

# A Robust and Secure Image Watermarking Technique for Digital Data: State-of-the-Art

Bhupendra Kumar Bhardwaj, Professor Dr. Satya Singh

Department of Computer Science & Applications  
M.G. Kashi Vidyapith Varanasi, India

**Abstract-** With the fast development of computer technology, research in the fields of multimedia (text, image, audio and video clip) security, image processing and robot vision have recently become popular. Digital image watermarking techniques is one of the best techniques for image authentication. Watermarking algorithms are designed to embed and extract digital watermarks within digital content, such as images, audio, or video. The basic objective of the watermarking technique is to enhance imperceptibility, capacity and robustness. When developing an effective watermark method, it's necessary to have a highly balanced trade-off between imperceptibility, capacity, and robustness. In this paper we presence about watermarking system, requirements for digital image watermarking, challenging issue of watermarking, application of watermarking, importance of watermarking, image watermarking classification, various watermarking techniques, attacks on watermarking process, performance measure for evaluating the image quality using metrics and a short view of watermarking tools. The work gives a view on various watermarking schemes in digital images that give new ideas to improve the already existing techniques.

**Index Terms-** Image Watermarking, Spatial Domain, Transform Domain, Evaluation Metrics, Attacks

## I. INTRODUCTION

One of the biggest challenges is how to secure of digital data (i.e. text, image, audio and video clip etc.) over the growth of internet in the current-era [23, 15]. Steganography, cryptography, biometrics, blockchain, and watermarking are various methods used for digital data protection by hiding data using intellectual property rights (IPR). Steganography is the method of hides secret information in a cover image for secure data communication. Cryptography is a method of protective communication by allows only the sender and receiver can view their messages. Biometrics is a method of authenticating people by their unique identities. Blockchain technology provides secure communication by recording transactions. Watermarking is a method of embedding and extracting watermark data in multimedia files like text, audio, video, or image. It maintaining their security and privacy while the visual quality of the cover data is preserved [10, 20]. Watermarking is used for various notable applications to secure digital content from unauthorized individuals [15]. For example in bank currency notes, a watermark is embedded which is used to check the originality of the note. The same concept of watermarking can be used in digital multimedia (text, image, audio and video clip etc.) contents for checking the authenticity of the original content. To achieve robust and secure protection of digital content, this paper reviews some of the image watermarking techniques, general characteristics

of digital watermarking system; various watermarking techniques are discussed in brief with the potential applications of the watermarking methodology, various possible attacks on image and watermarking tools. Finally, certain points are summarized based on the theory and experimental results obtained by various researchers.

## II. WATERMARKING SYSTEM

Watermarking is defined [24] as the action of hiding a message, text, logo or signature into digital media. A watermarking system might be described as a structure that contains two parts: an embedding part and extraction (detection) part which are explained in given Table 1.

The embedding part takes two inputs. One is the secrete digital data we want to secure (i.e encode) as a watermark, and the other is the host media (i.e. image or video) in which we want to embed the secreted message. The embedded message can be extracted by using the detector, which determines whether the information or secrete message exists or not.

In Figure-1, shows the general layout of the embedding and extraction procedure. Watermarking can be visible, for example the images are printed on money notes, or invisible

watermarking, for which the watermark is hidden inside the cover media.

Table 1 Generic Watermarking Algorithm

Embedding Process	Select Watermark- Choose the watermark data or a unique identifier associated with the content. Transform Domain- Convert the original content and watermark into a common transform domain (e.g., frequency domain using Fourier transform, discrete cosine transform, wavelet transform). Embedding Operation- Modify the coefficients in the transform domain to embed the watermark information. The modification should be subtle to ensure that the watermarked content is perceptually similar to the original. Inverse Transform: Convert the watermarked content back to the spatial or time domain using the inverse of the chosen transform
Extraction (Detection) Process	Transform Domain- Transform the watermarked content into the same domain used during embedding. Extracting Operation- Use the watermark extraction algorithm to analyze the transformed content and extract the watermark information. Decision Rule-Apply a decision rule to determine the presence or absence of the watermark. <i>The decision rule should be robust against common signal processing operations and attacks.</i>



Figure-1 Watermark system

Some general terms and definitions (i.e watermarking, watermark, cover media, embedding, extraction, detection, noise, attack, attacked data etc.[23]) are used in the area of watermarking. Watermarking- Whole process of embedding and extraction. Watermark- The secret information that are provided to be hidden. Cover media- In witch embed the secreted message also known as host media that carries the messages. Embedding- The process of inserting the digital content into the host media. Extraction- The process of extracting or detecting the embedded watermark (hidden information) from the watermarked (cover or host media) data. Detection- The procedure used for detecting whether the given media contains the watermark or not. Noise- this is defined as any unwanted component in the signal, introduced for example during transmission or through thermal processes. Attack- the artificial process used, intentionally or non-intentionally, which modifies the watermarked data and destroys or alters

the watermark in the data. Attacked data- The watermarked data which contains noise or errors caused by artificial modification.

