https://doi.org/10.69974/glskalp.01.01.49

GLS KALP Journal of Multidisciplinary Studies Volume 1; Issue 1; January - March 2021

# A Comprehensive Study of Digital Watermarking

**Sonali Chakraborty**[1]

## *Abstract*

*The rapid growth of the world wide web has considerably increased the accessibility and sharing of multimedia data. The availability of various image processing application software and tools has made data susceptible to modifications with higher level of expertise. As a result, the digital assets are facing severe challenges such as violation of copyright and intellectual property rights, security threat etc. It is difficult to ensure that the data received over the internet is same as shared by the owner. The authenticity and the integrity of the multimedia data received or shared over the internet can be preserved by embedding a digital watermark into the original image. The present study performs a comprehensive study of digital watermarking on still images. Some of the most probable threats on the still images are illustrated and a review of significant literature based on various watermarking techniques proposed by researchers over the past few decades is discussed. The main aim of the study is to gain a detailed insight about digital watermarking in order to pursue further research in the said area.*

***Keywords:*** *Digital watermarking; watermarking techniques; multimedia data; malicious attacks; security threats; image protection; image authentication; tamper detection*

## 1.0 Introduction

The growth of multimedia with information and communication technology has enabled easy accessibility and rapid sharing of enormous amount of data over the internet. The use of multimedia data such as images, audio and video provide an effective medium of communication as they are easy to understand. The availability of various image processing application software and tools has made the task of image tampering easier with higher level of expertise such that it is visually difficult to differentiate between the original and the modified image. As a result, the digital assets are facing severe challenges such as threat of unauthorized possession, violation of copyright and intellectual property rights, security threat etc.

[1] Department of Mathematical and Computational Sciences,
National Institute of Technology, Karnataka

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies Volume 1; Issue 1; January - March 2021

The authenticity and the integrity of the multimedia data received or shared over the internet cannot be guaranteed.

The present study performs a comprehensive review of digital watermarking with respect to still images. Section 2 illustrates the most probable attacks on the images and identifies the major threats arising due the attacks. Section 3 gives a theoretical explanation about digital watermarking and provides a classification based on various parameters. Some of the major emerging applications of digital watermarking are discussed in section 4. Section 5 gives a review of significant literature based on various watermarking techniques proposed by researchers while section 6 concludes the research study.

## 2.0 Attacks on the Images

The ease of sharing multimedia data over the internet and the availability of various image processing tools has made the digital images vulnerable to modifications. The data received over the internet are manipulated without the knowledge of the owner. Some of the most common types of attacks or modifications performed on the images *(Dirik and Memon, (2009), Mahidan and Saic, (2009a), Mahidan and Saic, (2009b), Elwin et. al, (2010) and Qu et. al, (2009))* are splicing, image retouching, geometrical transformations *(Dong et. al, 2005)* and copy – and move attacks *(Chen and Wang, 2009)*. Each of these attacks is briefly discussed below.

***a)*** **Splicing:** In this type of attack two independent images are combined to form a third image.

*Example1:* As shown in Figure 1, (a) and (b) depicts two independent images accessed from the web without the permission of the owner. However, the originality of these images as shared by the owner cannot be ensured. Using some of the easily available image processing tools a portion of the image from (b) has been cropped and is inserted into image (a). The resultant new image formed is (c).

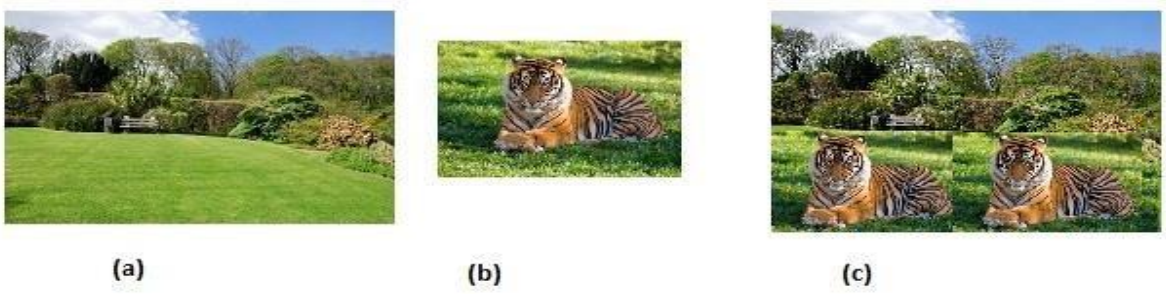


Figure 1: (a). Original image of a garden (b). Original image of a tiger (c). Image created by inserting portion of image (b) into image (a)

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

*Example 2:* A quite common type of malicious attack is illustrated in Figure 2 where a signature in an original document is replaced with a counterfeit signature. Figure 2 (a) shows a copy of an original invoice with the owner's signature while the forged scanned signature shown in (b) is used to replace the original signature in (a). Thus, the manipulated invoice is seen in (c). Such modifications performed on the documents are indistinguishable and are difficult to detectwithout the owner's knowledge.

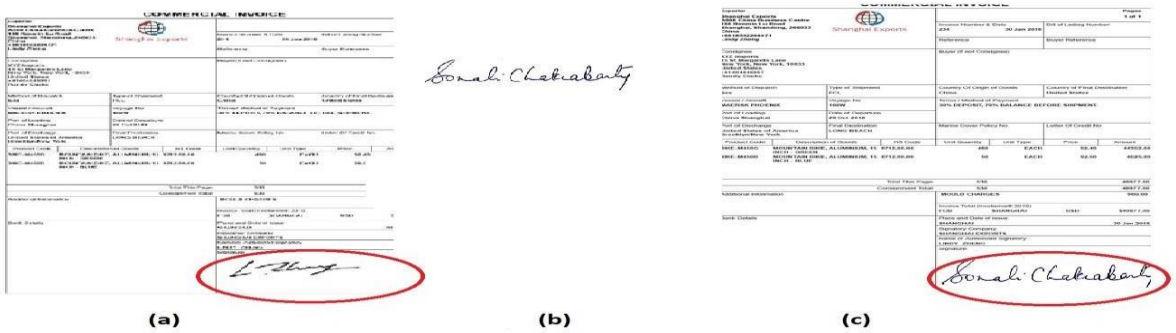


Figure 2: (a). Copy of an original invoice (b). Scanned image of a signature (c). Original invoice with manipulated signature

***b)*** **Image retouching:** In this type of attack the background of the image is either changed orenhanced for the purpose of improving the quality of the image.

*Example 3:* In Figure 3, image (a) is the original image in which the background of the imageis enhanced using image processing tools to increase the quality of the image. Such modifications or enhancements can be done on the images by increasing the hue, contrast or the brightness of the image. The enhanced image is seen in (b).


Figure 3: (a). Original image (b). Retouched image *(Elwin et. al, 2010)*

***c)*** **Geometrical transformations:** In this type of attacks, the images are altered by applying various transformation functions such as scaling, rotation and translation. The operation is performed by

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies Volume 1; Issue 1; January - March 2021

copying a portion of the image, applying transformation function on them and then inserting the transformed portion into the same image.

*Example 4:* Figure 4 (a) shows the original image having only one cartridge. The image of the cartridge has been copied, translated and then placed into the same image as seen in (b). Therefore, the originality of the image having only one cartridge has been modified with that of two cartridges. Such transformations done with ill intentions change the sense of the image and cause serious complications when produced as evidences during legal proceedings.


