PERFORMANCE EVALUATION OF VARIOUS WATERMARKING TECHNIQUES

Shikha Yadav[1] and Jeevan Bala[2]

Article History: Received: 10.05.2022 **Revised:** 15.06.2023 **Accepted:** 20.06.2023

ABSTRACT
Computerized watermarking has arisen as a possible answer for cutting-edge data copyright confirmation issues. The key assessment norms in strong watermarking tools for digital rights approval, file security, and automated intelligent media check are presented in this paper. Subtlety, security, and power are the crucial issues that drive research in vivacious watermarking plans. With the support of a couple of descriptive hypotheses recommended in the composition, this paper means to give a quintessence of lively watermarking plans in the evolving region. In the evolving region, repeat change strategies like DCT, DFT, DWT, and RDWT, are the most generally utilized methods to make strong watermarking computations. This review also covers the general construction of the copyrighting framework, continuous implementation details, features, depiction of information concealment techniques, or numerous different execution appraisal limits deemed by experts. This examination inspects and considers the presentation blueprint of a couple of states of craftsmanship accessible for good watermarking strategies.

Keywords: Digital Watermarking, Robustness, Imperceptibility

[1]Research Scholar, Computer Applications Lovely Professional University Phagwara, Punjab
shkydv@gmail.com
[2]Associate Professor, Computer Science Lovely Professional University Phagwara, Punjab
jeevan.26699@lpu.co.in
DOI: 10.31838/ecb/2023.12.si6.596

1. INTRODUCTION

The progression in the utilization of PCs, the web, and visual and sound development has made it conceivable to share progressed data everywhere. Notwithstanding, the straightforward entry and accommodation of different pictures dealing with contraptions have made it much less difficult to copy or change shared mechanized data. Thus, the issue of unlawful pantomime and adjustment of cutting-edge data has transformed into an authentic concern, provoking the improvement of systems that can save individuals' decency and authorized development privileges over shared electronic data.

Researchers have proposed a couple of information security techniques to resolve the issue of copyright protection. These systems can be named cryptography procedures and information-concealing strategies. The message is changed over into a solid configuration that can be decoded and recuperated by approved people utilizing cryptographic strategies. The huge impediment related to these procedures is that once the message is decoded, it is not generally gotten. Moreover, the course of cryptography is more intricate when contrasted with the information disguise cooperation. To act as an illustration of information-concealing methodologies, watermarking and steganography can without much of a stretch beat the imperatives of intricacy and data security present in cryptography techniques.

The problem with this strategy is that many people cannot see the appearance of a statement, making it unsuitable for most blended-media applications. The installing technique took on separating the data covering cycle as a steganography system or as a watermarking methodology. The cover thing and the watermark message should be irrelevant in steganography, yet they might be in watermarking. Watermarking methods can be evident or imperceptible, yet steganography is indistinct constantly. Considering the advantages and disadvantages of the different information security methodologies talked about above, it is sensible to presume that the computerized watermarking methodology is the most ideal decision It's appropriate for applications where patent rights or approval is a top priority.

Advanced watermarking entails embedding a few pieces of information (known as a watermark) into the original signal without interfering with its perception. Given no obvious outrageous goal, the watermark chosen could be a twofold methodology, such as a twofold logo, significant level imprint, biometric attributes of people, and so on. The installation or watermark association cycle and the watermark openness process are the two phases of a watermarking framework's development [28]. The host message, which should be blended in with the information to be used as a watermark, and the information to be used as a watermark are both required from a watermark perspective.

There are two types of watermarking for pictures: noticeable and imperceptible. Watermarks on logos, back notes, and advanced photographs are examples of visible watermarks that should be obvious to people with normal eyes. Getting rid of these watermarks, on the other hand, might be simple [1][2]. However, undetectable watermarks are encoded in a cryptic design that can only be accessed by supported users. The recovery of these watermarks required numerical estimations [29]. Watermarks of this kind are hard to see with the naked eye. Non-visible watermarks are more durable than visible ones.