### III. REQUIREMENTS FOR DIGITAL IMAGE WATERMARKING

Developing secured image watermarking provides protection and confidentiality. For Digital Data robustness, imperceptibility, capacity, and security are the basic requirements of any efficiency watermarking system [29]. In Figure 2, when we developing an effective watermark method, it's hard and necessary to maintain a good relationship between the primary watermarking requirements imperceptibility, capacity, and robustness[16].

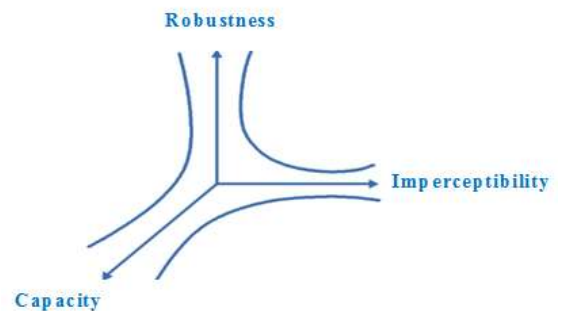


Figure 2 Tradeoff watermarking requirements

**Robustness-** Robustness is watermarking algorithm measure the ability to detect the watermark after common signal processing operations.

Watermarks should be robust against variety of geometrical and non-geometrical attacks [27]. Filtering, compression, geometric, noise, and histogram are some types of attacks. It is evaluated by PSNR metrics.

**Imperceptibility-** Imperceptibility in watermarking to preserve image quality, ensures watermark effectiveness and refer to ability how similar the original and the watermarked images are. It is evaluated by normalized correlation coefficient (NC) metrics, peak signal-to-noise ratio (PSNR), mean squared error (MSE), structural similarity index measure (SSIM), visual information fidelity (VIF) and human visual system (HVS) and The digital watermark should not affect the quality of the original image after it is watermarked [27].

**Capacity-** Capacity or data payload indicates the amount of information embedded in a watermarked image. It is evaluated by bit per pixel and the total bits. Security indicates that irrespective of targeted attacks, the inserted digital watermark cannot be removed. This property describes how much data

should be embedded as a watermark to successfully detect during extraction [27].

Computational cost- depends on watermarking algorithm complexity, watermark size and resolution, computational cost, the time taken for embedding and extracting watermarks. Need to maintain a good balance between computational cost and robustness [12].

False Positive- detects watermarks in images where none exist. Matrices for evaluating false positive watermarks are false positive rate (FPR), true positive rate (TPR) and receiver operating characteristic (ROC) curve.

Watermark Key- is a specific key that determines which elements are embedded. It contains Visual Keys, Invisual Keys Spatial Keys, Frequency Keys and Temporal Keys.

**Challenging Issue of Watermarking**

The most challenging issue that is existent in designing watermarking system has been its robustness and invisibility of the watermark (secret information), Resistance to attacks as cropping, scaling, countering tampering and compression, minimizing incorrect detections, maintaining watermark alignment, efficient embedding and detection, preventing unauthorized watermark removal, protecting against watermark estimation attacks, understanding human visual perception, resolving intellectual property disputes. In case of invisible watermarks, the watermarks scheme is served only as if they robustly survived in the host image irrespective of kinds of attacks. If any secret message is placed at the region of interest (ROI) of image, watermark would be secure, but the quality degrades. If watermarks are placed in non-region of interest (NROI), information can be cropped easily.

**Applications of Watermarking**

According to Applications Digital watermarking can be applied to: The developments of new types of watermarking techniques, algorithms and tools have paved the way for a wide variety of applications , such as Copyright Protection and Authentication, healthcare, transaction tracking, copy control, annotation and privacy control, tamper detection, invisible marking on paper and ID card security.

**Importance of Watermarking**

Copyright protection and security of digital content is a challenging for intellectual property protection, digital right management (DRM), content authentication and forensic tracking (identifies source of leaked content, tracks distribution and propagation) task in the current era [15, 28]. Identity theft, copyright violation and ownership identification are growing crimes, and have seen cyber-crime in general increasing [14]. Encryption, steganography and watermarking are some popular techniques used to provide security for secret data. Encryption techniques offer important security

components such as confidentiality, integrity, and authentication of digital data [14, 10]. It offers a major advantage since the digital data (watermark) is hidden within the host and exchanged without generating any kind of visible alert to the attacks [10]. Digital watermarking offers protection against tampering, access control, ownership authentication, non-repudiation, indexing, save memory, and bandwidth requirements [28, 14]. Thus, it has attracted considerable attention of multimedia community in the recent years.