Figure 4: (a). Original image (b). Geometrically transformed image *(Elwin et. al, 2010)*

***d)*** **Copy-Move attack:** In this type of attack, a portion of the image is copied and then pasted over some part of the same image for the purpose of hiding certain areas or information.

*Example 5:* Figure 5 (a) shows an image having two jeeps. In (b), one of the two jeeps have been covered by the image of a foliage copied from the same image and therefore the originality of image (a) is lost. Again, such attacks change the gist of the images and convey a wrong manipulated message which further causes serious problems.

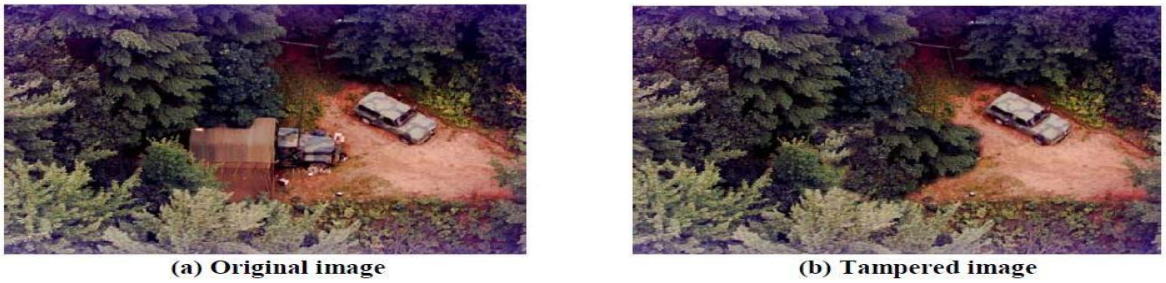


Figure 5: (a). Original image (b). Tampered image after copy move attack *(Huang et. Al, 2008)*

## 2.1. Threats on the Images

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

The major threats arising due to most common and probable attacks on the images discussed in the preceding sections are identified as follows:

- Loss in the originality of the images due to their rapid sharing, tampering and alterations
- No assurance about the authenticity and the integrity of images received or shared over theinternet
- Threat of unauthorized possession due to the modifications in the original image without the knowledge or the permission of the owner
- Unauthorized possession of digital assets leading to copyright and intellectual property violation *(Samuel and Penzhorn, 2004)*
- Change in the gist of the image due to malicious modifications on the important documents, printed text and images with an ill intention. This eventually increases the probability of security threat and complications during legal proceedings.

Distribution of modified images over the internet leads to spreading of wrong informationamong the web users.

## 3.0 Digital Watermarking: A Theoretical Overview

The challenges and the threats faced by the mages as identified in section 2.1 is a major concern. Various study and research are carried out for securing the authenticity and the integrity of the digital content shared over the internet. One of the ways to secure the images is by applying a cryptographic algorithm using a private-public key pair. The implementation of cryptographic algorithms for enforcing security has prerequisites and limitations *(Bartolini et. al, 2001)* which are mentioned as follows:

- The cryptographic algorithms require some additional information embedded into the data to be secured. The information is in the form of a header or a separate file comprising of the details about the applied algorithm such as the type and the name of algorithm, public key, hashing function used etc.
- One of the major limitations of the cryptographic algorithms is that they are not capable ofdetecting the type of attack on the image.
- By using cryptography, the tampered area in the image cannot be localized and identified.

Considering the drawbacks of the above suggested approaches, the authentication and the integrity of images can be protected by embedding some kind of information or a digital signature into the original image in the form of a digital watermark *(Haldar et. al, 2010)*. The digital watermarking is referred as: *"The act of hiding some information into an underlying data for the purpose of content protection or authentication"*. The image into which the watermark is embedded is referred as the host image or

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

original image and the information to be embedded is referred as a watermark *(Sarkar and Sanyal, 2014)*. An image having an embedded watermark into it is referred as a watermarked image. In order to authenticate an image or to detect any tampered area in an image, the embedded watermark is extracted from the watermarked image and is then compared with the original watermark. The digital watermarking process is represented using a block diagram in Figure 6.

A digital watermark can be a digital signature in the form of a logo of an organization, initials of the owner, parts of an image etc. In an ideal situation there should be no visual difference between the host image and the watermarked image. Figure 7 (a) depicts a host image into which the watermark (b) is embedded to form a watermarked image (c). Visually it is difficult to detect any difference between the host image (a) and the watermarked image (c). It is preferable that the watermark be embedded into a major portion of the host image such that any alteration to the watermark damages the host image *(Podilchuk and Zeng, (1998), Wolfgang et. al, (1999), Podilchuk and Delp, (2001))* and helps in detecting or localizing a tampered area in an image easily.

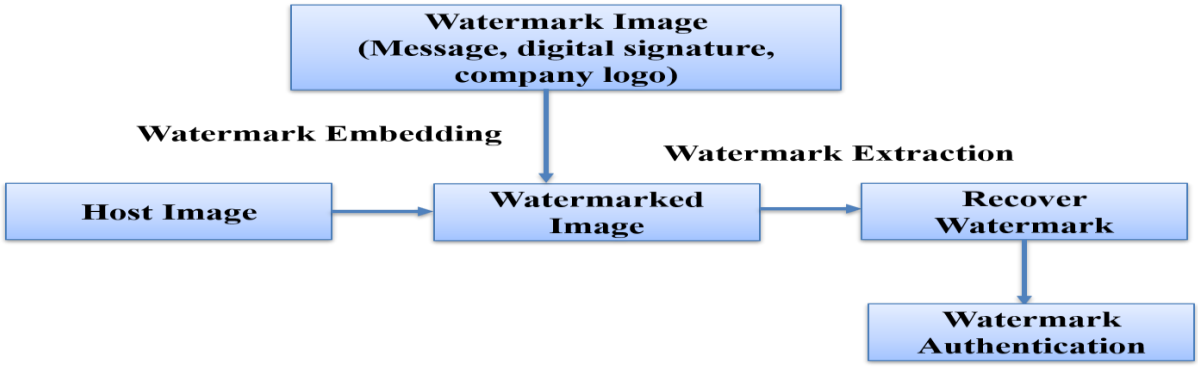


Figure 6: Block diagram of digital watermarking process

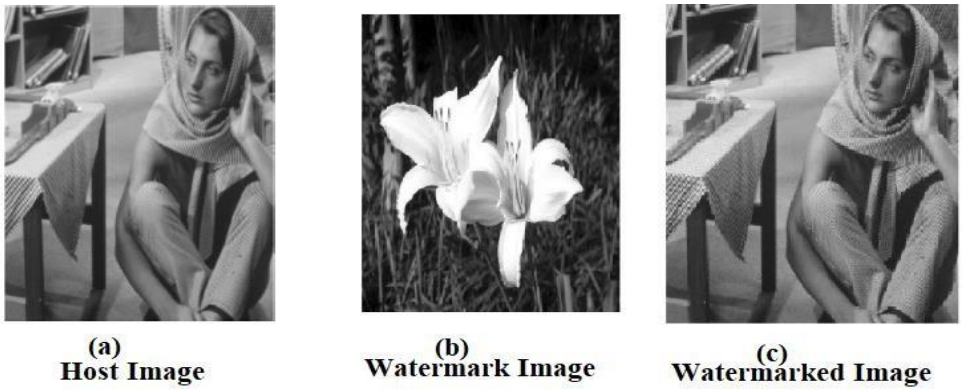


Figure 7: (a) Original host image (b) Watermark image (c) Watermarked image *(Mohanarathinam et. al, 2019)*

### 3.1. Classification of Digital Watermarking Techniques

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

The digital watermarking techniques are classified *(Chawla et. al, (2012) and Boreiry and Keyvanpour, (2017))* based on the human perception *(Vleeschouwer et. al, 2002)* i.e., whetherthey are noticeable or not, method of detection, domain of insertion (spatial or frequency domain), robustness of the algorithm *(Xuehua, (2010), Mohanarathinam et. al, (2019))* and the type of multimedia document on which it is applied such as image, audio or video. Figure 8 depicts the classification of watermarking techniques *(Allaf and Kbir, 2019)*.