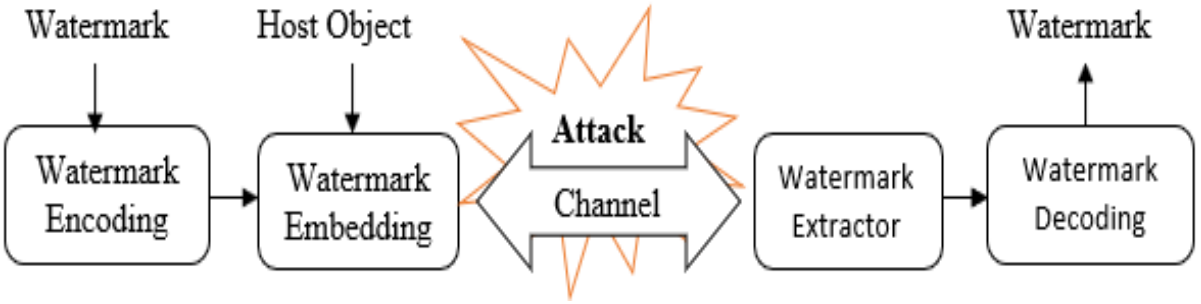

Figure 1: Watermarking Concept [36]

1.1 Watermark Process for Digital Image Security

Watermarking progressed picture is a notable strategy for safeguarding computerized pictures. It's an exceptional picture with a watermark. In the third watermarked picture, the got picture is shown.

The foundation of advanced picture watermarking is the technique for installing and extricating pictures. Without compromising the picture's apparent quality, the watermark is installed in the first picture utilizing an implanting strategy and a security key. The security key is kept hidden by the proprietor and is utilized to make the watermarked picture [13].

Components of Watermarking

i. Watermark Insertion

The watermark inserting and extraction process requires a cryptographic key, which can be either open or mysterious. The critical fills in as a safety effort, as it forestalls unapproved access [19]. The cover object is the first picture that will be watermarked. A watermark is one more picture utilized for watermarking on the cover picture. The consequence of superimposing the first picture and the watermarked picture is watermarked information.

ii. Watermark Extraction

The privileged intel is eliminated from the following watermarked picture now. The extraction cycle can be outwardly weakened, semi-blind, or non-blind depending upon the extraction assessment. The principal picture is ordinary during the non-blind extraction process, while the watermark from the following watermarked picture is taken out. During the extraction correspondence in the semi-blind cycle, the essential watermark is ordinary.

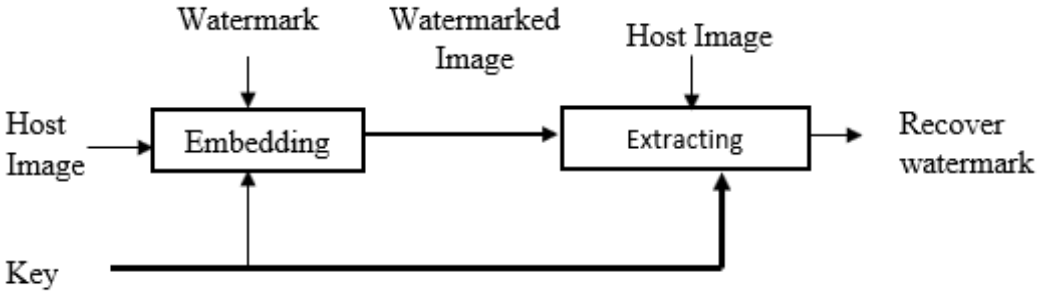

Figure 2: Embedding and extracting process of digital watermarking [38].

