Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 100-112
https://doi.org/10.56471/slujst.v6i.366

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Robust Watermarking Techniques for the Authentication and Copyright Protection of Digital Images: A Survey

Godwin Ugwu Onoja[1]*, Mustapha Aminu Bagiwa[2] and Aliyu Mohammad Kufena[3]
[1, 2,3]Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria.
[1]Department of Computer Science, Joseph Sawuan Tarka University, Makurdi, Nigeria.
onojason2003@yahoo.com[1*]

*Corresponding Author

Abstract

Digital image authentication and security are crucial concerns for the digital revolution since any image may be readily tampered with. Digital watermarking schemes were since been utilized to tackle a range of problems over time and involving the verification of digital images and copyright protection. In a real-world setting, watermarked contents are frequently subject to a succession of assaults which makes it necessary to strike a balance between resilience and imperceptibility in the face of attacks. There are numerous hazards to this, and numerous watermarking techniques have been created to counter them. Data with less perceptual distortion should be able to be included in a real watermarking technique in addition to restoring the original cover content. As a result, robustness, imperceptibility, and security are three crucial criteria for digital content's authentication and copyright preservation. This study therefore presents a careful review of some cutting-edge watermarking technologies used for copyright protection and authentication so as to identify their strengths and limitations. For clarity, this study shall explain some basic concepts of digital watermarking as well as the various forms of attacks on watermarks. The contributions from this work will be useful to researchers aim at developing efficient watermarking techniques.

Keywords: *Image Watermarking, Robustness, Image Authentication, Copyright Protection, hybrid domain, Geometric Attacks*

1. Introduction

Nowadays, content owners are keenly in search of technologies that will be capable of protecting their rights as well as secure their Information hiding therefore becomes a very vital issue in our current world of ever advancing technology. Information hiding is simply the masking of information such that an observer is unaware of its presence (Woo, 2007). The fundamental methods to conceal facts are cryptography, steganography and watermarking (Desai, 2012). Although facts hiding covers all three approaches, they nevertheless vary in their power and function. The sciences of cryptography involve sending communications in a unique way such that only the intended recipients can remove the mask and access the data, whereas steganography often refers to "covered writing" in which conversations are usually done secretly.

Despite the fact that digital content has long been protected with cryptographic techniques, decrypted data need extra security measures. A piece of artwork, for example, might be legitimately purchased but illegally transferred to others over peer-to-peer networks. Watermarking however is the embedding of content-dependent information that comes. Watermarks on paper currency and company official documents are examples of digital watermarks that are commonly used to verify their legitimacy. Equivalently, digital watermarking is used to verify the information included in digital contents because, as part of the content, it can help safeguard encrypted content even further. (Woo, 2007).

A modern and practical technology that can be used to authenticate and safeguard images is digital watermarking. A piece of data that is directly put on media is known as a digital watermark. It is undetectable by humans but easily

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

detectable by computers (Usman, 2010). The owner's data can be encoded using a watermarking technology, which is then preserved or disseminated over the Internet (Alzahrani, 2022). A good watermarking approach should be able to include data with little perceptual modification while also restoring the original cover material (Usman, 2010). Every digital image is susceptible to attacks thereby altering the authenticity and copyright protection of such image(s). Interestingly, with watermarking approach, it is possible to know that a digital image originally belongs to a particular owner (i.e., copyright protection) and that even when it has been tampered with by an attacker could be restored to its original form (i.e., authentication).

The methodology employed in this survey are;

- Examine and identifying the challenges of "information hiding" and the place of digital watermarking in Data protection and preservation
- Review current trends in image watermarking
- Look at techniques that perfectly fulfill some of the specifications for image watermarking
- Outline difficulties that should be resolved in upcoming research.

This paper therefore consists of five major sections which include; the introduction to "information hiding" methods as well as the viability of digital watermarking. Secondly, a brief history of watermarking and how it all started is described. Thirdly, an overview of digital watermarking approaches based on domain and applicability is also discussed. Next is a review of related "watermarking techniques on image authentication and copyright protection" after which the paper was concluded.

2. A Synopsis of digital watermarking's History

The practice of concealing data in another medium is quite old, as demonstrated by steganography. The phrase "digital watermarking" did, however, not become popular until 1993, when Tirkelet al. (1993) proposed two methods for concealing data in photographs. These techniques are based on the modification of (Least Significant Bit) LSB pixel values. UKEssays, 2018). But paper watermarking had already begun before that, in Italy in the 13th century, about 1282 AD, when tiny wire designs were imprinted on paper molds to produce watermarks (Cox, Miller, and Bloom, 2002). But in the seventeenth century, their use swiftly spread throughout Europe. At this period, watermarks were employed to identify the paper manufacturer or trade guild that produced the paper.

Today, watermarks are still employed as manufacturer's marks and to deter counterfeiting. The German word wassermarke, which denotes a distinctive mark on paper, is said to have been the source of the English word watermark in the 18th century. In 1954, Muzak secured a patent for watermarking musical works; it was used up until about 1984. (Miller and Cox, 2002). The phrase "digital watermarking" was first used by Tirkelet al. (1993), and this is when the field of digital watermarking really began to take off.

Blind watermarking, introduced by Pivaet al. (1997) in 1997, does not depend on the original cover work to identify the watermark signal (Barni and Bartolini, 2004). After that, the majority of the study focused on developing novel algorithms based on the spread spectrum-based embedding and blind detection concepts. Chen and Wornell (2001) employed the idea of quantization index modulation-based embedding of a watermark signal to create the third significant advancement in watermarking. Informed embedding, coding-based watermarking, reversible watermarking, fragile watermarking for authentication, and semi-fragile watermarking systems are some of the most recent advancements in watermarking technology (Barni and Bartolini, 2004). Today, watermarks are still employed as manufacturer's marks and to thwart fraud and other nefarious actions.