Based on the human perception, digital watermark is classified as either perceptible or imperceptible:

**a. Perceptible watermark**: In case of perceptible or visible watermark, the watermark image can be recognized or noticed with the host image. For example: Overlaying an on-screen graphics or a logo on an image for the purpose of copyright protection.

**b. Imperceptible watermark**: With imperceptible or invisible watermark, the message or the watermark image is hidden within the host image. For example *:* Embedding a secret message or a code within the host image for the protection and detection of malicious image tampering. Invisible watermarks are either fragile, semi-fragile or robust.

**i. Fragile watermark:** Fragile watermarking techniques are sensitive to the changesin an image. The tampered images are detected based on the state of the watermark. These watermarking techniques are used for protecting the integrity of the image since they have the capability to detect a tampered image.

**ii. Semi-fragile watermark:** Semi-fragile watermarking techniques are those that accept fewer operations such as compression, less noise etc. but are sensitive to transformations such as cropping, shifting, rotation etc.

**iii. Robust watermark:** Robust watermarking techniques are resistant to some image transformations, processing and lossy compression. During image transformation, compression or attacks the embedded watermarks are not destroyed. These watermarking algorithms are majorly used for embedding copyright information into the host image.

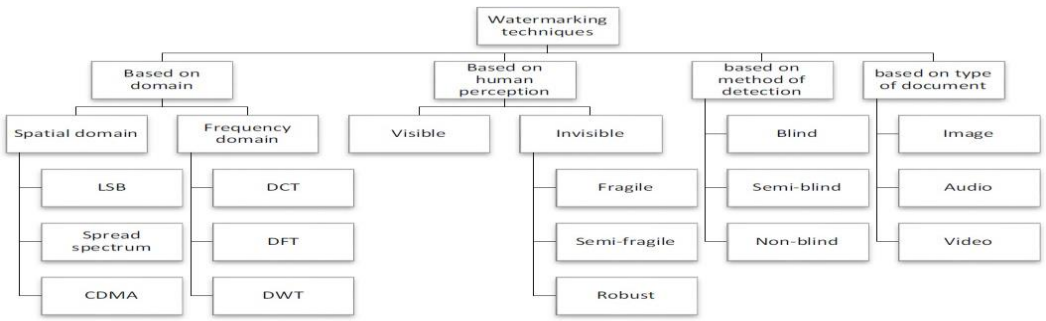


Figure 8: Classification of watermarking techniques *(Allaf and Kbir, 2019)*

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

The watermarking techniques are also classified based on the domain in which they are inserted i.e., spatial or frequency domain:

a. **Spatial domain techniques:** The spatial domain techniques are applied on the pixels of the image by embedding a watermark in the form of least significant bits (LSB) or by using the statistical characteristics of the pixel or by hiding watermark in the texture part of the image.

b. **Frequency domain techniques:** These techniques use the frequency components of the image. Frequency domain algorithms embed watermark in the transform domain of the image and thereafter convert the image to spatial domain. The majorly used frequency domain methods are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT),Discrete Wavelet Transform (DWT) and Discrete Slantlet Transform (DST) *(Mundher et. al, 2014)*.

Although the frequency domain techniques provide better security, recovering the watermark from the host image at the receiver's end is a complex process *(Chandrakar and Bagga, 2013)*. Moreover, performing computations using frequency domain is also quite complex as compared to using spatial domain techniques *(Schyndel et. al, 1994)*. Table 1 depicts a comparison between the watermarking methods based on spatial and frequency domain in terms of complexity, capacity and robustness *(Allaf and Kbir, 2019)*.

**Table 1: Comparison between spatial and frequency domain techniques *(Allaf and Kbir, 2019)***

| Characteristics | Spatial Domain | Frequency Domain |
|---|---|---|
| Complexity | Low | High |
| Capacity | High | Low |
| Robustness | Low | High |

## 4.0 Applications of Digital Watermarking

The wide range of applications of digital watermarking includes image authentication, image tampering and fraud detection, content protection, source tracking, copyright protection etc. Source tracking and tampered image detection helps in the prevention of spreading of fake, edited and manipulated images. Dissemination of such fake images misleads the people and disturbs the peace of the society. The use of digital watermarking for copyright protection prevents the ownership violation and preserves the owners right for its intellectual property.

Some of the major emerging application areas of digital watermarking are discussed as follows:

1. **Healthcare** *(Coatrieux et. al, (2006), (Singh and Rai, (2018), Allaf and Kbir, (2019))*: Thedevelopment of multimedia with information technology has given a boost to the healthcare sector by enhancing the

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies Volume 1; Issue 1; January - March 2021

services such as telemedicine, seamless sharing of electronic records of patients etc. The sharing of confidential patient data over the internet requires security of healthcare information management. Various digital watermarking techniques developed for the protection of healthcare management *(Memon et. al, (2011), Al-qershi and Khoo, (2011), Gunjal and Mali, (2012), Abhinav and Chandan, (2014), Gull et. al, (2018))* can be used for securing patient records and to provide authentication, verificationand hiding the data.

2. **Video surveillance** *(Bartolini et. al, 2001)***:** Video surveillance is widely used as a means for implementing security by continuously monitoring institutions, industries, sensitive areas, remote locations etc. The visual data captured is stored in a central unit and is used for analysis during any attack or in case of legal proceedings. Therefore, it is necessary to protect the visual data against any malicious attacks or tampering. Use of watermarking- based authentication is helpful for detecting the content tampering and for getting the original data.

3. **Binary document images** *(Brassil and Gorman, (1996), Brassil et. al, (1999), (Chen et. al, (2001), Hu, (2005), Daraee and Mozaffari, (2014))*: The use of binary document images has increased due to the easy availability of scanners and digital cameras. Digital documents are majorly used in bank cheque, engineering and architectural drawings, road maps, art works, literature, e-books, art works etc. There arises a need to protect the digital documents from copyright threats, copy control marginal note, and authentication. Watermarking techniques can be applied to the binary documents for the protection againstvarious threats and attacks. Digital watermark can be embedded using various methods such as shifting a line, word, or character in a text *(Low et. al, (1995a), Low et. al, (1995b), Maxemchuk and Low, (1997), Low et. al, (1998), Low and Maxemchuk, (1998))* modifying the boundaries *(Mei et. al, 2001)* partitioning the image into fixed blocks *(Koch and Zhao,(1995), Pan et. al, (2000), Wu et. al, (2000), Tseng and Pan (2000))* modifying the features of the character *(Bhattacharjya and Ancin, (1999), Amamo and Misaki, (1999))* or the run-length patterns *(Matsui and Tanaka, 1994)* or the half-tone images *(Baharav and Shaked, 1999)*.