1.2 Classification of Watermarking Images

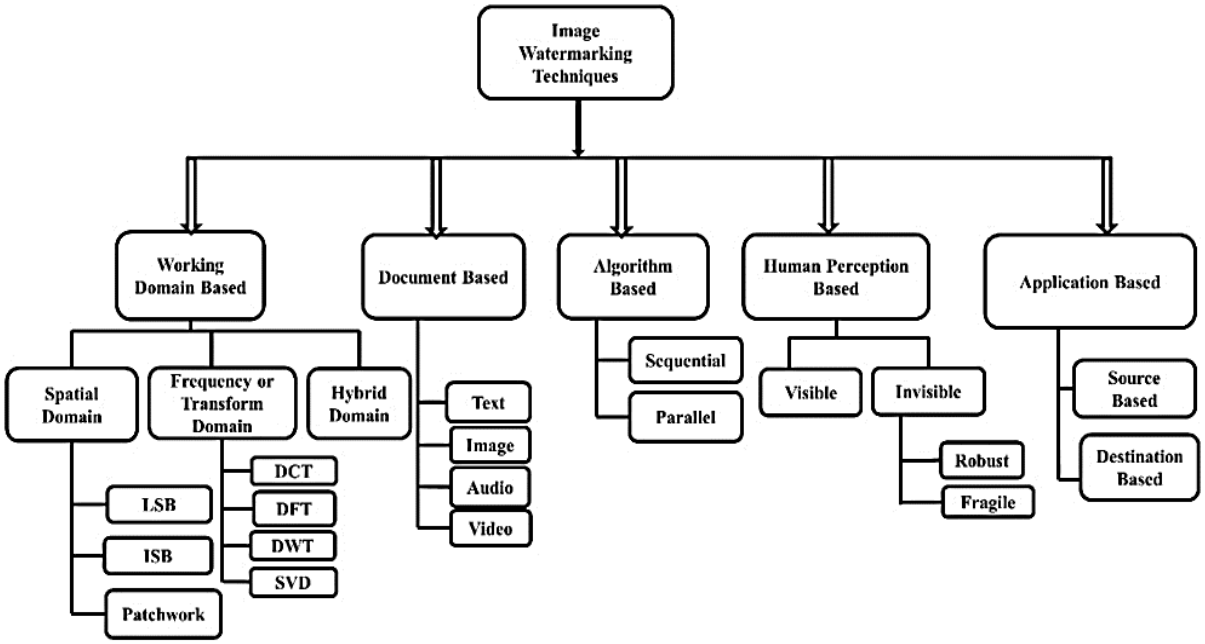

Figure 3: Flowchart of Digital Watermarking

a. According to Human Perception

i. Visible Watermarking: The contrast between noticeable and subtle watermarks is that apparent watermarks are apparent to the unaided eye, while indistinct watermarks are theoretical and can't be recognized just by checking the substance out.

ii. Invisible Watermarking: The undetectable watermarking can likewise be isolated into two sorts: vigorous and delicate watermarking. The expression "vigorous watermarking" alludes to the way that the watermark is unaffected by any unlawful changes made to the watermarked content. A delicate watermark, then again, is demolished assuming that somebody attempts to inaccurately change or alter the watermarked information. semi-delicate watermarks are lenient toward specific picture control assaults, for example, JPEG pressure yet touchy to different changes, for example, picture trimming.

b. According to the Attached Host Signal /Multimedia

i. Picture Watermarking: In picture watermarking strategies, the picture is utilized to conceal the computerized information. At the point when pictures are shared on the web, guarding them is utilized.

ii. Video Watermarking: In video watermarking, watermarks are added to video transfers to oversee video applications. Watermarking procedures for pictures have been reached out to video watermarking. Ongoing extraction and pressure vigor are expected for this technique.

iii. Sound Watermarking: MP3 has become one of the most in-vogue application fields because of web tune arrangement.

iv. Text Watermarking: The watermark is in the text style shape as well as the space between the text style and the line spaces.

c. According to Domain Watermarking

i. Spatial Domain Watermarking: In spatial region watermarking systems, the power expected gains of a few proportional to the application of a picture are straightforwardly unique to mask the watermark information. [3, 9-12]. Using a watermark bit to change the Least Significant Bits (LSBs) of the intensity values of the presenter picture [2] is the easiest way to install the watermark. Watermarking strategies are simple to implement in the spatial domain and provide a high information limit. Another advantage of this strategy if any one of the watermarks can drive forward through the assault, the purpose of watermarking is met. The spatial space methodologies are unable to overcome images dealing with assaults such as JPEG compression and commotion augmentation [1, 14].It combines features such as sound reduction and picture management. The Least Significant Bit estimation is a popular method in spatial region watermarking. This method adjusts the pixels with the most non-basic pieces (LSB). More LSB pieces can be used for pictures in general [11].

LSB: With regards to spatial area watermarking, the most un-huge piece alteration calculation is the most well-known. The most un-critical piece (LSB) of one haphazardly picked pixel can be changed to cover the main piece (MSB) of one more for this situation. An irregular sign is delivered when a particular key is squeezed. The watermark is put on all huge pieces of the host picture and can be eliminated in much the same way. An assortment of approaches can be utilized to handle the host picture. This technique is both straightforward and compelling to carry out. The most uncritical pieces communicate less helpful data and, thus, don't influence the host picture's quality. It gives incredible perceptual straightforwardness while leaving the host picture unaffected.

Patch Work: Patchwork is a pseudo-irregular factual strategy that encodes repetitive examples with a Gaussian dispersion and inserts it undetectably into a unique picture. Two fixes, An and B, are picked aimlessly, and the picture information in the initial (A) fix is blurred, while the picture information in the second (B) fix is obscured. Non-mathematical picture modifications are more impervious to interwoven methodologies, and the interaction is autonomous of the first picture's substance. [20]

ii. **Transform Domain Watermarking:** The spatial area is exorbitantly fragile and instantly controlled by watermarking approaches. When appeared differently about repeat space estimations, these techniques are certainly less impenetrable to many sorts of attacks. These burdens unquestionably stand apart from the headway of progress region watermarking procedures, which even more cover data in the change space of a sign rather than time. This approach moves an image to the repeated space by applying a pre-described change to the picture. The watermark is then introduced by changing the change region coefficients of the main picture using various changes, for instance, the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD).