3. Digital Watermarking

Applying a watermark to a multimedia file is known as digital watermarking (Mahbuba and Mohammad, 2020). Any digital material, including images, audio, and video, has the potential to conceal data. Digital information may be illegally retained, copied when conveyed across a digital transmission medium. Watermarking digital images is another method of assuring tamper resistance, intellectual property ownership, and the secrecy of multimedia content.

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 100-112
https://doi.org/10.56471/slujst.v6i.366
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Watermarking systems for digital images may be modeled as a procedure for communication comprising an embedder as well as a detector. To begin, a stego image is created by subtly implanting a watermark signal into a host image. The signal requires no additional storage capacity. The picture of the stego is then conveyed to the customer. During this procedure, distortions due to unintended alteration, mischievous assaults, and data compression may occur. Eventually, a watermark detector is utilized to determine if a possibly deformed image contains a watermark (Woo, 2007). Watermark "embedding" and "extraction" are the two essential components of the process of digital image watermarking for a secured communication framework. At the section of the watermark insertion, the cover picture undergoes pre-processing, and after that, the image's entropy is calculated. The encoder then adds a watermark image to the cover image's high entropy value using optical image coding technology and a secret key. Before creating the watermarked image, the method then gathers data on the phase-shape as well as on the amplitude of the laser beam. Figure 1 shows how to embed the watermark (Mahbuba and Mohammad, 2020).

Watermark embedding approach, yields a watermarked image $D_{W,}$ as expressed by equation 1.

$$\text{WatermarkedImage} D_w = E(I, ETP, W, K) \quad (1)$$

where E denotes "the encoding algorithm", I denote "the host image", ETP represents "the information entropy", W denotes "the watermark image", and "the security key" is represented by K.

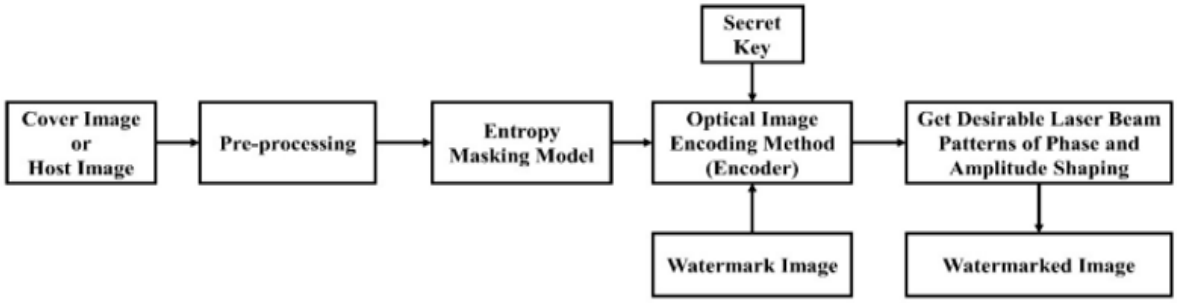

Figure 1: Flow Diagram of Watermark Embedding process

The following stage consists of determining how and in what method the watermark can be successfully extracted from the host image. At this stage, the watermarked image is again preprocessed. Thereafter the algorithm collects the phase shaping data as well as the amplitude from the laser beam patterns. After the collection is successfully done, the entropy of all the involved beam patterns is computed. To guarantee increased robustness and imperceptibility, a high entropy value is employed for watermark extraction. Figure 2 depicts how a decoder usually decodes the given image to produce or find the watermark image by means of the same key (Mahbuba and Mohammad, 2020).

The watermark extraction procedure is also defined by equation 2.

$$\text{Watermark Image } W^{!} = e(D_w, K, ETP, I) \quad (2)$$

where, W^1 is the watermark image, the encoding algorithm is represented by e(.), the cover image is represented by I, the information entropy is represented by ETP, and the security key is represented by K.

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 100-112
https://doi.org/10.56471/slujst.v6i.366
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

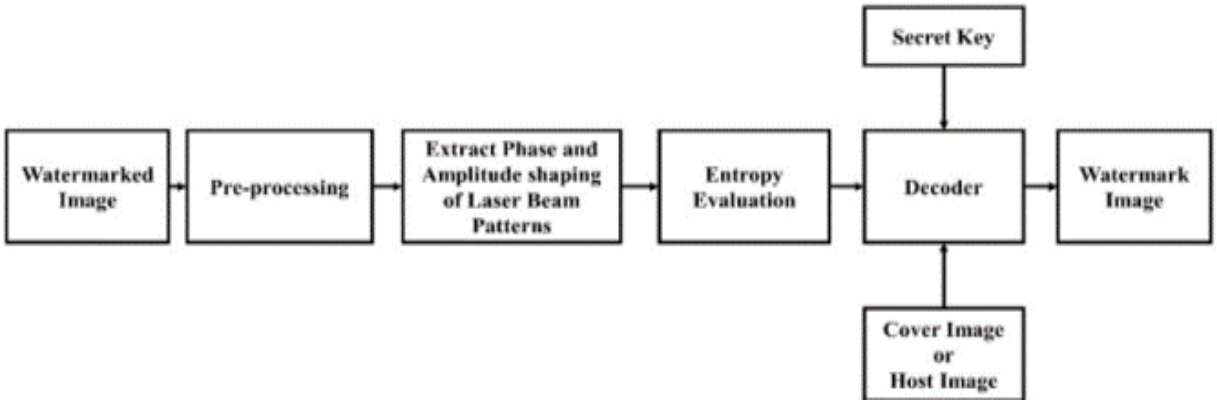

Figure 2: Flow Diagram of a watermark Extraction process.