**IV. IMAGE WATERMARKING CLASSIFICATIONS**

Different ways of image watermarking are categorized on perceptibility based, domain based, robustness based, and extraction based [11]. The image watermarking classification is summarized in Table II.

Table 2. Classification of Image Watermarking

Classification Criteria	Watermarking types
Based on Perceptibility	Visible- The watermark is clearly seen in the image. Invisible- Encoded within an image and not visible
Based on Domain	Spatial- Changes the value of pixel/bit sequences/code segments, of arbitrarily selected portions of images [26]. E.g.: LSB, patchwork, and SSM modulation. Frequency- Transforming the image by using the frequency domain [16]. E.g.: DCT, DFT, DWT, SVT, LWT, and KLT.
Based on Robustness	Fragile- Easily find out if the data has been altered. Preferred in integrity protection and content authentication. Semi-fragile- Resist for some transformations, but not for harmful transformations. <u>Used to verify the authenticity of an image.</u> Robust- Protects against a variety of geometric and non-geometric attacks without altering the watermark contents.
Based on Extraction	Blind- Removal of the embedded information requires only the watermarked image. Its applications are copyright protection, and e-voting. Semi-blind- Embedding does not require original data but requires a watermark or side information Non-blind- Requires the host image to detect the watermarked image.

In the spatial domain pixels directly hold embedding. In an attack-free environment, it is simple to put into practice. It is usually used to detect tampering. Its advantage is having an easy and quick operation. And the drawback is compression, geometric distortion, and filtering cause vulnerability and in

the transform domain the cover image's coefficients are altered. It offers compression, compatibility, robustness, and filtering during embedding. It is more secure than the spatial domain. But the drawback is having high computational time complexity.

### Various Watermarking Techniques

#### Watermarking Based on Spatial Domain

The spatial domain involves directly manipulating the pixel values of the image without transforming it into another domain, such as frequency or color space. In spatial domain schemes secret data is directly inserted or slightly modifies the pixels of the cover image. LSB, SSM (spread spectrum modulation), spatial spread spectrum (SSS), pixel value modification (PVM), patchwork and correlation-based techniques are the main techniques used in the spatial domain [4,25]. The spatial domain is not more robust against any kind of attack.

**Least Significant Bit Coding (LSB)** - LSB spatial domain watermarking in the spatial domain is a basic technique, it serves as a starting point for understanding the principles of information hiding in digital images. LSB spatial domain watermarking is a technique used to embed watermark information into digital images by manipulating the least significant bits of the pixel values. Digital images are represented by pixels, each having intensity values. For grayscale images, each pixel has a single intensity value, while for color images, each pixel has separate intensity values for red, green, and blue (RGB). In LSB spatial domain watermarking, Modifies the least significant bit of pixel values in each channel is modified to embed the watermark information. To extract the watermark information, the recipient reads the least significant bit of each pixel value from the watermarked image.

R. Van Schyndel, A. Tirkel, and C. Osborne [31] proposed two LSB techniques. In the first method the Least Significant Bit of the image was replaced with a PN sequence while in the second a pseudo-noise (PN) sequence was added to the Least Significant Bit. Though this method was simple but lacks of basic robustness. It was able to survive simple operations such as cropping, any additive noise, however, it was not possible to process the composite image under operations such as intensity enhancement, resampling, requantization, image enhancement, etc. On one hand, once this scheme was discovered, it becomes an easy task for the intruder to alter or detect the hidden information.

**Patchwork Technique-** The patchwork technique in watermarking is a method used to embed a watermark into an image by dividing it into patches and modifying selected patches to carry the secret data. The patchwork technique is advantageous because it allows for a distributed embedding of the watermark across the image, making it more resilient to

attacks that may focus on specific regions. Additionally, by modifying only a subset of patches, the impact on image quality is minimized. Patchwork technique in watermarking to make the secret data perceptually invisible while being robust against various attacks. For watermark embedding selected patches are modified to embed the watermark. The modification can be achieved by subtly altering the pixel values. For extraction, during watermark detection, the image is again divided into patches, and the watermark is extracted from the modified patches using the localization information.

W. Bender, D. Gruhl and N. Morimoto, A. Lu [5] proposed watermarking scheme based on statistical method called patchwork. In patchwork,  $n$  pairs of image points,  $(A, B)$  were randomly chosen. The image data in  $A$  were slightly brightening points while that in  $B$  were darkened. Patchwork was independent of the host image. Though this method was simple and easy showing reasonably high resistance to most non geometric image modifications. However there were some limitations such as extremely low embedded data rate and hence this technique was useful to low bit-rate applications only. Also it was necessary to keep a register about where the pixels in the image lie.