Discrete Cosine Transform (DCT): This method makes use of an invention that divides a visual sign into 8*8 non-covering units. Following that, block-wise DCT is directed, followed by the determination of watermarking coefficients. Finally, the marked image is obtained by performing a reverse DCT on each 8*8 square.

Discrete Walvet Transforms (DWT): The picture is gone through a progression of low-pass and high-pass channels in this strategy. A picture is separated into four equivalent sub-groups, every one of which incorporates low recurrence (LL), flat elements (LH), vertical highlights (HL), and corner-to-corner highlights (HH). It is a suggested approach since it gives a solid and safe watermarking arrangement. [21-22]

d. According to Detection Process

i. Visual Watermarking: Private watermarking is the best word for it. A unique substance is expected for visual watermarking. It is the most dependable watermarking approach.

ii. Semi Blind Watermarking: Semi-private watermarking is one more name for it. Unique information isn't needed for watermark discovery in this watermarking approach. The fundamental thought behind this approach is to check whether the watermark can be recognized.

iii. Blind Watermarking: Watermarking that isn't apparent to the unaided eye is alluded to as visually impaired watermarking or public watermarking. The first information as well as the inserted watermark aren't needed for this sort of watermark. This is the type of watermarking that requires the most exertion.

1.3 Characteristics of Watermarking

Advanced watermarking's key requirements can be seen as traits or elements. Various applications regularly require watermarking properties. The numerous attributes of watermarking are utilized in various ways in the application plan. Coming up next are the essential attributes/properties of watermarking.

Robustness

The image manipulation framework considered any picture and numerical pursuit, like sifting, replicating, editing, scaling, pressure, and rotational, and it should also turn either strategic or incidental with a high likelihood whether there's any quite minor change/acclimation to the picture [2-4].

Fidelity

The watermark's devotion alludes to its aversion to even the littlest alteration. The essential property of a delicate watermark is that it becomes imperceptible at whatever point it is exposed to unlawful alteration.[3]

Payload

Any watermarking system's payload is an important feature.

The term "payload" means the maximum amount of pieces that a watermarking scheme can encode except dropping the concept of significant data. [4]

Security

The watermark's security is determined by its ability to be impalpable to unapproved sides as well as its resistance to hostile attacks [2].

Imperceptibility
It determines the similarity between the presenter and watermarked images [2-4].

1.4 Watermarks Attacks

Removal Attack
A removal assault's goal is to remove the watermark information from the watermarked object. These attacks take advantage of the fact that the watermark is frequently an additional substance noise signal contained in the host signal.[5]

Geometric Attack
There are three unique kinds of mathematical assaults:

The first is a revolution assault, in which the picture's installation is turned fundamentally to annihilate the watermark separated. The subsequent method is known as the scaling assault; in this, any worth is added to each picture system. The third assault is known as the editing assault: it is a notable assault where the worth of the segment in the pixel picture is supplanted by the worth of '0' instead of the chromatic worth. The watermark's solidarity is decreased thus [23].

Joint Attack
In a joint assault, at least two assaults are aimed at a watermarked picture simultaneously to delete the watermark. This assault could incorporate obscuring, scaling, trimming, and revolution [23-24].

Protocol Attack
The assailant's goal in this attack is to ensure that the entire watermarking order is followed. The assailant claims ownership of watermark records after separating the watermark. It makes it hard to tell who actually owns the records. The invertible watermarks contain this convention attack [23]. The insights cannot be removed from the image when using a watermark that is not invertible.

Compression Attack
These days, a lot of sights and sound information, like advanced pictures, are sent through PC organizations. It is vital for preserving extra room, execution time, and data transmission. Therefore, the picture is compressed and the watermark is broken up into the picture. To safeguard photographs against accidental assaults, watermark pictures should be included in the packed structure [25]

Cryptographic Attack
In these kinds of assaults, the assaulters utilize animal power to find provisos in the primary implanting technique and delete the watermark data. Nonetheless, on the off chance that the inserting system is convoluted, these assaults can be effectively mitigated.[26][27]

Ambiguity Attack
In this assault, the aggressor has its watermark with a steady payload limit, similar to a genuine watermark. This watermark is put on the genuine picture, and the assailant claims responsibility for the picture.[21]

Collusion Attack
The attacker employs watermark templates in this attack.[22]

Through collaboration, the attacker removes the watermark from the original watermarked image using these templates. After that, the attacker inserts its data into the watermarked image and transfers it to the destination location. Also, the attacker claimed to be the owner of the modified image.

1.5 Applications of Watermarking Techniques
The following figure presents several applications of digital image watermarking such as Authentication, Tamper Detection, Media Security, Broadcast monitoring, Copyright Protection, etc., that rely on these requirements.