3.1 Digital Image Watermarking Techniques

To have a better understanding on the working domains, this study shall look into the different digital image watermarking techniques.

3.1.1 Watermarking Approaches in Spatial Domain

By using a range of techniques in the spatial or temporal domain that are selected by the owner(s), this technology incorporates watermark data into the host image. "Least significant bit (LSB) modification algorithms, intermediate significant bits (ISB), and patchwork algorithms" are some of the methods used in this domain. These techniques have an immediate impact on the pixels of the original image. By altering the pixel values according to the author's logo or signature data, the watermark can be added (Olanrewaju, 2011). Spread spectrum and correlation-based algorithms are further strategies related to this field. In some pixels of a color or grayscale picture, the bit that has the lowest-order is transposed.

The bit with lowest order particular pixels of a color or grayscale image is flipped in the majority of systems, which use pixel intensities at designated positions in space to represent images. In accordance with the value of the pixel's intensity at such designated positions, the resultant watermark could be noticeable or hidden. These tactics can embed large amounts of data; however, the injected material may be easily detected by many attackers (Mukherjee, 2004). A single remaining watermark will be regarded as a success despite losing most of the photos as a result of many attacks because a little object can be implanted more than a few times.

3.1.1.1 The Intermediate Significant Bit (ISB) modification approach

By keeping the watermark pixels that are close to a completely filled or unfilled region in the source image pixels, ISB techniques replace the pixels of the actual image with those of the watermark. The actual or "original" image-file pixel is positioned within any of the range's edges after the watermark pixel value has been compared to the bitplane range (Jane, 2014). Grayscale images comprise eight-bit planes, the first of which contains the MSB while the eighth of the bit planes occupies the LSB, and then the rest two to seven are utilized as the ISB (Zeki et al., 2020). Robustness does not decrease in the face of geometric transformation attacks like scaling and rotation, where pixel intensities are unaffected by their new locations.

3.1.1.2 Patchwork approach

A statistical technique known as "Patchwork" combines redundant pattern encoding using a Gaussian distribution to covertly insert itself into an original image. The image information of the first patch (A) is degraded and that of the second patch (B) is darkened. A pseudo-random choice of two patches is made in situations as this and further asymmetrical coding, feature recognition, or both may be used to boost resistance, but scaling, translation, or rotation prior to decoding may cause the code to be lost. Patchwork loses precision even though it is resistant to cropping. The "pseudo-random bitstream" is produced by means of picking pairs of pixels from the main image. The "bit of information" d, which stands for the distinction that exists between the two pixels, encoded into the pair; if $d = 0$ or if $d > 0$, the encoding

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 100-112
https://doi.org/10.56471/slujst.v6i.366
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

is 0 and the pixels are reversed. "The next pair can be advanced if d is found to be bigger than a predetermined threshold or it is found to be equal to zero (Singh and Chadha, 2013)". This method doesn't work well with text graphics, but it does with large areas of random texture. "A region of the image with a randomly occurring texture pattern is replicated to an adjacent area of the image and each texture region is recovered using autocorrelation (Wu et al., 2020)".

Patchwork procedures are usually found to be more resistant to non-geometric image alterations, as the process does not affect the original image's content (Mahbuba and Mohammad, 2020)

3.1.2 The frequency (or transform) domain watermarking algorithms

This technique transforms image(s) that is/are represented in a frequency domain by using a pre-defined transform (Mahbuba, 2020). The original image's transform domain coefficients are eventually subjected to modification using a variety of transforms, such as the "discrete cosine transform (DCT)", "discrete Fourier transform (DFT)", "discrete wavelet transform (DWT)", "singular value decomposition (SVD)", "Hadamard", "cat", "FFT", "PHT", and "Fresnel transform", among others, to embed the watermark. In the end, it employs an inverse transformation and a correct key to extract the watermark. "To recreate the original signal in the frequency domain, the frequency components of each sinusoid of an image must be recombined by adding phase shift information (Tao et al, 2014)". Many efforts in the transform domain show improved reliability, robustness as well as imperceptibility as counter proofs to many assaults like compression, noise, filtering, cutting, and rotation. The transform domain Techniques are discussed briefly here.

3.1.2.1 The Discrete Cosine Transform (DCT)

A Fourier transform with a small amount of data points is referred to as the DCT. Only real numbers may be used in this situation. Discrete cosine transforms which is known by the acronym (DCT) by altering frequency content, splits a picture into its suitable frequency coefficients, which are sums of cosine functions that represent frequency components. The volatility of the DCT coefficients determines their usefulness. Take for an instance, the DCT is critical for the reduction of image(s) in the JPEG image format.

3.1.2.2. The Discrete Fourier Transform (DFT)

"Discrete Fourier transform" which is generally referred to by the acronym DFT, has the characteristic of distributing samples equally. In this case, the "discrete-time Fourier transform (DTFT)" changes a series of predefined length samples of a function into a succession of identical-length samples with equal spacing. The DTFT employs a series of intricate exponential functions that are harmonically coupled. The original input sequence is represented in the frequency domain by the DFT, which then generates a discrete and periodic signal. Applications for DFT include Fourier analysis, sinusoidal spectrum analysis, filters, combination operations, image processing, and signal processing (Mahbuba and Mohammad, 2020).