**Predictive Coding Scheme-** Predictive coding in watermarking is a method where the watermark (secret data) is embedded by predicting pixel values and adjusting them based on the prediction error. Predicting the value of a pixel based on neighboring values and insert/embedding the secret information in the prediction error. The difference between the actual pixel values and the predicted values represents the prediction error. Linear predictive coding (LPC), non-linear predictive coding (NLPC), adaptive predictive coding (APC), different pulse code modulation (DPCM) and autoregressive (AR) modeling are uses different predictive coding schemes in watermarking. Pixel different (PD) coding, gradient-based predictive coding (GBPC), adaptive prediction error (APE) coding and wavelet-based predictive coding (WBPC) techniques are applying in watermarking. Predictive error expansion (PEE), predictive quantization index modulation (PQIM), predictive amplitude modulation (PAM) and predictive frequency modulation (PFM) are very popular scheme using in watermarking. The difference between the actual pixel values and the predicted values is then analyzed to extract the watermark. Tanaka for gray scale images [28] proposed the correlation between adjacent pixels was exploited. A set of pixels where the watermark had to be embedded was chosen and alternate pixels were replaced by the difference between the adjacent pixels. This was further improved by adding a constant to all the differences. A cipher key was created which enabled the retrieval of the embedded watermark at the receiver. This was much more robust when compared to LSB coding. Predictive coding experimental result in watermarking is higher robustness against attacks, improved imperceptibility and efficient embedding and

detection. Disadvantages are computational complexity and sensitive robustness against certain attack as scaling.

### Watermarking Based on Transform Methods

Transform domain or frequency domain techniques are performed by manipulation of the orthogonal transform domain of a signal or image. DCT, DWT, FFT, DFT, SVD are based on transform watermarking.

DCT- Embedding secret message in DCT coefficients. Widely used DCT based transform coding are modified discrete cosine (MDCT) and forward discrete cosine transform (FDCT). Discrete Cosine Transform method inserts a watermark by splitting the host image into 8X8 non overlapping blocks. It decomposes a signal into low or middle or high-frequency bands. It mostly embeds information in midrange frequencies to achieve a good trade-off between imperceptibility and durability.

DFT- Discrete Fourier Transform (DFT) is a mathematical operation that transforms a Discrete-time signal and a finite or discrete number of frequencies into its frequency domain representation. It does not have all of the frequencies that make up an image. So it does not have enough samples to adequately characterize the spatial domain image. It divides images into sine and cosine forms. It withstands transformations. DFT implementation by matrix multiplication, fast Fourier transform (FFT) algorithms, butterfly diagram, radix-2 FFT and radix-4 FFT.

DWT- Discrete Wavelet Transform is sampled wavelets at discrete intervals. DWT decompose a signal into different frequency subbands, representing the signal in the time-frequency domain. Haar DWT, Daubechies DWT, Coiflet DWT, Biorthogonal DWT and Symlet DWT are different type of DWT. Its localization and multiresolution properties make it more flexible. It embeds partition data into distinct frequency components. The DWT decomposes signal into different sub bands as LL (i.e. LOW-LOW subband represent the low-frequency components of an image), HH (High-High subbands represent the high-frequency components), LH (LOW-HIGH subband represents the horizontal high-frequency and vertical low-frequency components of an image), and HL [6]. A Daham, M Ouslim, Y Hamed and W Djaber [2] proposed watermarking transformed techniques to improve the robustness and security for hidden secret message. These teams apply DWT that the low frequency signal or information is captured to embed the encoded mark. This method can resist some attacks but security performance of the method hardly satisfactory.

SVD- Singular value decomposition (SVD) decomposition is applied directly into the cover image's pixel values, and the information is embedded by modifying the coefficients of SVD decomposition of the cover image [13]. Embedding a

watermark by altering the host image's SVD decomposition coefficients. Watermarking based on Singular Value Decomposition (SVD) is a technique used to embed information (watermark) into digital media, such as images or videos, for the purpose of copyright protection, authentication, or content integrity verification. The SVD-based watermarking method takes advantage of the mathematical properties of SVD to hide the watermark in a way that is difficult to detect or remove without the proper key or information.

Singular Value Decomposition (SVD): SVD is a mathematical technique that decomposes a matrix into three other matrices:  $A=USV^T$ , where A is the original matrix, U and V are orthogonal matrices, and S represents a diagonal matrix with singular values.