4. **Relational database** *(Guo, (2011), Farfoura et. al, (2012), Khanduja et. al, (2012), Khanduja, (2017))*: Initially, the implementation of digital watermark was focused on multimedia data only, but now it has been extended to the database systems due to its increased usage in real-life applications *(Haldar et. al, 2010)*. The need to protect the relational databases using digital watermarking was identified by the researchers *Khanna and Zane (2000)* and *Agrawal and Kiernan (2002)*. Using digital watermarking for protecting the relational databases ensures its integrity *(Hacigumus et. al, (2002), Agrawal et. al, (2003))*, helps in data mining applications *(Agrawal and Srikant, 2000)*, used during online B2B interactions *(Hu and Grefen, 2002)*, used for ownership identification and information recovery *(Khanduja et. al, 2014)* etc.

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

5. **Forensic science** *(Guojuan and Dianji, (2011), Piva, (2013))*: Digital watermarking image forensics is used for copyright protection and acts as a record of authenticity for electronic evidence in legal proceedings. The documents used for watermarking in forensics can be images, video, audio and text images. Robust digital watermarking is used for mediating the source of the image while fragile watermarking gives an assurance of authenticity of the image. There are two forms of watermarking used in image forensics, i.e. active and passive. In case of passive image forensics *(Guojuan and Dianji (2011), Allaf and Kbir, (2019))* the authenticity of the digital images can be determined after extracting the watermark image from the host image. While in case of active image forensics, watermark image is embedding using the digital cameras used while capturing the images. The use of active image forensics is not been popular since the watermarking digital cameras incur huge investments to be capable of embedding a watermark into the image.

## 5.0 Review of Literature

A significant review on digital watermarking *(Hartung and Kutter, (1999), Muharemagic and Furht, (2001), Wang et. al, (2009), Zhang, (2009), Angelo et. al, (2010), Haldar et. al, (2010), Wojtowicz and Ogiela, (2012), Husain (2012), Chandrakar and Bagga, (2013), Sarkar and Sanyal, (2014), Farooq et. al, (2015), Verma and Jha, (2015), Tyagi and Singh, (2016), Pal et.al, (2018), Mohanarathinam et. al, (2019))* is performed and the techniques are classified based on their domain (spatial or frequency), characteristics, functionality, approach and granularity. Authors *Kaur and Kaur (2013)* performed a comparison of digital watermarking with other data hiding techniques such as steganography, fingerprinting, cryptography and digital signature. *Tao et. al. (2014)* performed a review of various frequency / transform domain watermarking techniques on the basis of theoretical analysis and their performance.

### 5.1. Performance Evaluation of Watermarked Image

The most frequently used quality metrics *(Naveed et. al, (2015) and Allaf and Kbir, (2019))* are used for evaluating the performance of the watermarked image are Mean Square Error (MSE), Peak-Signal-to-Noise Ratio (PSNR), Structural Similarity (SSIM), Euclidean distance (ED). Other used quality metrics *(Kuttera and Petitcolas, 1999)* are: Image Fidelity (IF), Normalized Mean Square Error (NMSE) and Correlation Quality (CQ). The Peak-Signal-to- Noise Ratio (PSNR) is measured in decibels and is the most commonly used metrics for measuring the ratio of noise between the original and watermarked image. Desirable PSNR value should be greater than 30 dB. In order to get a good quality watermarked image large PSNR and small MSE values are desirable *Potdar et. al (2005)*. PSNR is calculated as:

$$PSNR(I, Iw) = 10 \times \log_{10} \frac{(MAXI^2)}{MSE}$$

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

*where,*

$MAX_I$ is the maximum possible pixel value of the original image *I* (for an image representedwith 8 bits the MAXI = 255)

MSE is the Mean Square Error between the original and the watermarked image and ismeasured as:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} (I(i,j) - I_w(i,j))^2$$

where,

*I (i, j)* represent the original image

*Iw (i, j)* is the watermarked image

*M x N* is the dimensions of the image

A review of digital watermarking techniques classified based on the domain in which they are inserted is presented. Section 5.2 discusses the techniques based on spatial domain while thosebased on the frequency or transform domain is discussed in section 5.3.

### 5.2. Spatial Domain Techniques

The spatial domain algorithms for embedding a watermark are directly applied on the pixels of the host image. A digital watermark is embedded into the host image using various techniquessuch as: in the form of LSB *(Schyndel et. al, (1994), Bamatraf et. al, (2010))*, by using the statistical characteristics of the pixel or by hiding the watermark in the texture part of the image *(Xuehua, 2010)*. The watermarking techniques which embed the information into the LSB of the host image are less likely to produce visual artifacts in the image (*Yeung and Mintzer, 1997)*. Moreover, the LSB of the image gets modified with any alteration in image, and therefore image verification becomes easier. But it is also to be noted that altering an image without modifying the LSB is not very difficult and in this case image verification based on LSB fails to detect an altered image. Using LSB approach fails to determine the modified areas in the image. To overcome the drawbacks of the approaches based on modification of LSB of the image, an invisible watermarking technique for protecting the integrity of the image has been proposed by authors *Yeung and Mintzer (1997)*. Their approach was used to verify if anypart of the image had undergone any changes. The approach consisted of two processes; watermark embedding with generation of verification key and extraction. In the first step the watermark image was embedded into the host image and generated a

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

pseudo random number referred as a verification key. In the second step the embedded watermark was decoded from the host image based on the verification key and then extracted for verification. *Singh et. al (2012)* proposed a method to convert the watermark into an 8-bit image and then embed it to the LSB of the original image. Thereafter, during the extraction process, the watermark was scaled to check the quality of the watermarked image.

Cryptographic algorithms and hashing were used in various ways with the spatial domain watermarking techniques for securing the watermark along with the host images. As suggested by *Friedman (1998)* a digital signature can be attached to an image which can either be encoded or can be secured using a hash function. With this approach, the digital signature attached with the image requires extra bandwidth and storage. Moreover, any changes made to the image can be detected but its position cannot be located. *Wong (1998)* in his technique used cryptography and hashing function for verifying the integrity and the ownership of the image. The image was verified by extracting the watermark from the watermarked image using a secretkey known only to the owner and a cryptographic hash function. With an inappropriate secret key, the obtained image was equivalent to random noise. The proposed technique was capable of detecting and localizing the changes in an image. *Fridrich et. al (2000)* proposed an index independent watermarking approach using an encryption mapping approach. The encryption mapping approach or the block cipher considered a block of local neighbours of a pixel. The image was authenticated by scanning each individual row. By using more than one pixel for encryption mapping the attacks on the image was prevented since some neighbours used in the mapping function had already been modified earlier. *Lin et. al (2005)* presented a hierarchicaldigital watermarking approach using parity checking, average intensities of the pixels and secret key with public chaotic algorithm for tamper recovery. Due to the hierarchical nature ofthe approach, the level of image inspection increased with the hierarchy and hence increased the accuracy of tamper localization. The proposed approach was quite sensitive to error pixels; i.e., for one tampered pixel in a block, the whole block was considered invalid. Later, as an extension to the approach by *Lin et. al (2005)*, *Lee and Lin (2008)* proposed a dual watermarking approach where two copies of watermark were kept for each non-overlapping block. The process was performed using three steps. During the first step, a watermark was embedded into an image. In the second step, the tampered blocks were detected using a 3-level hierarchical error block checking. In the third step, tampered blocks were recovered using 2- stage block recovery scheme. Another low-cost colour image watermarking approach for protecting the most valuable area in the image was by using quad tree for segmenting the image into large and small regions *(Phadikar et. al, 2009)*. The larger regions of the image are the regions having uniform intensities while the non-uniform portions depicting the critical information of the image were represented using the smaller regions. By inserting the encrypted watermark into the variable sized small region helped in protecting the image form attacks without any visual distortions.