3.1.2.3. The Discrete Wavelet Transform (DWT)

A transformation based on mathematical concepts that breaks down a signal into wavelet instead of frequencies is referred to as discrete wavelet transform (DWT). One uniqueness of this procedure is that the wavelets are discretely sampled. One great benefit of DWT above Fourier transforms is the temporal resolution (i.e., DCT and DFT). The signal is decomposed using a collection of wavelets, which are mathematical in nature. The fundamental DWT image watermarking algorithm transforms an actual image into three (3) distinct stages. To insert the watermark, the sub-bands "LH3, HH3, and HL3" are used at three (3) dissimilar levels. Sub bands occupy a broad part of the image's frequency spectrum and that eventually makes the system's robustness to improve (Najafi, 2017). According to Mahbuba and Mohammad (2020), "the wavelet transform can be used in digital signal processing, image compression, and signal noise reduction". "In DWT approach, the system inserts the watermark into the cover image using an algorithm and afterwards uses the inverse DWT (IDWT) to retrieve the watermarked image knowing well that when adopting a wavelet transform, high frequency resolution may be acquired at low frequencies and high time resolution can be produced at high frequencies (Mahbuba and Mohammad, 2020)".

3.1.2.4 Singular Value Decomposition (SVD)

One great approach that effectively retrieve watermark even after alteration is the Singular value decomposition (SVD) methodology. It is mathematically defined as the result of a real or complex matrix. The SVD approach extends

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

the polar decomposition to generalize the eigen decomposition of a symmetric matrix with non-negative eigenvalues to any m n matrix. The SVD transformation has a very high applicability in statistics and digital signal processing, hence the reason why it is widely used. This approach can effectively retrieve the watermark even after alteration, hence, simulation results showed that the watermarked image had a greater quality and was more resistant to different attacks when compared to prior techniques.

3.1.3 Hybrid domain watermarking algorithm

This technique combines the spatial and the transform domain approaches to provide robustness and improve the data insertion qualities. The combination could include (spatial + transform) domains (shih and Wu, 2003), (Spatial + Spatial) domains, (Transform + Transform) domain (Kumar, 2019) as well as in other multiple combination form (Sridhar, 2018). Several studies carried out revealed that the hybrid domain watermarking techniques usually outperform the spatial as well as the transform domain techniques seeing that it combines the strength of multiple techniques.

4. Review of Related works on Image Authentication and Copyright Protection

Digital watermarking as one of the most efficient ways to hide information can be accomplished using spatial, transform or hybrid domains. We hereby present some related works with respect to the domains for clarity of the digital watermarking concept.

4.1 Spatial Domain Watermarking Techniques

Yeo and Kim (2003) suggested a generalized patchwork approach based on additive and multiplicative patchworks. Using statistical data, the approach embeds and identifies the watermark. In order to accurately identify watermark data, the approach utilizes what is known as location-shift as well as scale-shift techniques. Their proposed scheme has demonstrated some high level of resilience to compression attacks. The watermark may be added to an image using redundant pattern encoding and erased with a secret key connected to the decoding process. This algorithm is ideal. Used for huge expanses of random texture image, but has limited robustness against random bend attacks.

Hajjaji*et al.* (2011) proposed medical image watermarking, which entails embedding a collection of data into a medical image. The watermarking approach checks the integrity and confidentiality of medical information and maintains patient and hospital data confidentiality by using the least significant bits (LSBs). At a compression rate of 10%, the watermark is effectively retrieved. Although this approach is utilized for digital image authentication, it has a disadvantage in that not all of the replacement data can be recovered successfully in the presence of specific attacks, such as Gaussian noise.

By using a modified bit replacement algorithm in the spatial domain, Pal et al. (2012) suggested a biomedical picture watermarking approach that outperforms the basic LSB technique as is currently used. They started with the lowest order and worked their way up to the higher orders, inserting several copies of the same data into different areas of the cover image. Hence, even if some of the data is destroyed as a result of an attack, they may still gather the remaining data and, using the bit majority approach, recover the watermark from the cover image.

The "dual intermediate significant bit (DISB)" model, in which each pixel of the host image has two bits added to it and the remaining six bits are changed to change the original pixel, was studied by Mohammed *et al.* (2014). If the original and embedded images differ, the image to be used as watermark could be selected by picking the pixel value that is closest to the original. The model proposed here by Mohammed *et al.* (2014) was found to produce a superior quality watermarked image when related to LSB techniques. As a consequence, the DISB strategy provides strong attack resistance while simultaneously increasing the quality of watermarked images. It is, however, less resistant to geometric attacks such as scaling and rotation and has a one-pixel limit.

Abraham and Paul (2019) proposed an approach for spatial color image watermarking that does not impair image quality or modify perceived color. All image blocks have the watermark because it improves image quality and assault resistance, enabling verification and/or recovery. To ensure that the implanted bits are less disruptive when viewed by humans, they gave M1 the name of the embedding mask and M2 the name of the compensating mask. The modified pixels

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 100-112
https://doi.org/10.56471/slujst.v6i.366
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

are barely visible when compared to the surrounding pixels. According to experimental results, the proposed method retrieved the watermark data not minding if the least significant bits were already damaged or not, and the algorithm ensured that a very good peak signal-to-noise ratio (PSNR) value is achieved. The limitation of this algorithm is that the watermark extraction is difficult and this is because no detectable variance is observed between the "cover image" and the "watermark image".

Muyco and Hernandez (2019) employed LSB hash code to secure the source document, then extracted the hash code to generate a result that looked identical to the original in an inquiry. To authenticate digital Images, the LSB hash technique use a hashing strategy that conceals the hash function. The embedded watermark that was used to extract the data in this case is hidden. This algorithm is used for histogram analysis and the Harming distance; however, it has been discovered to be vulnerable to a number of attacks.