Watermark Embedding: The host image is decomposed using SVD:  $A=USV^T$ . The watermark (usually represented as a matrix) is embedded into the singular values or other components of the decomposition.

Watermark Extraction: To extract the watermark, the watermarked image is again decomposed using SVD:  $A'=U'S'V'^T$ . The watermark (or secret information) is extracted from the modified singular values or other components.

Ankur Rai, Harsh Vikram Singh [17] proposed a hybrid watermarking scheme (DWT-SVD) and an SVM model for classification. They used a unique key to scramble embedded data. DWT's spatio-frequency localization feature as well as SVD's intrinsic algebraic properties are also considered. V Santhi, A Thangavelu [32] proposed a robust color image watermarking method based on DWT-SVD transforms with taking some advantage of YUV. First, the color host image is converted into RGB system, then converted to YUV domain where intensity (Y) and chrominance (UV) components are decorrelated. Here, the secret information can be hidden either in intensity components or in colour components. First of all, RGB components of the host image are converted into YUV colour spaces, then DWT and SVD are applied respectively. According to the SVD-modifying method, exchanges of singular values of the watermark signal and singular values of the cover image. This method provides high normalized correlation values after applying attacks, between the original and extracted watermark image that shows its high robustness, but low imperceptibility. Furthermore, once the algorithm was discovered, it improved the capacity, because it takes advantage of all bands. There are basically two problems occurring, first is the lack of security and the second problem is the possibility of false positive error. Fei Yan, Hesheng Huang, and Xu Yu [3] proposed, to embed logos in ROIs, LSB was employed, while RONI used DWT and SVD to embed text. QRW was

used to encrypt logo images and the BSO algorithm was used to determine an optimal scaling factor.

### Watermarking With Cryptography

Watermarking with cryptography involves embedding a digital watermark into cover image using cryptographic techniques such as symmetric-key cryptography, asymmetric-key cryptography, hash functions and digital signature. The goal is to ensure the integrity and authenticity of the watermark while protecting it from unauthorized removal or tampering. Watermarking with cryptography can be achieved as.

**Generate a Cryptographic Hash Function:** Choose a cryptographic hash function (e.g., SHA-256 (Secure Hash Algorithm 256-bit), SHA-3 (Secure Hash Algorithm 3)) to create a hash of the watermark data.

**Embedding the Watermark:** Combine the watermark with the cryptographic hash or a representation of it. The algorithm to embed this combined data into the content such as host image. The watermark should be imperceptible to the human senses and capable of avoid altering the quality of the content significantly.

**Encryption of the Watermark:** Optionally, encrypt the watermark or the hash before embedding it. This adds an extra layer of security. Use a symmetric or asymmetric encryption algorithm depending on the requirements. If encryption is used, manage the cryptographic keys securely. The keys should be kept confidential and only shared with authorized parties.

**Verification:** To verify the watermark's integrity and authenticity, extract the embedded watermark from the content. Decrypt the watermark data if encryption was applied. Recalculate the hash or use the decrypted hash and compare it with the original hash. If they match, the watermark is intact and hasn't been tampered with.

**Detection and Recovery:** The process of detection and recovery typically involves verifying the integrity of the watermark, checking its authenticity, and recovering the embedded data (watermark) from the content. Recovery involves extracting the embedded watermark and returning it to a usable form.

In case of tampering or removal attempts, take appropriate action, such as alerting the user or initiating a recovery process.

D. Bouslimi, G. Coatrieux, M. Cozic and C. Roux [22] proposed a method to achieve security, a substitutive watermarking approach, quantization index modulation, was employed in conjunction with an encryption algorithm, a

stream cipher algorithm (e.g., the RC4), or a block cypher algorithm. A Anand and AK Singh [1] proposed the encryption-then-compression technique which is more secure data against possible attacks as applying chaotic encryption to the cover image to obtain an encrypted image. Compressed data are obtained by applying the set partitioning in hierarchical trees (SPIHT) to the encrypted image. At the receiver side, the whole process is reversed to obtain the decrypted image. Sara T. Kamal, Khalid M. Hosny, Taha M. Elgindy, Mohamed M. Darwish, Mostafa M. Fouda [2] presented a novel encryption technique for both grayscale and colour medical images. Image blocks were jumbled, rotated, and randomly permuted in a zigzag manner. A chaotic logistic map produces a key that may be used to diffuse the jumbled image.

### Watermarking Using Deep Learning

Deep learning is a sort of machine learning in which neural networks are used to derive useful feature representations from the input. Deep learning-based dataconcealing models train models to hide information invisibly and reliably using the encoder-decoder network topology. It eliminates the requirement for specialist knowledge when constructing data hiding methods and improves security due to its black-box nature.