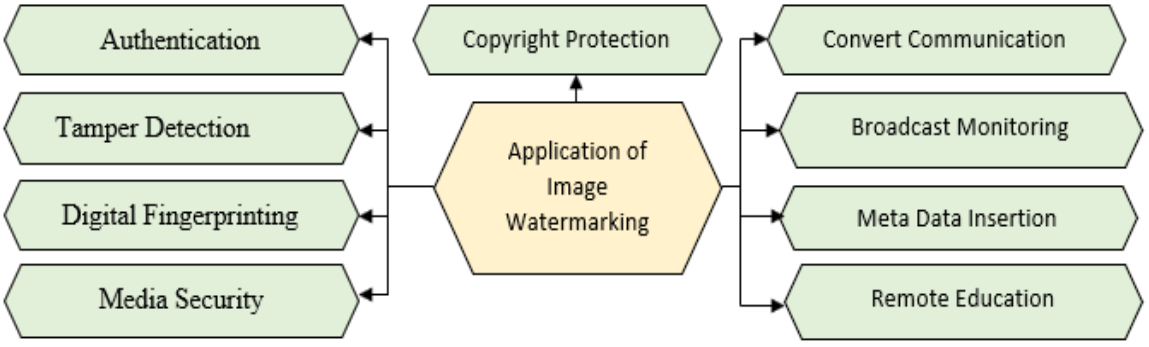

Figure 3: Applications of Watermarking [37]

2. RELATED WORK

When an assault is used on a digitally watermarked image, the image's copyright fails.

The goal of this section is to explore past work with the respective research area and work accordingly

2.1 Review of Watermarking Techniques

Narima Zermi et.al [9] proposed an outwardly debilitated watermarking approach for clinical picture security. The proposed plot keeps a fantastic, watermarked picture and remains especially incredible against a couple of standard attacks.Sharma et.al [10] moved toward clinical information as (ECG) signal. An ECG watermarking is created using repetitive discrete wavelet change (RDWT) and solitary worth deterioration (SVD).

Honsy et. Al [11] proposed an original numerous zero-watermarking strategy for clinical pictures given new symmetrical multi-channel fragmentary requests that moved Gegenbauer minutes (FrMGMs).

Mohsin et.al [12] proposed a watermarking technique for grayscale pictures, in which lifting wavelet change and particular worth deterioration are taken advantage of given multi-objective counterfeit honeybee province advancement.

Hatoum et.al [13] considered in contrast a Fully Convolutional Neural Network Denoising Attack (FCNNDA) which annihilates the watermarks while protecting the nature of the watermarked pictures. FCNNDA was likewise contrasted with different sorts of assaults to show the distinction between quality and strength. The exploratory outcomes affirmed that the FCNNDA could be viewed as a destructive assault.

Balasamy and Suganyadevi [14] concentrate on presenting a clever clinical picture watermarking strategy by fluffy-based Region of Interest (ROI) determination and wavelet change way to deal with implanting an encoded watermark. In the first place, the source picture will go through fuzzification to decide the basic focuses through the focal and last power along the spiral line. Second, the watermark picture is adjusted to the time-recurrence space through wavelet decay where sub-groups are traded given greatness esteem acquired through strategic planning. In each sub-band every one of the pixels gets traded, bringing about a completely scrambled picture that ensures the watermark to a safe, solid, and rugged structure.

Sayed Mohammad Raza Mousavi [16] a vigorous plenoptic picture watermarking has been presented given Graph-based Transform (GBT). An improvement has been utilized to observe the best chart design of GBT. Watermarking was assessed utilizing BER, SSIM, and PSNR models and Gaussian clamor assaults with differing powers.

Shahzad Alam et.al [17] proposed double security strong watermarking (DSRW) approach for picture insurance in the DWT area, which is utilized in the IoT keen layer, in light of a crossbreed improvement calculation. To make the LH and HL subbands, utilize the reallocated differential wavelet change (RI-DWT). To find the ideal module for watermark inclusion, the better feline multitude streamlining (ICSO) method was introduced to track down the picture watermark power.

Yazan Salman et.al [18] presented Depth-Image-Based-Rendering (DIBR) strategy to uphold three-dimensional pictures. To offer copyright insurance for DIBR 3D photographs, a visually impaired and the hearty computerized watermarking procedure has been introduced.

Amita Singha et.al [19] utilized crossover signals are utilized as watermarking. "Crossover" alludes to the utilization of the two pictures and sound signs as watermarks. This proposed procedure expects to expand the mystery of the correspondence between the needed gatherings by utilizing mixture signals and by conveying the watermark signals on each side of the host signal. For doing such, regular strategies DWT and SVD are utilized unexpectedly.