By establishing the PSNR and the Nigerian Communications Commission (NCC) threshold values, Zeki *et al.* (2019) demonstrated the potency and weaknesses that are experiential in digital image watermarking approaches. The disclosed watermarking approach implanted four (4) watermarks, one by one, into the ISB of six (6) gray scale files by replacing the original image pixels with new pixels and preserving their values equivalent to the values of the original pixel. Based on the PSNR and NCC values, their proposed approach was more resilient against typical image processing procedures including operations that filters, blurs, compresses or simply add noise to an image, but suffers limitation in terms of resilience against geometric assaults (e.g., scaling and rotation).

We are convinced to agree with Aaqib (2016) that spatial domain watermarking is easy and has a relatively high computing speed, but it is less resilient against attacks, as evidenced by evaluated research on spatial domain watermarking approaches.

4.2 Frequency/Transform Watermarking Techniques

In their work, Pun (2009) developed a technique based on a Gaussian low pass filter that was resistant to JPEG compression. In this method by Pun (2009), adaptive quantization was used to sample twelve DCT coefficients that inserts the watermark as it embeds 4096 bits of information in a 512 × 512-pixel picture. Pun's (2009) approach has a low imperceptibility and is less resistant to geometric assaults like scaling, rotation, filtering, and cropping.

Ramana *et al.* (2009) posited a frequency-domain watermark embedding and extraction approach that includes checks for salt and pepper and Gaussian noise assaults. The goal of this method is to authenticate the image content. A watermark was employed to the discrete wavelet transform of the novel image (DCT). Thus, the algorithm by Ramana *et al.* (2009) is represented by the function:

$$I_w(x, y) = I(x, y) + K_w(x, y) \quad (3)$$

The gain factor is k, and $I_w(x, y)$ is the watermarked picture. As k grows, the watermarked image's durability improves, but the final watermarked image's quality degrades, resulting in reduced imperceptibility.

Vaishnavia and Subashini (2014) proposed a durable and undetectable approach for inserting a watermark into an image in the "RGB" color space. This approach of watermarking simply implants the designated watermark into some unique parameters. Such implanted watermark may be regained by carefully identifying the blue channel of the cover image and applying SVD on it. When compared against current methodologies for digital image security, the novel approach stood out to be more resilient against median filtering, motion blur and to noises such as salt-and-pepper noise, Gaussian noise as well as JPEG compression attacks, but lacking in robustness against rotation, cropping, and scaling.

Chen *et al.* (2015) presented a digital image watermarking approach that exploits the wavelet-based threshold classification methodology. The image's complexity is evaluated by the algorithm in regards to resilience and imperceptibility. This methodology cautiously splits the host image into chunks, and each of the chunks is chosen for watermark insertion. The DWT coefficient is then categorized on the basis of lower frequency sub-bands using the optimal sub-bands. An all-embracing testing was done on the method, with the findings confirming the system's good resilience

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

and imperceptibility to numerous common assaults, but has a relatively weak resistance to geometric assaults like cropping.

Gaata (2016) offered research predicated somewhat on Fourier transform and visualized systems attributes in which the host image is divided into non-overlapping blocks and watermark bits are introduced into the chosen coefficients of each block based on predetermined criteria. This technique, which is more resilient for copyright protection and authenticity, can reduce various sorts of assaults such as "gamma noise, Gaussian noise, sharpness, blurring and filtering". It is not, however, robust to geometric operations.

Ambadekar *et al.* (2018) presented an approach for securing copyright information in the DWT domain by inserting a watermark and extracting it via watermark encryption. This method proved impervious to noise, geometric, and compression challenges. The two-dimensional DWT as well as the associated selection approaches are used to separately convert the colored cover image and the watermarked content from the "RGB" model into "YIQ" model. Ambadekar *et al.* (2018) designed this algorithm for copyright protection and content authentication. The method ensures that the system is immune to lossy compression assaults as well as to attacks due to Gaussian noise. However, the solutions are restricted since they lack resilience against cropping, scaling, and other changes.

Although frequency/transform approaches outperform spatial domain techniques in terms of resilience, they suffer from restricted payload capacity and weaker robustness against particular attacks.

4.3 Hybrid Domain Watermarking Techniques

Chouhan *et al.* (2011) used a combination of dynamic stochastic resonance and the singular value decomposition for the watermarking. When compared to other techniques, the approach is more resistant to a range of distortions, but it has a false positive problem. This is owing to the fact that only the singular values of the watermark are inserted in the host image, and the singular vectors of non-existent watermarks can be used to extract an estimate of watermark from the host image. This algorithm has a false positive problem and the main drawback of these techniques is that they are having limited robustness.

Kumar (2019) suggested a new strategy for protecting digital contents' right in a hybrid domain. By using the "least significant bits" and "wavelet transform" "DWT" and "SVD", Kumar (2019) safeguards digital information while it is being transmitted over an insecure channel. These algorithms cautiously separated the host image into sub-bands "LL", "HL", "HH", and "LH" using a frequency domain transformation process. The watermark is removed using embedding processes that have been previously described. The technique proposed by Kumar (2019) is aimed for copyright protection and digital content security. This hybrid method enhances the system's quality and endurance against a variety of assaults, such as Gaussian noise and JPEG compression, but it is less resistant to geometric attacks.