H. Kandi, D. Mishra, and S. Gorthi [18] proposed an autoencoder CNN for the watermarking process. Simulated attack layers for various attacks and a strong factor that controlled the image's robustness against imperceptibility. A. Anand, A.K. Singh [8] present a novel techniques for COVID-19 patient's CT scan images, used redundant discrete wavelet transform (RDWT), Hessenberg Decomposition (HD), and randomised singular value decomposition (RSVD). Turbo coding is used to minimise channel noise in EPR. The extracted watermark was denoised using a deep neural network to increase its durability (DNN). Anusha Chacko, Shanty Chacko [9] using various integration strengths, and chosen DCT coefficients average selected DCT blocks are determined. An Arnold transform has scrambled the binary watermark. During the image carrier, based on DLCNN the watermark is detected and extracted using a pattern recognition model

### Watermarking With Biometric/Blockchain

Watermarking combined with biometrics or blockchain introduces additional layers of security, integrity, and authentication for digital content. Many scholars applied biometric-based watermarking algorithms for authentication, confidentiality, reliability, achieve good accuracy and achieve high robustness for the watermarking system [12].

**Watermarking with Biometrics:** Embed biometric features, such as fingerprint or iris data, into the watermark (i.e. Digital content) to establish ownership or authentication. The

combination of the watermark and biometric information can provide a stronger link between the content and the user. In Multi-Biometric Watermarking: Combine multiple biometric modalities for watermarking to enhance security and reliability. For example, combining fingerprint and facial features.

**Blockchain for Traceability-** Use blockchain to create an immutable and transparent record of the watermarking process, ensuring traceability and provenance. Store information related to the watermark, such as timestamps, watermarking parameters, and authentication data, in a blockchain. This can be used to verify the legitimacy of content and a novel watermarking process.

1-Utilize smart contracts on the blockchain to automate aspects of rights management. For example, smart contracts can enforce usage policies and facilitate automatic payments or permissions. 2-Access Management: Blockchain can be used for decentralized identity management, providing a secure and tamper-resistant way to manage access control for watermarked content. 3-Ownership Verification: Represent content ownership through tokens on a blockchain. The transfer of ownership can be recorded in a transparent and secure manner. 4-Evidence of Ownership: The blockchain serves as an immutable ledger, providing evidence of ownership and the history of watermarking operations, which can be crucial in legal disputes or intellectual property cases.

NF Sahib, M Mohammed, S Naji and EA Hamed [7] propose an algorithm for the biometric watermarking system with a frequency domain in the cover medical images. Firstly watermark's image iris code of the sender side as a sender authentication key, and then encryption is performed by XOR for the patient information. In this process first, embed the two watermark images and then DWT transform is applied to convert the original image into a watermarked image.

### Types of Attacks on Watermarks

**Attack-** The artificial process used, intentionally or non-intentionally, which modifies the watermarked data and destroys or alters the watermark in the data.

**Attack Data-** The watermarked data which contains noise or errors caused by artificial modification. General types of the attacks are removal attack, geometrical attack, cryptographic attack, oracle attack, and protocol and security attacks.

**Removal Attacks-** These attacks aims at removing watermarks from the watermarked image by intentionally performing image processing operations, such as quantization, lossy compression, averaging, re-modulation, demodulation, collusion attacks, block replacement attacks, de-noising and filtering. Lossy compression (JPG and VQ compressions) of images which restricts the size of watermark. When

manipulating the modulation of signal, the attacker first forecasts watermark using variety of filters (median, high pass and wiener), then subtracts it from the watermarked image and finally adds the Gaussian noise to it. This type of attacks is commonly known as collusion attacks. However, on the other hand, as a mosaic attack, the attacker splits the watermarked image into small portions and tries to reassemble it using HTML table, with an intention of removing the inserted watermark.

**Geometrical Attacks-** This aims to making changes to the watermarked image to challenge the detection or extraction of the embedded watermark. In geometrical attacks, attackers try cropping the image from sides, delete/edit/shift some rows or columns of pixels randomly or with intentional alterations made to a digital watermark. The common geometrical attacks are translation, rotation, shearing, affine transformation, scaling, aspect ratio changes, cropping, column/line removals, jitter, and random bending.

**Protocol Attacks-** It aims at creating ambiguity of ownership and by attacking the watermarking application itself, using the concept of invertible watermarks. The protocol attacks sets another requirement for design of watermarking tools i.e., watermark extraction must be impossible from any images, which are in fact not watermarked. In this case false positive rate must be at minimum. Also, protocol attacks take the advantage of loopholes in the management or implementation process of watermarking.