P.Sivananthamaitrey et.al [20] present a double watermarking approach in which a powerful and delicate watermark is embedded freely into standard and clinical pictures to lay out proprietorship characters and to track down the picture's secret adjusted regions. The repetitive coefficients procured utilizing the fixed wavelet change (SWT) help in expanding the watermark's host picture holding capacity without undermining its impalpability or vigor. The frail watermark supports figuring out where the alters are in the picture.

Soo M. Sian et al. [15] proposed that the computerized pictures' unwavering quality and fidelity be improved. Steganography, the encode and unscramble technique, and computerized picture watermarking are all used to protect images from being hacked.

2.2 Comparative Analysis of Existing Watermarking Techniques

There are various tables in this part that are categorized depending on watermarking techniques, including characteristics and robustness.

Table 1: Comparative Analysis based on their robustness

Ref	Goals	Technique Used	Input	Visual Imperceptibility	Watermarked Type	Robustness
[6]	Increased robustness and imperceptibility	DCT and GA	**Cover Image** Size: 512*512 **Watermarked** Size: 32*32	PSNR – 30.22 dB	Blind **Domain** = Spatial	NCC – Range **[0.844-1]**
[7]	to separate the visual highlight vectors of clinical pictures	SIFT and Bandelet-DCT)	**Cover Image** Size: 512*512 **Watermarked** Size: 32*32	PSNR – 34.94 dB	Non – blind **Domain**=Transform	NCC – Range **[1]**
[8]	To be more efficient in Computational Components	direct current (DC) coefficient	**Cover Image** Size: 512*512 **Watermarked** Size: 64*64	PSNR – 48.95 dB	Blind **Domain** = Spatial	NCC – Range **[1]** SSIM – 0.9856
[15]	More resistance in geometrical attacks	DC CWT, Schur Decomposition	**Cover Image** Size: 512*512 **Watermarked** Size: 32*32	PSNR – 46.764 dB	Blind **Domain** = Hybrid	NCC – Range **[0.9228-1]** SSIM – 0.9993
[16]	Retrieve data reversibly and also check the authenticity of color images	HBS+DCT	**Cover Image** Size: 512*512 **Watermarked** Size: 64*64	PSNR-56.22 dB	Fragile **Domain**= Hybrid	NCC – Range **[0.964-1]** SSIM – 0.9985
[17]	To resolve the problem of copyright protection	DC+DCT	**Cover Image** Size: 512*512/512*512	PSNR – 50.0839 dB	Blind Domain= Spatial	NCC – Range **[1]** SSIM – 0.9856
[18]	Installing the variety watermarked in the variety picture	2D DWT, SVD, Chaotic map	**Cover Image** Size: 512*512 **Watermarked** Size: 64*64	PSNR – 84.0414 dB	Blind Domain = Frequency	NCC – Range **[0.984-1]**
[28]	to check the robustness of geometrical attacks	Prime number distribution theory	**Cover Image** Size: 256*256 **Watermarked** Size: 32*32	PSNR – 41.33 dB	Fragile Domain =Spatial	NCC – Range **[1]**
[29]	Lower the complexity and improve robustness in geometrical attacks	Zero watermarking	**Cover Image** Size: 512*512 **Watermarked** Size: 64*64	PSNR – 58.098 dB	Blind Domain = Spatial	NCC – Range **[0.9954-1]** BER-[0.0007-0]
[30]	Improve the robustness of attacks	DTCWT, SVD	**Cover Image** Size: 512*512 **Watermarked** Size: 128*128/64/64	PSNR-65.075 dB	Blind Domain = Hybrid	NCC – Range **[0.9965-1]**
[31]	Improve robustness and good visuality	SVD based RGB	**Cover Image** Size: 1024*1024 **Watermarked** Size: 32*32	PSNR – 48.975 dB	Blind Domain = Frequency	CC – Range **[0.9942-1]**

[32]	Found robust and visual watermark without any distortion in attacks	DWT-DCT-SVD	**Cover Image** Size: 256*256 **Watermarked** Size: 128*128	NA	Visible Domain = Frequency	NCC – Range **[0.990-1]**
[33]	Reduced the volume of storage of fingerprint images in watermarked	2D-DCT	**Cover Image** Size: 512*512 **Watermarked** Size: 512*512	PSNR – 41 dB	Blind Domain = Frequency	NCC – Range **1** BER – Range **0**
[34]	To be more robust in tamper detection in medical images	QHIS, SD, DWT	**Cover Image** Size: 256*256 **Watermarked** Size: 64*64	PSNR – 30 dB	Blind Domain = Frequency	NCC – Range **[0.95-1]**
[35]	Understand whether the image is manipulated or not.	QR, FT	**Cover Image** Size: 512*512 **Watermarked** Size: 64*64	PSNR – 62.780 dB	Fragile Domain = Frequency	NCC – Range **[0.999-1]**