To enable higher resiliency, Assini *et al.* (2018) developed new approaches for protecting medical images by integrating "DWT", "DCT", and "SVD". In this scenario, the medical image has an invisible watermark image placed in it. The "third-level (3L)" DWT procedure is cautiously performed on the medical host image. In this situation, the DWT coefficients of the medical host image's high-frequency sub bands are employed. The "DCT" and "SVD" transforms are subsequently employed and formed into the host image. The Wiener, average, and median filters all enhance imperceptibility and resilience to "Gaussian, salt-and-pepper" noise introduction. The technique's drawback is that it does not have the capability of resisting assault such as "HE", "LPGF", "JPEG compression", JPEG2000, rotation, cropping, sharpening, blurring, resizing, "PN", "GWN", print//scan as well as combined assaults.

Takore *et al.* (2018) employ edge detection to determine the optimum location for embedding the watermark by combining the LWT, DCT, and SVD. The particle swarm optimization (PSO) technique was employed to manage the trade-off between robustness and imperceptibility. The results of the experiments reveal that the scheme is robust to a variety of assaults while maintaining the perceptual quality of the host image. Despite the strength and capability of the scheme by Takore *et al.* (2018), their method is found to be more vulnerable to JPEG2000, print//scan assaults, desynchronization attacks as well as combination attacks than other algorithms.

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Jain and Ghanekar (2018) present a frequency domain-based hybrid DCT-SVD approach for increasing watermark capacity in their article. In this effective watermarking approach, the Arnold transform is utilized to texturize the watermark logo. The watermark logo's SVD is applied after the host image is subjected to two-dimensional DCT. Different weights are selected based on lowered singular values in order to lessen the host image's distortion. "GN", "LPGF", "histogram equalization", "JPEG compression", JPEG2000, sharpening, blurring, resizing, "PN", "GWN", de-synchronization assaults as well as combined attacks, however suffers a relatively weak resilience by this technique.

To secure copyright information, Hamidi *et al.* (2018) integrated two dual-transform domain methodologies: "DFT" and "DCT". On achieve imperceptibility, DFT is first performed to the host image. To improve the system's resilience, the DCT is adapted to the magnitude of the DFT of the host image. The watermark is encrypted before being inserted in the middle-band DCT coefficients of the host image. The approach indicates that the host image as well as the watermarked image have no obvious differences in appearance. The system however is deficient in its capability to resist assault in the forms of rotation, sharpening, blurring, "AF", "MF", "wiener filter", print//scan, resizing, de-synchronization as well as combination assaults.

Liu *et al.* (2018) suggested a blind dual watermarking approach for digital color image authentication and copyright protection. Copyright protection is given by invisible resilient watermarks, while image authentication is provided by fragile watermarks in their proposed approach. "The first watermark is encoded for copyright protection, and owing to the discrete wavelet transform (DWT) in YCbCr color space, it may be retrieved blindly without access to the host image". Fragile watermarking, on the other hand, employs an upgraded "least significant bits (LSB)" replacement procedure in "RGB" components to authenticate the image. The validity and authenticity of a distrustful image could be evaluated blindly independent of the host image and the original watermark. The suggested technique is ideal for securing expensive original images owing to its mixture of robust and fragile watermarking. Findings from the approach by Liu *et al.* (2018) disclosed that the suggested watermarking system can survive different processing assaults and precisely detect the image's tampered area. However, because it is not robust against geometric and combined assaults, it is restricted in its capacity to retrieve the tampered region once a watermarked image has been tampered with.

In another work, Zhang *et al.* (2019) exposed the host image to varying amounts of DWT before subjecting it to DCT. This approach is intended to secure multimedia and safeguard intellectual property. The spread transform known as "QIM" is then used to implement the watermark insertion. The approach beats previous methods in terms of resilience and imperceptibility, although it still has a weak resistance to "HE, JPEG 2000, rotation, sharpening, blurring, AF, MF, Wiener filter, print/scan assault, resizing, PN, GWN, SN, desynchronization, and combined attacks".

A framework called "Robust color image watermarking for copyright protection" is provided in some other research by Abdulrahman and Ozturk (2019). The "DCT" and "DWT" are used in conjunction and applied to an "RGB" host image after it has been split into 3 constituent parts (red, blue, and green). Subsequently, by the use of Arnold transform, the grayscale watermark image is encoded. The DCT coefficient for each portion is determined once the encrypted watermark is split into equal proportions. DCT coefficients from the watermark component are subsequently incorporated in the color host image's DWT sub bands. The study demonstrates that scaling, noise addition, rotation, filtering, and JPEG compression do not affect the watermarked image. Furthermore, in terms of imperceptibility, the system beats previous approaches.

Savakar and Ghuli (2019) suggested an inner and outer watermarking strategy for copyright protection by merging blind and nonblind watermarking technologies. DWT has been used to insert a binary watermark image in the inner host image using the inner methodology. DWT and SVD are utilized in the embedding of inner watermarked image into the outer cover image. The watermark is extracted in a backwards fashion. In addition to combining spatial and transform domain approaches, recent improvements have included combining the spatial and transform domains with artificial intelligence procedures such as "machine learning" and "artificial neural network" techniques to improve performance. To find the optimal embedding function, these algorithms are utilized. "Gaussian noise, salt-and-pepper noise, Poisson noise, speckle noise, rotation, and JPEG compression" are all ineffective against the suggested system. Nevertheless. It is

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

vulnerable to "HE, LPGF, JPEG 2000, cropping, sharpening, blurring, AF, MF, resizing, GWN, Wiener filter, print/scan attack, desynchronization, and combined attacks".