**Copy Attacks-** It aims at prediction of watermark and replicates it on to other data without the knowledge of secret keys involved. Also, development of image-dependent watermarks is the best solution to thwart these kinds of attacks.

**Legal Attacks-** It attempts in doubting the technical evidences on watermarks and watermarking schemes, while proving the ownership in the courts.

**Cryptographic Attacks-** This envisages in finding the lengthy secret keys by exhaustive searches.

**Oracle Attacks-** It provides the original host image from watermarked image using a watermark detector or extraction algorithm.

**Disable Detection Attacks-** It aims at breaking the relation between the watermark and host carrying it without affecting the existence of watermark.

**Ambiguity Attacks-** The attacker embeds multiple fake watermarks in order to mislead the detector. The ambiguity attacks occur in systems with multiple watermarks. In this

scheme the order in which the watermarks are inserted is ambiguous.

### Performance Evaluation Metrics

The performance measure for evaluating the quality of image, calculated by its robustness, imperceptibility and capacity.

Evaluation of Imperceptibility- Commonly used measures for imperceptibility evaluations are Mean Squared Error (MSE), Image Fidelity (IF), Peak Signal-to-Noise Ratio (PSNR), and Euclidean distance (ED). PSNR is calculated for verifying the image's quality after the embedding process. Image Fidelity (IF) gives the amount of imperceptibility of the watermark in a watermarked image.

**Evaluation of Robustness-** Normalized Cross-Correlation and Bit Error Rate are parameters used for robustness analysis. Normalized Cross- Correlation (NCC) calculates the similarity of the host watermarked image and extracted watermark image. The value of NCC should be nearest to 1.

**Evaluation of Capacity-** The embedding of capacity  $C$  is measured using in bits per pixel [21].

$$C = \frac{\text{Total number of bits embedded}}{\text{Total number of pixels in the image}}$$

### Watermarking Tools

There are various watermarking tools available for adding watermarks to image. Watermarking tools are employed as a way to protect Intellectual Property rights and to prevent illegal forgery and piracy [19]. The recent researches on watermarking tools proposed, robust algorithms for watermark embedding and extraction digital data host. Some popular options include Adob Photoshop, Lightroom and online tools like Watermark.ws, iWatermark [30]. Some other online tools are (1)uMark Lite (2)WTM PLUS (3)Water marquee (4)Lunapic (5) Visual water mark (6)Mass water mark (7) Water mark lib (8) Alamoos (9)TSR water mark (10)More water marker , (11)Photo Watermark Professional (12)Fast water mark (13)Watermark Master , (14)Watermark.ws (15)Cooltweak (16)Picture stamper (17)Water mark passion (18)Easy watermark studio lite (19)Bytescout watermarking (20)Snagit (21) Jaco Watermark (22)Star Watermark (23)Arclab Watermark (24)BiggerBids Image Watermarking Tool (26)Batch Watermark Creator.

## V. CONCLUSION

Digital watermarking is commonly used for copyright protection, authentication, and tamper detection in multimedia content such as images, audio, and video. In this paper we present, a lot of efficient watermarking techniques have been developed for various notable applications. The overall process of watermarking, major Characteristics, novel applications, general embedding and extraction procedures as

well as potential challenges in this field. This study summarized various features of watermarking tools and suggests the suitability of its usage in accordance with users. Also, briefed various possible attacks on image watermarking tools, which needs to be addressed at large in future towards copyrights for data protection in terms of ownership security and intellectual property.

## REFERENCES

1. A Anand , and AK Singh (2022). A Comprehensive Study of Deep Learning-based Covert Communication. ACM ACM Trans Multimed Comput App, 18, no. 2s (2022): 1–19.
2. A Daham, M Ouslim, Y Hafed and W Djaber (2022). Robust Watermarking Method to Secure Medical Images Applied to Ehealth. 13th International Conference on Information and Communication Systems, 379–385.
3. Fei Yan, Hesheng Huang, and Xu Yu(2022). A multi-watermarking scheme for verifying medical image integrity and authenticity in the Internet of Medical Things. IEEE Transactions on Industrial Informatics.
4. MS Moad, MR Kafi, A Khaldi(2022). A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocess Microsyst 90:104490.
5. NF Sahib, M Mohammed, S Naji and EA Hamed (2022). Verification approach for medical data in e-healthcare system based on biometric and watermarking. Period Eng Nat Sci (PEN) 10(2), 408–417.
6. Sanivarapu Prasanth Vaidya, (2022). Fingerprint-based robust medical image watermarking in hybrid transform.
7. Sara T.Kamal, Khalid M.Hosny, TahaM.Elgindey, Mohamed M. Darwish, MostafaM.Fouda(2021). A New Image Encryption Algorithm for Grey and Color Medical Images. IEEE Access.
8. A. Anand, A.K. Singh(2021). Dual Watermarking for Security of COVID- 19 Patient Record. IEEE Transaction on Dependable and Secure Computing .
9. Anusha Chacko, Shanty Chacko(2021). Deep learning-based robust medical image watermarking exploiting DCT and Harris hawks optimization,” International journal of Intelligent Systems.
10. A. Anand and A. K. Singh (2020). Joint watermarking-encryption-ECC for patient record security in wavelet domain. IEEE Multi Media 27, 66–75.
11. A. Anand and A. K. Singh(2020). Watermarking techniques for medical data authentication: A survey. Multimedia Tools and Applications.
12. NF Mohammed, MJ Jawad, and SA Ali (2020). Biometric-based medical watermarking system for verifying privacy and source authentication. Kuw J Sci, 47, no. 3.