In the above table, a review of previous work in digital watermarking techniques is provided. Some popular approaches that have been studied in the past include spatial. In addition, future work might benefit from combining strategies and domain and frequency domain techniques. Furthermore, the spatial domain digital watermarking technology is less robust and hence less recommended. Robustness, imperceptibility, security, and capacity are used to evaluate the watermarked image's performance. The visual imperceptibility of the watermarked image and the robustness of the watermarking were two of the most important factors applying them in a hybrid form to improve not just the robustness of the watermarked image, but also to reduce the disadvantages of each method individually.

2.3 **Datasets**

Datasets	**No. of images**
USC-SIPI	306 images are 8 bits/pixel for black and white images, 24 bits/pixel for color images.
BOSS	10,074 images with 512*512
UCID (Uncompressed Colour Image Database)	1338 images.
HDR (High-dynamic-range)	105 images contain 14 bits image with size 4284 × 2844.

3. RESEARCH GAPS

1. Most of the research works on black and white images and watermarking extraction images have lower accuracy and robustness.
2. Color images and their watermarking apply several different algorithms, but their watermark extraction ratio is not too perfect.
3. Deep learning and FCNNDA algorithm can be used in more attacks for robustness.
4. The performance of PSNR and SSIM should be improved in deep learning models.

4. CONCLUSION

Copyright insurance and copyright validation of computerized information spread over various interpersonal organizations have now turned into a need. A few advanced watermarking strategies have been presented by analysts over these years, however, every technique is related to its upsides and downsides. This overview paper shows an exhaustive investigation of different advanced watermarking strategies consolidating change area procedures and records different benefits and disservices related to them. The general arrangement of the watermarking structure, different application locales, and required credits, alongside estimations that could be used to separate the introduction of cutting-edge watermarking, is introduced. In this paper, an outline of the change in space-based strategies accessible for computerized watermarking has been classified. With the change space strategy, this paper additionally gives a rundown of some of the late-evolved hybridized advanced watermarking strategies. This shows that the flow research pattern is towards the mixture of a few methodologies.

REFERENCES

1. Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing, 6(12), 1673–1687.
2. Kutter, M., & Petitcolas, F. A. P. (1999). The fair benchmark for image watermarking systems in security and watermarking of multimedia contents. International Society for Optics and Photonics, 3657, 226–240.
3. Cox, I. J., & Miller, M. L. (2002). The first 50 years of electronic watermarking. EURASIP Journal on Advances in Signal Processing, 2, 820936.
4. Cox, I. J., Miller, M. L., & Bloom, J. A. (2001). Digital watermarking. Chapter 5—Watermarking with Side Information (p. 2001). Amsterdam: Elsevier.
5. Alshanbari, H. S. (2021). Medical image watermarking for ownership & tamper detection. Multimedia Tools & Applications, 80(11).
6. Agarwal, N., & Singh, P. K. (2022). Discrete cosine transforms and genetic algorithm-based watermarking method for robustness and imperceptibility of color images for intelligent multimedia applications. Multimedia Tools and Applications, 1-27.
7. Fang, Y., Liu, J., Li, J., Cheng, J., Hu, J., Yi, D., ... & Bhatti, U. A. (2022). Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT. Multimedia Tools and Applications, 1-17.
8. Su, Q., Niu, Y., Wang, Q., & Sheng, G. (2013). A blind color image watermarking based on DC component in the spatial domain. Optik, 124(23), 6255-6260.
9. Nikolaidis, N., & Pitas, I. (1998). Robust image watermarking in the spatial domain. Signal Processing, 66(3), 385–403.
10. Chang, C.-C., Hwang, K.-F., & Hwang, M.-S. (2000). A digital watermarking scheme using human visual effects. Informatica (Ljubljana), 24(4), 505–511.
11. Karybali, I. G., & Berberidis, K. (2006). Efficient spatial image watermarking via new perceptual masking and blind detection schemes. IEEE Transactions on Information Forensics and security, 1(2),256–274.
12. Cheng, L.-M., Cheng, L. L., Chan, C. K., & Ng, K. W. (2004) Digital watermarking based on frequency random position insertion. In ICARCV 2004 8th Control, Automation, Robotics, and Vision Conference, 2004 (vol. 2, pp. 977–982)
13. Hatoum, M. W., Couchot, J. F., Couturier, R., & Darazi, R. (2021). Using Deep learning for image watermarking attack. Signal Processing: Image Communication, 90, 116019.
14. Wenyin, Z., & Shih, F. Y. (2011). Semi-fragile spatial watermarking based on local binary pattern operators. Optics Communication, 284(16–17), 3904–3912.
15. Liu, P., Wu, H., Luo, L., & Wang, D. S. (2022). DT CWT and Schur decomposition-based robust watermarking algorithm to geometric attacks. Multimedia Tools and Applications, 81(2), 2637-2679.
16. Hussan, M., Parah, S. A., Jan, A., & Qureshi, G. J. (2022). A Hybrid Domain Fragile Watermarking Technique for Authentication of Color Images. In Proceedings of International Conference on Computational Intelligence and Data Engineering (pp. 57-64). Springer, Singapore.
17. Su, Q., & Chen, B. (2018). Robust color image watermarking technique in the spatial domain. Soft Computing, 22(1), 91-106.
18. Wang, K., Gao, T., You, D., Wu, X., & Kan, H. (2022). A secure dual-color image watermarking scheme based on 2D DWT, SVD, and Chaotic map. Multimedia Tools and Applications, 1-32.
19. Singha, A., & Ullah, M. A. (2021). An image watermarking technique using hybrid signals as watermarks. Multimedia Systems, 27(1), 89-109.
20. Fu, G., & Peng, H. (2007). Subsampling-based wavelet watermarking algorithm using support vector regression. In The International Conference on EUROCON, 2007 Computer as a Tool.
21. Hao Li, Lianbing Deng, Zhaoquan GU, "A Robust Image Encryption Algorithm Based on a 32-bit Chaotic System", IEEE, 2020
22. Dayanand g. Savarkar, Anand Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme", Springer, Volume-S13369-019-03751-8, 2019
23. Surekha, Dr. G. N. Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January 2011.