Abdulrahman and Ozturk (2019) suggested using DCT and DWT to create a watermarking solution for solid color photos. The RGB cover image is split or broken down to red, green, and blue sections using this process. In some areas of each color, DCT and DWT are employed. Using Arnold transform, the gray watermark picture is rotated. The concealed watermark image is modified by the introduction of DCT. The modified watermark image is then separated into smaller, equal pieces. Four DWT bands in colored areas of the cover image include the DCT coefficients for each watermark segment. Different image processing procedures, for example, rotation, resizing, filtering, jpeg compression as well as sound added to tagged images, have been used to show the strength of the suggested color image's watermarking. The findings reveal that the suggested strategy is resilient against direct and indirect assaults and protects the visibility of tagged images, but it is not robust against print/scan and combination attacks. This approach however can be used to safeguard copy rights.

Alzahrani (2022) has developed a system for enhancing the Visibility and Strength of Digital Image Watermarking Based on DWT-SVD. The advanced system is to handle real types of water-marked attacks, gaining maximum protection and adequate level of visibility and durability. DWT and SVD methods have been used to analyze the true kinds of assaults. The "DWT" method was utilized in the insertion of the cover image on four (4) levels. Each of the four (4) levels was prepared utilizing the SVD technique. High "signal-to-noise ratio (PSNR)" and "similarity index (SSIM)" format was used as a parameter to measure visibility and "standard correlation (NC)" was used to assess the intensity of the marked image(s). The findings revealed that the suggested DWT-SVD performed well in recognizing various assaults but Its measure of robustness against geometric attacks is not determined**.**

Despite the fact that our literature shows that hybrid domain techniques outperform spatial and frequency domain techniques, existing hybrid methods still face the challenge of achieving content authentication and copyright protection at the same time due to a lack of robustness against attacks, particularly geometric and print/scan attacks, as well as combined attacks such as "Histogram equalization (HE)"+ "Gaussian noise (GN)", "HE" + "salt-and-pepper noise (SPN)", and others (Mahbuba and Mohammad, 2020).

5. Conclusion

Watermarking digital images using different ways has become a common approach for "identification, integrity verification, tamper detection, copyright protection, and digital security of images". This paper therefore took a critical look at some of the most common state-of-the-art watermarking styles and observed that certain watermarking technologies are easy to execute while others are difficult. Some algorithms have a little effect on image quality, while others have a large one. Some are extremely resistant to typical image processing techniques, but not geometric assaults. The few strategies that are somewhat gallant to withstand geometric attacks are on the other hand, tremendously vulnerable to other sorts of noise. It is also obvious that certain criteria must be satisfied in order to create good digital watermarking designs. Imperceptibility, robustness, capacity, and security are among the four essential needs. Although meeting imperceptibility, robustness, and capacity needs all at the same time is almost difficult, a decent trade-off between the three is expected. Further research should be focused on developing new strategies that can survive many forms of attacks in order to accomplish robustness and security, which includes digital image authenticity and copyright protection. Hybrid watermarking technologies, according to our findings, are more resilient and give improved imperceptibility while maintaining excellent security. The existing approaches do, however, have certain drawbacks: they aren't extremely resistant to all geometric and print/scan assaults, and they can't stand up to combination attacks hence militating against digital image authentication and copyright protection. This study therefore suggest that further works should strive to bridge these gaps and ensure a system that will be resilient to geometric and print/scan attacks as well as to combination attacks.

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

References

Singh, P. and Chadha, R.S. (2013). A survey of digital watermarking techniques, applications and attacks. *Int. J. Eng. Innov. Technol*. 2:165–175.

Aaqib, R. (2016). Digital watermarking applications and techniques: A brief review. *International Journal of Computer Applications Technology and Research*, 5(3): 147-150

Abdulrahman, A. K. and Ozturk, S. (2019). A novel hybrid DCT and DWT based robust watermarking algorithm for color images. *Multimedia Tools and Applications*, 78:17027–17049.

Abraham, J. and Paul, V. (2019). An imperceptible spatial domain color image watermarking scheme. *Journal of King Saud University*, 31:125–133.

Alzahrani A. (2022). Enhanced invisibility and robustness of digital image watermarking based on DWT-SVD. *Applied Bionics and Biomechanics*, 2022: 1-13 doi.org/10.1155/2022/5271600

Ambadekar, S.P., Jain, J. and Khanapuri, J. (2018). Digital image watermarking through encryption and dwt for copyright protection. *Journal of Recent Trends in Signal and Image Processing*, 727:187–195.

Assini, I., Badri, A. Badri, A., Safi, K., Sahel, A. and Baghdad, A. (2018). A robust hybrid watermarking technique for securing medical image. *International Journal of Intelligent Engineering and Systems*, 11(3):169–176.

Barni, M. and Bartolini, F. (2004). Watermarking systems engineering: Enabling digital assets security and other application. New York: CRC Press. 500p.

Chen, B. and Wornell, G. W. (2001). Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Trans. Inf. Theory*, 47(4):1423-1443

Chen, Z., Chen, Y., Hu, W. and Qian, D. (2015). Wavelet domain digital watermarking algorithm based on threshold classification. *International Conference on Swarm Intelligence*, 9142:129–136.

Cox, I. J. and Miller, M. L. (2002). The first 50 years of electronic watermarking. *EURASIP Journal on Applied Signal Processing*, (2): 126 - 132

Cox, J, Miller, M. L. and Bloom, J.A. (2002). Digital watermarking and fundamentals. San Francisco: Morgan Kaufmann.

Desai, H. V. (2012). Steganography, cryptography, watermarking: A comparative study. *Journal of Global Research in Computer Science*,3(12):33-35

Discrete Wavelet Transform. Available online: https://en.wikipedia.org/wiki/Discrete_wavelet_transform (accessed on 23 October 2019).

Gaata, M.T. (2016). An efficient image watermarking approach based on fouriertransform. *International Journal of Computer Application*. 136: 8–11.