13. Sajjad Bagheri Baba Ahmadi, Gongxuan Zhang and Songjie Wei (2020). Robust and hybrid SVD-based image watermarking schemes: A survey, Multimedia tools and applications.
14. Chauhan Digvijay Singh, A. K. Singh, B. Kumar, and J. P. Saini, (2019). Quantization based multiple medical information watermarking for secure e-health. Multimedia Tools and Applications, 78, 3911–3923.
15. Yao Yuanzhi, Weiming Zhang, Hui Wang, Hang Zhou, and Nenghai Yu (2019). Content-adaptive reversible visible watermarking in encrypted images. Signal Processing, 164, 386–401.
16. A. K. Singh, B. Kumar, S. K. Singh, M. Dave, V. K. Singh, P. Kumar, S. P. Ghreera, P. K. Gupta, and A. Mohan(2017). Guest editorial: Robust and secure data hiding techniques for telemedicine applications. Multimedia Tools and Applications 76, 7563–7573.
17. Ankur Rai, Harsh Vikram Singh (2017). SVM based robust watermarking for enhanced medical image security. Multimedia Tools and Applications, Springer link.
18. H. Kandi, D. Mishra, and S. Gorthi(2017). Exploring the learning capabilities of convolutional neural networks for robust image watermarking. Computing. Security. 65.
19. N. Dey, S.S. Ahmed, S. Chakraborty, P. Maji, A. Das, A., S. S. Chaudhuri (2017). Effect of trigonometric functions-based watermarking on blood vessel extraction: an application in ophthalmology imaging, International Journal of Embedded Systems, 90-100.
20. S. P. Mohanty, A. Sengupta, P. Guturu, and E. Kougiannos (2017). Everything you want to know about watermarking: From paper marks to hardware protection. IEEE Consumer Electronics Magazine 6, 83–91.
21. Barun Pandhwal, D.S. Chaudhari (2013.) An Overview of Digital Watermarking Techniques. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1.
22. D. Bouslimi, G. Coatrieux, M. Cozic and C. Roux(2012). A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images. IEEE Transactions on Information Technology in Biomedicine.
23. Ensaf Hussein, Mohamed A. Belal (2012). Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 7.
24. Manpreet Kaur, Sonika Jindal, Sunny Behal(2012), A STUDY OF DIGITAL IMAGE WATERMARKING, International Journal of Research in Engineering & Applied Sciences.
25. A Piva and M Barni (2008). Watermarking: An overview. IEEE Signal Processing Magazine, 25(1), 35-46.
26. I. J. Cox, M. L. Miller, and J. A. Bloom (2002), “Digital Watermarking and fundamentals”, Morgan Kaufmann, San Francisco.
27. Sin-Joo Lee and Sung-Hwan Jung(2001), A Survey of Watermarking Techniques Applied to Multimedia, ISIE.
28. F. Hartung, and M. Kutter( 1999), Multimedia Watermarking Techniques, IEEE Proc. IEEE, Special Issue on Identification and Protection of Multimedia Information, vol. 87, 1079–1107.
29. Petitcolas Fabien A., Anderson Ross J., Kuhn Markus G (1999). Information Hiding – A Survey, Proceedings of IEEE, Special issue on protection of multimedia content, 1062-1078.
30. Surekha Borra, Nilanjan Dey, Lakshmi H R, Amira S. Ashour(2017). Digital Image Watermarking Tools: State-of-the-Art.
31. R. van Schyndel, A. Tirkel, and C. Osborne (1994). A digital watermark. Proc. IEEE Int. Conf. Image Processing, vol. 2, 86–90.
32. V Santhi, A Thangavelu (2009). DWT-SVD combined full band robust watermarking technique for color images in YUV color space. Int J Comput Theory Eng 1(4):424.