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies Volume 1; Issue 1; January - March 2021

Authors *Surekha and Swamy (2011)* embedded binary watermark into the image using visual cryptography which created two shares of the watermark. One share of the watermark was superimposed on the host image while the other one was kept secret with the owner. Three techniques were proposed while embedding the watermark. The *single watermarking embedding* technique created public share and private share for embedding and extracting a binary watermark from the host image. It was extended to *multiple watermarking embedding* technique and *iterative watermark embedding* where the same binary watermark was embedded into different positions of the original image. The approaches were tested on different types of images against various attacks and it was found that the approaches failed to resist the rotation attack completely.

Other approaches were also used in the spatial domain watermarking techniques such as randomly modified the intensity of the pixels of the host image for protecting the copyright of digital images *(Nikolaidis and Pitas, 1998)*. In this process, during watermark detection, a comparison of the mean intensity values of marked and unmarked pixels was carried out. The proposed watermarking approach was resistant to JPEG compression and low passes filtering. Authors *Phiasai and Temdee (2014)* proposed a watermarking technique for protecting the copyright of facial images using phase correlation technique for embedding the watermark. Cropping a face from an image without the permission of the owner was prevented by embedding a binary watermark into the facial region of the image. The extraction of the watermark did not require the original image. In order to check if any image tampering had been done, the watermarked pixel was subtracted with the predicted pixel. Authors *Tiwari andSharma (2017)* presented an image authentication approach based on vector quantization (VQ) specifically suitable for aerial images. Robust and semi-fragile watermarks were embedded into the host image in successive two stages and therefore ensured double protection to the images. By combining robust watermarking with VQ ensured the security of the host image

whereas semi-fragile watermarks with VQ helped during the authentication of the received images. The approach was tested using PSNR and bit error rate threshold benchmarks.

### 5.2. Frequency Domain Techniques

The majorly used frequency domain methods are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) *(Farooq et. al, 2015)* and Discrete Slantlet Transform (DST) *(Mundher et. al, 2014)* as discussed in section 3.1. The frequency domain algorithms embed a watermark into the frequency/ transform domain of theimage and thereafter convert the image to spatial domain. *Fridrich (1998)* divided the image into larger blocks of size 64 x 64 for embedding a watermark into each block with the help of a secret key, block number and the content of the block. The

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

identification number of the camera used for capturing the image was considered as a secret key. In order to detect and verify the image, the author extracted few bits from each block and for each block the numberof correctly recovered blocks is added and the probability of getting correct blocks was calculated. The approach was found robust against noise and sharpening. Authors *Kundur andHatzinakos (1998)* used the DWT domain of the image for embedding the watermark into the host image. The approach helped in detecting tampered images and other distortions arising due to filtering and compression. The watermark was embedded by quantizing the co-efficientusing a user defined key such that any changes in the signal (image) would change the watermark. The difference in the embedded and extracted watermark depicted the changes made in the image.

*Fridrich and Goljam (1999)* proposed two techniques based on modulating the DCT co- efficient for embedding the watermark. In the first technique, the middle band of frequencies were modulated while the second technique modulated the lower band frequencies. Both the techniques were first converted into a standardized form for comparison and thereafter the other parameters such as the strength of the watermark, its threshold value (decision statistics) was adjusted. The techniques were implemented for embedding one of 1 -bit and another 60-bit watermark. Various transformations were applied on the images for testing the robustness of each watermarking technique. Based on the testing results, the author concluded that the second approach of modulating lower band frequencies gave better results for both 1-bit and 60-bit watermark.

Cryptographic algorithms were also used by researchers for embedding a secured watermark into the host image using the frequency domain. Authors *Tai and Chang (2003)* embedded a binary watermark logo into a host image by encrypting the bitmap form of the watermark image using DES algorithm and a secret key. A unique ID was generated with each image known only to the owner using which the encrypted watermark could be retrieved. The simulation of the algorithm depicted that it was robust against noise and cropping attacks. *Samuel and Penzhorn (2004)* presented a watermarking technique in which the watermark image was encrypted using AES algorithm and thereafter was hashed using Secure Hash Algorithm (SHA- 1). Using double encryption helped in ensuring the integrity of the watermark image. The watermark was embedded and extracted using DCT and the approach was found robust against scaling and cropping of the host image. *Tiwari et. al (2013)* in his proposed algorithm encrypted the digital watermark using DES algorithm and then embedded it into the original image after applying two-level DWT on it. The application of DES algorithm using a secret key ensured security of the watermark and the two-level DWT preserved the robustness of the approach. *Mundher et. al (2014)* used the DST of an image for embedding an encrypted watermark for ownership authentication. The encrypted watermark was converted into a random sequence of bits. Initially, the host image was divided into red, green and blue channels and the watermark

was embedded into all the three channels using DST. The performance evaluation was done by computing PSNR and the most suitable channel for embedding the watermark was selected. The experimental analysis of the approach was performed for collecting the initial results by applying salt and pepper noise and Poisson noise on the host image. The results concluded that the blue channel in their host image was most suitable for watermark embedding.

Bit decomposition technique was used for embedding multiple watermarks in an image *Niu et. al (2000)* in order to prevent the attackers from embedding his own watermark in the same image. The bit decomposition technique divides a gray level digital watermark into a series of binary images which were embedded into different positions of the original image. The robustness of the approach was tested by applying some image transformation functions to and it was observed that the approach was capable of resisting normal image processing operations and compression. *Wang et. al (2008)* proposed a fragile chaotic watermarking algorithm for the authentication of JPEG images. To embed a watermark into the host image, the DCT co- efficient of the image was directly modified after quantization. The proposed approach was less complex as computations for full decoding and re-encoding was avoided. The experimental results depicted that the approach was sensitive to tamper localization in the image. *Xuehua (2010)* applied a series of transformations on the host image using the DCT-based for protecting the embedded copyright information into a host image. The experimental observations proved that the DCT based approaches were resistant to compression, cropping, filtering and scaling. In order to compare the robustness of the watermarking approaches against various image transformations such as rotation, scaling, shearing and addition of noise, authors *Aparna and Ayyappan (2014)* performed an experimental analysis of different watermarking techniques based on DCT, DWT and a combination of DWT and DCT. The approaches were applied on the complete image and also after dividing the host image and watermark into four parts and the efficiency of the algorithms was measured using PSNR. The experimental results depicted that the algorithms based on the combination of DCT-DWT were robust against different attacks as compared to the other approaches in case of complete images. While in case of a divided images, the approach was resistant to noise attacks only.