24. Navneet Kumar Mandhani, "Watermarking Using Digital Sequences", MS thesis, Andhra University, August 2004.
25. Hao Li, Lianbing Deng, Zhaoquan GU, "A Robust Image Encryption Algorithm Based on a 32-bit Chaotic System", IEEE, 2020
26. Dayanand g. Savarkar, Anand Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme", Springer, Volume-S13369-019-03751-8, 2019
27. Zermi, N., Khaldi, A., Kafi, R., Kahlessenane, F., & Euschi, S. (2021). A DWT-SVD-based robust digital watermarking for medical image security. Forensic Science International, 320, 110691.
28. Xia, Z., Zhang, W., Duan, H., Wang, J., & Wei, X. (2022). The fragile watermarking scheme in the spatial domain is based on the prime number distribution theory. Multimedia Tools and Applications, 1-20.
29. Yang, J., Hu, K., Wang, X., Wang, H., Liu, Q., & Mao, Y. (2022). An efficient and robust zero watermarking algorithm. Multimedia Tools and Applications, 1-19.
30. Zuo, M. J., Cheng, S., & Gong, L. H. (2022). Secure and robust watermarking scheme based on the hybrid optical bi-stable model in the multi-transform domain. Multimedia Tools and Applications, 1-24.
31. Goléa, N. E. H., Seghir, R., & Benzid, R. (2010, May). A bind RGB color image watermarking based on singular value decomposition. In ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010 (pp. 1-5). IEEE.
32. Navas, K. A., Ajay, M. C., Lekshmi, M., Archana, T. S., & Sasikumar, M. (2008, January). Dwt-dct-svd based watermarking. In 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08) (pp. 271-274). IEEE.
33. Lebcir, M., Awang, S., & Benziane, A. (2022). Robust blind watermarking approach against the compression for fingerprint image using 2D-DCT. Multimedia Tools and Applications, 1-23.
34. Sanivarapu, P. V. (2022). Adaptive tamper detection watermarking scheme for medical images in the transform domain. Multimedia Tools and Applications, 81(8), 11605-11619.
35. Nejati, F., Sajedi, H., & Zohourian, A. (2022). Fragile watermarking based on QR decomposition and Fourier transform. Wireless Personal Communications, 122(1), 211-227.
36. Nematollahi, Mohammad Ali, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales. Digital watermarking. Springer Singapore, 2017.
37. Zainol, Zurinahni, Je Sen Teh, Moatsum Alawida, and Abdulatif Alabdulatif. "Hybrid SVD-based image watermarking schemes: a review." IEEE Access 9 (2021): 32931-32968.
38. Akter, Afroja, and Muhammad Ahsan Ullah. "Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm." In 2014 International Conference on Informatics, Electronics & Vision (ICIEV), pp. 1-6. IEEE, 2014.