Research teams have used frequency domain methods and made an effort to strike a balance between visual imperceptibility and resilience. In this essay, we examine numerous watermarking techniques applied on digital photos in the recent past.

**Authors' Note**

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the pa-per was free of plagiarism.

## References

Abraham, Jobin and Varghese Paul. "An imperceptible spatial domain color image watermarking scheme". *Journal of King Saud University - Computer and Information Sciences* 31.1 (2019): 125–133. 10.1016/j.jksuci.2016.12.004.

Agarwal, Namita, Amit Kumar Singh, and Pradeep Kumar Singh. "Survey of robust and imperceptible watermarking". *Multimedia Tools and Applications* 78.7 (2019): 8603–8633. 10.1007/s11042-018-7128-5.

Cox, I, et al. "Digital watermarking and steganography". (2007).

Dixit, A and R Dixit. "A Review on Digital Image Watermarking Techniques". *International Journal of Image, Graphics & Signal Processing* 9.4 (2017). 10.5815/ijigsp.2017.04.0.

Kumar, Chandan, Amit Kumar Singh, and Pardeep Kumar. "A recent survey on image watermarking techniques and its application in e-governance". *Multimedia Tools and Applications* 77.3 (2018): 3597–3622. 10.1007/s11042-017-5222-8.

Kumar, Sanjay and Ambar Dutta. "Performance analysis of spatial domain digital watermarking techniques". *2016 International Conference on Information Communication and Embedded Systems (ICICES)* (2016): 1–4. 10.1109/ICICES.2016.7518910.

Kumar, Sanjay, Binod Kumar Singh, and Mohit Yadav. "A Recent Survey on Multimedia and Database Watermarking". *Multimedia Tools and Applications* 79.27-28 (2020): 20149–20197. 10.1007/s11042-020-08881-y.

Liu, Shuai, Zheng Pan, and Houbing Song. "Digital image watermarking method based on DCT and fractal encoding". *IET Image Processing* 11.10 (2017): 815–821. 10.1109/RTEICT.2016.7808145.

Liu, Yang, et al. "Secure and robust digital image watermarking scheme using logistic and RSA encryption". *Expert Systems with Applications* 97 (2018): 95–105. 10.1016/j.eswa.2017.12.003.

Sanjay, Kumar and Ambar Dutta. "A study on robustness of block entropy based digital image watermarking techniques with respect to various attacks". *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (2016): 1802–1806. 10.1109/RTEICT.2016.7808145.

Sherekar, S, V Thakare, and S Jain. "Role of Digital Watermark in e-governance and ecommerce". *International Journal of Computer Science and Network Security* 8.1 (2008): 257–261.

Singh, A K, et al. "Medical Image Watermarking: Techniques and Applications. Book series on Multimedia Systems and Applications". (2017).

Singh, P and R S Chadha. “A survey of digital watermarking techniques, applications and attacks”. *International Journal of Engineering and Innovative Technology (IJEIT)* 2.9 (2013): 165–175. 10.1007/s11042-020-08881-y.

Song, Chunlin, et al. “Analysis of Digital Image Watermark Attacks”. *2010 7th IEEE Consumer Communications and Networking Conference* (2010): 1–5. 10.1109/CCNC.2010.5421631.

Su, Qingtang, Zihan Yuan, and Decheng Liu. “An Approximate Schur Decomposition-Based Spatial Domain Color Image Watermarking Method”. *IEEE Access* 7 (2019): 4358–4370.

Vaidya, P and C M Pvssr. “A robust semi-blind watermarking for color images based on multiple decompositions”. *Multimedia Tools and Applications* 76.24 (2017): 25623–25656. 10.1007/s11042-017-4355-0.

Voloshynovskiy, S, et al. “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks”. *IEEE Communications Magazine* 39.8 (2001): 118–126. 10.1109/35.940053.

**Embargo period:** The article has no embargo period.

**To cite this Article:** , Pavan A C, and M T Somashekara. “**An Overview on Research Trends, Challenges, Applications and Future Direction in Digital Image Watermarking** .” International Research Journal on Advanced Science Hub 05.01 January (2023): 08–14. http://dx.doi.org/10.47392/irjash.2023.002