## 6.0 Conclusion

In the present study, a comprehensive study about digital watermarking is performed. Since the widespread accessibility and sharing of multimedia data over the internet has resulted into severe challenges such as loss in originality of the images, threat of unauthorized possession, violation of copyright and intellectual property rights and security threat, embedding a digital watermark into the host image has been identified as one of the ways to protect the images against integrity attacks. The following conclusions are derived from the study:

https://doi.org/10.69974/glskalp.01.01.49
GLS KALP Journal of Multidisciplinary Studies
Volume 1; Issue 1; January - March 2021

- Digital watermarking has been identified as one of the better options for detecting and localizing tampered area in the images as compared to using only cryptographic algorithms for protecting the digital data.
- However, cryptographic algorithms and hashing functions were used to encrypt the digital watermark before embedding for providing security to the watermark.
- Initially, digital watermarking was used to protect multimedia data only but now its applications has been extended to secure the database systems also due to their increased usage in real-life applications.
- In order to protect the complete image from malicious attacks it is preferable to embed the watermark into a major portion of the host image rather than embedding only in the region of interest. Embedding the watermark into multiple portions of the host image, helps in easy detection and localization of tampered area.
- In order to have no visual difference between the host image and the watermarked image, the spatial domain techniques which embed the watermark into the LSB of the host image are preferred as they are less likely to produce visual artifacts in the image. Also, the LSB of the image gets modified with any alteration in image and therefore image verification becomes easier.
- On the other hand, sometimes the LSB approach also fails to determine the modified areas in the image since altering an image without modifying the LSB is not very difficult. In this case the modified areas in the image cannot be detected.

The frequency domain watermarking techniques provide better security as compared to the spatial domain techniques, but performing computations while recovering the watermark from the host image is quite complex.

## References

Abhinav, S., & Chandan, S. (2014). Medical image authentication through watermarking. *International Journal of Advanced Research in Computer Science & Technology*

Agrawal, R., & Srikant, R. (2000, May). Privacy-preserving data mining. In Proceedings of the 2000 ACM SIGMOD international conference on Management of data (pp. 439-450)

Agrawal, R., & , J. (2002, January). Watermarking relational databases. In VLDB'02: Proceedings of the 28th International Conference on Very Large Databases (pp. 155-166). Morgan Kaufmann

Agrawal, R., Haas, P. J., & Kiernan, J. (2003, June). A system for watermarking relational databases. In Proceedings of the 2003 ACM SIGMOD international conference on Management of data (pp. 674-674).

Amano, T., & Misaki, D. (1999, September). A feature calibration method for watermarking of document images. In Proceedings of the Fifth International Conference on Document Analysis and Recognition. ICDAR'99 (Cat. No. PR00318) (pp. 91-94). IEEE.

D'Angelo, A., Cancelli, G., & Barni, M. (2010). Watermark-based authentication. In Intelligent Multimedia Analysis for Security Applications (pp. 365-402). Springer, Berlin, Heidelberg.

Allaf, A. H., & Kbir, M. A. (2018, October). A review of digital watermarking applications for medical image exchange security. In The proceedings of the third international conference on smart city applications (pp. 472-480). Springer, Cham.

Al-Qershi, O. M., & Khoo, B. E. (2011). Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images. Journal of digital imaging, 24(1), 114-125.

Aparna, J. R., & Ayyappan, S. (2014, April). Comparison of digital watermarking techniques. In 2014 International conference on computation of power, energy, information and communication (ICCPEIC) (pp. 87-92). IEEE

Bamatraf, A., Ibrahim, R., & Salleh, M. N. B. M. (2010, December). Digital watermarking algorithm using LSB. In 2010 International Conference on Computer Applications and Industrial Electronics (pp. 155-159). IEEE

Bartolini, F., Tefas, A., Barni, M., & Pitas, I. (2001). Image authentication techniques for surveillance applications. Proceedings of the IEEE, 89(10), 1403-1418

Baharav, Z. Z., & Shaked, D. (1999, April). Watermarking of dither halftoned images. In Security and Watermarking of Multimedia Contents (Vol. 3657, pp. 307-316). International Society for Optics and Photonics.

Batthini, G., Chaudhary, A., & Chaudhari, S. P. (2015, December 11). Scholarly Journals in Entrepreneurship. Papers.ssrn.com. https://ssrn.com/abstract=2702276 or http://dx.doi.org/10.2139/ssrn.2702276

Bhattacharjya, A. K., & Ancin, H. (1999, October). Data embedding in text for a copier system. In Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348) (Vol. 2, pp. 245-249). IEEE.

Boreiry, M., & Keyvanpour, M. R. (2017, April). Classification of watermarking methods based on watermarking approaches. In 2017 Artificial Intelligence and Robotics (IRANOPEN) (pp. 73-76). IEEE.

Brassil, J., & O'Gorman, L. (1996, May). Watermarking document images with bounding box expansion. In International Workshop on Information Hiding (pp. 227-235). Springer, Berlin, Heidelberg.

Brassil, J. T., Low, S., & Maxemchuk, N. F. (1999). Copyright protection for the electronic distribution of text documents. Proceedings of the IEEE, 87(7), 1181-1196

Coatrieux, G., Lecornu, L., Sankur, B., & Roux, C. (2006, August). A review of image watermarking applications in healthcare. In 2006 International conference of the IEEE Engineering in Medicine and Biology Society (pp. 4691-4694). IEEE.

Chandrakar, N., & Bagga, J. (2013). Performance comparison of digital Image watermarking techniques: a survey. International Journal of Computer Applications Technology and Research, 2(2), 126-130

Chawla, G., Saini, R., & Yadav, R. (2012). Classification of watermarking based upon various parameters. International Journal of Computer Applications & Information Technology, 1(II).

Chen, M., Wong, E. K., Memon, N. D., & Adams, S. F. (2001, November). Recent developments in document image watermarking and data hiding. In Multimedia Systems and Applications IV (Vol. 4518, pp. 166-176). International Society for Optics and Photonics.

Chen, W. C., & Wang, M. S. (2009). A fuzzy c-means clustering-based fragile watermarking scheme for image authentication. Expert Systems with Applications, 36(2), 1300-1307.

Daraee, F., & Mozaffari, S. (2014). Watermarking in binary document images using fractal codes. Pattern Recognition Letters, 35, 120-129.

Dirik, A. E., & Memon, N. (2009, November). Image tamper detection based on demosaicing artifacts. In 2009 16th IEEE International Conference on Image Processing (ICIP) (pp. 1497-1500). IEEE.

Dong, P., Brankov, J. G., Galatsanos, N. P., Yang, Y., & Davoine, F. (2005). Digital watermarking robust to geometric distortions. IEEE Transactions on Image Processing, 14(12), 2140-2150.

Aditya, T. S. (2010, December). Survey on passive methods of image tampering detection. In 2010 International Conference on Communication and Computational Intelligence (INCOCCI) (pp. 431-436). IEEE.

Farfoura, M. E., Horng, S. J., Lai, J. L., Run, R. S., Chen, R. J., & Khan, M. K. (2012). A blind reversible method for watermarking relational databases based on a time-stamping protocol. Expert Systems with Applications, 39(3), 3185-3196.

Farooq, O., Khan, Y. U., Gupta, B., & Datta, S. (2006). Wavelet based tamper-proofing of digital images. IETE Technical Review, 23(6), 349-356.

Fridrich, J. (1998, October). Image watermarking for tamper detection. In Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No. 98CB36269) (Vol. 2, pp. 404-408). IEEE.

Fridrich, J., & Goljan, M. (1999, April). Comparing robustness of watermarking techniques. In Security and Watermarking of Multimedia Contents (Vol. 3657, pp. 214-225). International Society for Optics and Photonics.

Fridrich, J., Goljan, M., & Baldoza, A. C. (2000, September). New fragile authentication watermark for images. In Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101) (Vol. 1, pp. 446-449). IEEE.

Friedman, G. L. (1993). The trustworthy digital camera: Restoring credibility to the photographic image. IEEE Transactions on consumer electronics, 39(4), 905-910.

Gull, S., Loan, N. A., Parah, S. A., Sheikh, J. A., & Bhat, G. M. (2020). An efficient watermarking technique for tamper detection and localization of medical images. Journal of ambient intelligence and humanized computing, 11(5), 1799-1808.

Gunjal, B. L., & Mali, S. N. (2012). ROI based embedded watermarking of medical images for secured communication in telemedicine. International Journal of Computer and Information Engineering, 6(8), 997-1002.

Guo, J. (2011, May). Fragile watermarking scheme for tamper detection of relational database. In 2011 International Conference on Computer and Management (CAMAN) (pp. 1-4). IEEE.

Zhou, G., & Lv, D. (2011, April). An overview of digital watermarking in image forensics. In 2011 Fourth International Joint Conference on Computational Sciences and Optimization (pp. 332-335). IEEE.

Hacigumus, H., Iyer, B., & Mehrotra, S. (2002, February). Providing database as a service. In Proceedings 18th International Conference on Data Engineering (pp. 29-38). IEEE.

Halder, R., Pal, S., & Cortesi, A. (2010). Watermarking Techniques for Relational Databases: Survey, Classification and Comparison. J. Univers. Comput. Sci., 16(21), 3164-3190.

Hartung, F., & Kutter, M. (1999). Multimedia watermarking techniques. Proceedings of the IEEE, 87(7), 1079-1107.

Hu, J., & Grefen, P. W. P. J. (2002, August). Component based system framework for dynamic b2b interaction. In Proceedings 26th Annual International Computer Software and Applications (pp. 557-562). IEEE.

Hu, S. (2005, March). Document image watermarking algorithm based on neighborhood pixel ratio. In Proceedings. (ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. (Vol. 2, pp. ii-841). IEEE.

Huang, H., Guo, W., & Zhang, Y. (2008, December). Detection of copy-move forgery in digital images using SIFT algorithm. In 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application (Vol. 2, pp. 272-276). IEEE.

Husain, F. (2012). A survey of digital watermarking techniques for multimedia data. MIT International Journal of Electronics and Communication Engineering, 2(1), 37-43.

Kaur, G., & Kaur, K. (2013). Digital watermarking and other data hiding techniques. International Journal of Innovative Technology and Exploring Engineering, 2(5), 181-183.

Khanduja, V., Khandelwal, A., Madharaia, A., Saraf, D., & Kumar, T. (2012, October). A robust watermarking approach for non-numeric relational database. In 2012 International Conference on Communication, Information & Computing Technology (ICCICT) (pp. 1-5). IEEE.

Khanduja, V., Chakraverty, S., Verma, O. P., Tandon, R., & Goel, S. (2014, February). A robust multiple watermarking technique for information recovery. In 2014 IEEE International Advance Computing Conference (IACC) (pp. 250-255). IEEE.

Khanduja, V. (2017). Database watermarking, a technological protective measure: Perspective, security analysis and future directions. Journal of information security and applications, 37, 38-49.

Khanna, S., & Zane, F. (2000, February). Watermarking maps: hiding information in structured data. In Proceedings of the eleventh annual ACM-SIAM symposium on Discrete algorithms (pp. 596-605).

Zhao, J., & Koch, E. (1995, August). Embedding Robust Labels into Images for Copyright Protection. In KnowRight (pp. 242-251).

Kundur, D., & Hatzinakos, D. (1998, October). Towards a telltale watermarking technique for tamper-proofing. In Proceedings 1998 International Conference on Image Processing. ICIP98 (Cat. No. 98CB36269) (Vol. 2, pp. 409-413). IEEE.

Kutter, M., & Petitcolas, F. A. (1999, April). Fair benchmark for image watermarking systems. In Security and watermarking of multimedia contents (Vol. 3657, pp. 226-239). International Society for Optics and Photonics.

Lee, T. Y., & Lin, S. D. (2008). Dual watermark for image tamper detection and recovery. Pattern recognition, 41(11), 3497-3506.

Lin, P. L., Hsieh, C. K., & Huang, P. W. (2005). A hierarchical digital watermarking method for image tamper detection and recovery. Pattern recognition, 38(12), 2519-2529.

Low, S. H., Lapone, A. M., & Maxemchuk, N. F. (1995, November). Document identification to discourage illicit copying. In Proceedings of GLOBECOM'95 (Vol. 2, pp. 1203-1208). IEEE.

Low, S. H., Maxemchuk, N. F., Brassil, J. T., & O'Gorman, L. (1995, April). Document marking and identification using both line and word shifting. In Proceedings of INFOCOM'95 (Vol. 2, pp. 853-860). IEEE.

Low, S. H., Maxemchuk, N. F., & Lapone, A. M. (1998). Document identification for copyright protection using centroid detection. IEEE Transactions on Communications, 46(3), 372-383.

Low, S. H., & Maxemchuk, N. F. (1998). Performance comparison of two text marking methods. IEEE Journal on Selected Areas in Communications, 16(4), 561-572.

Mahdian, B., & Saic, S. (2009, February). Detection and description of geometrically transformed digital images. In Media Forensics and Security (Vol. 7254, p. 72540J). International Society for Optics and Photonics.

Mahdian, B., & Saic, S. (2009, December). A Cyclostationarity Analysis Applied to Scaled Images. In International Conference on Neural Information Processing (pp. 683-690). Springer, Berlin, Heidelberg.

Matsui, K. (1994). Video steganography: -how to secretly embed a signature in a picture. IMA Intellectual Property Project Proc., 1994, 1, 187-206.

Maxemchuk, N. F., & Low, S. H. (1997, October). Marking Text Documents. In ICIP (3) (p. 13).

Megalingam, R. K., Nair, M. M., Srikumar, R., Balasubramanian, V. K., & Sarma, V. S. V. (2010, February). Performance comparison of novel, robust spatial domain digital image watermarking with the conventional frequency domain watermarking techniques. In 2010 International Conference on Signal Acquisition and Processing (pp. 349-353). IEEE.

Mei, Q. G., Wong, E. K., & Memon, N. D. (2001, August). Data hiding in binary text documents. In Security and watermarking of multimedia contents III (Vol. 4314, pp. 369-375). International Society for Optics and Photonics.

Memon, N. A., Chaudhry, A., Ahmad, M., & Keerio, Z. A. (2011). Hybrid watermarking of medical images for ROI authentication and recovery. International Journal of Computer Mathematics, 88(10), 2057-2071.

Mohanarathinam, A., Kamalraj, S., Prasanna Venkatesan, G. K. D., Ravi, R. V., & Manikandababu, C. S. (2020). Digital watermarking techniques for image security: a review. Journal of Ambient Intelligence and Humanized Computing, 11(8), 3221-3229.

Kirovski, D. (2006). Multimedia watermarking techniques and applications. CRC Press.

Muharemagic, E. and Furht, B. (2001). Multimedia watermarking techniques and applications

Mundher, M., Muhamad, D., Rehman, A., Saba, T., & Kausar, F. (2014). Digital watermarking for images security using discrete slantlet transform. Applied Mathematics & Information Sciences, 8(6), 2823.

Naveed, A., Saleem, Y., Ahmed, N., & Rafiq, A. (2015). PERFORMANCE EVALUATION AND WATERMARK SECURITY ASSESSMENT OF DIGITAL WATERMARKING TECHNIQUES. Science International, 27(2).

Nikolaidis, N., & Pitas, I. (1998). Robust image watermarking in the spatial domain. Signal processing, 66(3), 385-403.

Niu, X. M., Lu, Z. M., & Sun, S. H. (2000). Digital watermarking of still images with gray-level digital watermarks. IEEE Transactions on Consumer Electronics, 46(1), 137-145.

Pal, P., Singh, H. V., & Verma, S. K. (2018, May). Study on watermarking techniques in digital images. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 372-376). IEEE.

Pan, H. K., Chen, Y. Y., & Tseng, Y. C. (2000, July). A secure data hiding scheme for two-color images. In Proceedings ISCC 2000. Fifth IEEE Symposium on Computers and Communications (pp. 750-755). IEEE.

Phadikar, A., Maity, S. P., & Rahaman, H. (2009, March). Region Specific Spatial Domain Image Watermnarking Scheme. In 2009 IEEE International Advance Computing Conference (pp. 888-893). IEEE.

Phiasai, T., Chamnongthai, K., & Temdee, P. (2014, May). A method for watermarking on facial images. In 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE) (pp. 1-4). IEEE.

Piva, A. (2013). "An overview of image forensics," ISRN Signal Processing, Hindawi.

Podilchuk, C. I., & Zeng, W. (1998). Image-adaptive watermarking using visual models. IEEE Journal on selected areas in communications, 16(4), 525-539.

Podilchuk, C. I., & Delp, E. J. (2001). Digital watermarking: algorithms and applications. IEEE signal processing Magazine, 18(4), 33-46.

Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. (pp. 709-716). IEEE.

Qu, Z., Qiu, G., & Huang, J. (2009, June). Detect digital image splicing with visual cues. In International workshop on information hiding (pp. 247-261). Springer, Berlin, Heidelberg.

Samuel, S., & Penzhorn, W. T. (2004, September). Digital watermarking for copyright protection. In 2004 IEEE Africon. 7th Africon Conference in Africa (IEEE Cat. No. 04CH37590) (Vol. 2, pp. 953-957). IEEE.

Sarkar, T., & Sanyal, S. (2014). Digital watermarking techniques in spatial and frequency domain. arXiv preprint arXiv:1406.2146.

Van Schyndel, R. G., Tirkel, A. Z., & Osborne, C. F. (1994, November). A digital watermark. In Proceedings of 1st international conference on image processing (Vol. 2, pp. 86-90). IEEE.

Singh, A. K., Sharma, N., Dave, M., & Mohan, A. (2012, December). A novel technique for digital image watermarking in spatial domain. In 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing (pp. 497-501). IEEE.

Singh, H. V., & Rai, A. (2019). Medical image watermarking in transform domain. In Smart Innovations in Communication and Computational Sciences (pp. 485-493). Springer, Singapore.

Surekha, B., & Swamy, G. N. (2011). A spatial domain public image watermarking. International Journal of Security and Its Applications, 5(1), 1-12.

Tai, G. C., & Chang, L. W. (2003, October). A novel public digital watermarking for still images based on encryption algorithm. In IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003. Proceedings. (pp. 264-267). IEEE.

Tao, H., Chongmin, L., Zain, J. M., & Abdalla, A. N. (2014). Robust image watermarking theories and techniques: A review. Journal of applied research and technology, 12(1), 122-138.

Tiwari, A., & Sharma, M. (2018). An Image Authentication Algorithm Using Combined Approach of Watermarking and Vector Quantization. Journal of Intelligent Systems, 27(1), 31-45.

Tiwari, N., Ramaiya, M. K., & Sharma, M. (2013, February). Digital Watermarking using DWT and DES. In 2013 3rd IEEE International Advance Computing Conference (IACC) (pp. 1100-1102). IEEE.

Tseng, Y. C., & Pan, H. K. (2001, April). Secure and invisible data hiding in 2-color images. In Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213) (Vol. 2, pp. 887-896). IEEE.

Tyagi, S., Singh, H. V., Agarwal, R., & Gangwar, S. K. (2016, March). Digital watermarking techniques for security applications. In 2016 International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESES) (pp. 379-382). IEEE.

Verma, V. S., & Jha, R. K. (2015). An overview of robust digital image watermarking. IETE Technical review, 32(6), 479-496.

De Vleeschouwer, C., Delaigle, J. F., & Macq, B. (2002). Invisibility and application functionalities in perceptual watermarking an overview. Proceedings of the IEEE, 90(1), 64-77.

Wang, H., Ding, K., & Liao, C. (2008, April). Chaotic watermarking scheme for authentication of JPEG Images. In 2008 International Symposium on Biometrics and Security Technologies (pp. 1-4). IEEE.

Wang, F. H., Pan, J. S., & Jain, L. C. (2009). Digital watermarking techniques. In Innovations in Digital Watermarking Techniques (pp. 11-26). Springer, Berlin, Heidelberg.

Wójtowicz, W., & Ogiela, M. R. (2012). Security issues on digital watermarking algorithms. Annales Universitatis Mariae Curie-Sklodowska, sectio AI–Informatica, 12(4), 123-139.

Wolfgang, R. B., Podilchuk, C. I., & Delp, E. J. (1999). Perceptual watermarks for digital images and video. Proceedings of the IEEE, 87(7), 1108-1126.

Wong, P. W. (1998, May). A watermark for image integrity and ownership verification. In PICS (pp. 374-379).

Wu, M., Tang, E., & Lin, B. (2000, July). Data hiding in digital binary image. In 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast-Changing World of Multimedia (Cat. No. 00TH8532) (Vol. 1, pp. 393-396). IEEE.

Xuehua, J. (2010, May). Digital watermarking and its application in image copyright protection. In 2010 International Conference on Intelligent Computation Technology and Automation (Vol. 2, pp. 114-117). IEEE.

Yeung, M. M., & Mintzer, F. (1997, October). An invisible watermarking technique for image verification. In Proceedings of international conference on image processing (Vol. 2, pp. 680-683). IEEE.

Zhang, Y. (2009, June). Digital watermarking technology: A review. In 2009 ETP international conference on future computer and communication (pp. 250-252). IEEE.