Hajjaji, M.A., Mtibaa, A. and Bourennane, E. (2011). A watermarking of medical image: Method based "LSB". *Journal of Emerging Trends in Computing and Information Sciences*, 2(12):714-721.

Hamidi, M., Haziti, M. E., Cherifi, H. and Hassouni, M. E. (2018). Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform. *Multimedia Tools and Applications*, 77(20):27181–27214.

Jain, P. and Ghanekar, U. (2018). Robust watermarking technique for textured images. in Proceedings of the 6th International Conference on Smart Computing and Communications (ICSCC), pp. 179–186, Kurukshetra, India.

Jane, O. and Elbasi, E. (2014). A new approach in non-blind watermarking method based on DWT and SVD via LU decomposition. *Turk. J. Electr. Eng. Comput. Sci*. 22:1354–1366.

Kaur, E.J.; Kaur, E.K. (2012). Digital watermark: A study. *Int. J. Adv. Res. Comput. Sci. Softw. Eng*. 2:159–163

Kumar, A. (2019). A Review on implementation of digital image watermarking using LSB and DWT. *Inf. Commun. Technol. Sustain. Dev*. 933:595–602.

Lin, C., Wu, M., Bloom, J.A., Cox, I.J., Miller, M.L. and Lui, Y.M. (2001). Rotation, scale, and translation resilient watermarking for images. *IEEE Trans. Image Process.* 10:767–782.

Liu, X.L., Lin, C.C., & Yuan, S.M. (2018). Blind dual watermarking for color images' authentication and copyright protection. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(5), 1047–1055. doi:10.1109/tcsvt.2016.2633878

Mahbuba and Mohammad (2020). Digital image watermarking techniques: A review. *information*, 11(110):1-42

Mohammed, G.N., Yasin, A. and Zeki, A.M. (2014). Robust image watermarking based on dual intermediate significant bit (DISB). *In Proceedings of the 6th International Conference on CSIT, Amman, Jordan*, pp. 19–22

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Muyco, S.D and Hernandez, A.A. (2019). Least significant bit hash algorithm for digital image watermarking authentication. *In Proceedings of the 5th International Conference on Computing and Artificial Intelligence*, *Bali, Indonesia*, pp.150–154.

Najafi, E. A. (2017). Robust Embedding and Blind Extraction of Image Watermarking Based on Discrete Wavelet Transform. *J. Math. Sci*. 1:307–318.

Obimbo, C. and Salami, B. (2012). Using Digital Watermarking for Copyright Protection, Watermarking – in Gupta, M.D.(Ed.), InTech, Available from: http://www.intechopen.com/books/watermarking-volume-2/using-digital-watermarking-for-copyright-protection. 2:137-158.

Pal, K, Ghosh, G. and Bhattacharya, M. (2012). A comparative study between LSB and modified bit replacement (MBR) watermarking technique in spatial domain for biomedical image security. *International Journal of Computer Applications and Technology*, 1(1):30-39.

Piva, A., Barni, M. Bartolini, F. and Cappellini, V. (1997). DCT-based watermark recovering without resorting to the uncorrupted original image, *Proceedings of International Conference on Image Processing*, vol.1 pp. 520-523.

Pun, C.M. (2009). High capacity and robust digital image watermarking. *In Proceedings of the 5th International Joint Conference on INC, IMS and IDC, Seoul, South Korea* 25–27. pp. 1457–1461.

Ramana, P.R., Munaga, V.N., Prasad, K, and Sreenivasa, R (2009). Robust Digital Watermarking of Color Images under Noise attacks. *International Journal of Recent Trends in Engineering*, 1(1):334-338.

Rathor, B. and Saharan, R. (2017). Steganography using bit plane embedding and cryptography. *In Proceedings of the 1st International Conference on Smart System, Innovations and Computing*, Jaipur, India, Vol. 79, pp. 319–330.

Savakar, D. G. and Ghuli, A. (2019). Robust invisible digital image watermarking using hybrid scheme. *Arabian Journal for Science and Engineering*, 44(4):3995–4008.

Shih, F.Y. and Wu, S.Y. (2003). Combinational image watermarking in the spatial and frequency domains. *J. Pattern Recognit. Soc*. 36:969–975.

Sridhar, P. A. (2018). Robust digital image watermarking in hybrid frequency domain. *Int. J. Eng. Technol.* 7:243–248.

Takore, T. T. Kumar, P. R. and Devi G L. (2018). A new robust and imperceptible image watermarking scheme based on hybrid transform and PSO. *International Journal of Intelligent Systems and Applications*, 10(11):50–63.

Tao, H., Chongmin, L., Zain, J.M. and Abdalla, A.N. (2014). Robust image watermarking theories and techniques: A review. *J. Appl. Res. Technol.* 12:122–138.

Tirkel, A.Z., Rankin, G.A., Van Schyndel, R.M., Ho, W.J., Mee, N.R.A., Osborne, C.F. (1993). Electronic Water Mark. *DICTA 93, Macquarie University*, pp. 666–673.

UKEssays. (November 2018). The History of The Digital Watermarking Techniques. Retrieved from https://www.ukessays.com/essays/information-technology/the-history-of-the-digital-watermarking-techniques-information-technology-essay.php?vref=1

Usman, I. (2010). Digital Watermarking Using Machine Learning Approaches. A dissertation submitted for the degree of Doctor of Philosophy in Computer and Information Sciences to The Department of Computer and Information Sciences, Pakistan Institute of Engineering and Applied Sciences, Islamabad, Pakistan.

Vaishnavia, D. and Subashini, T.S. (2014). Robust and invisible image watermarking in RGB color space using SVD. *In Proceedings of the Communication Technologies, Kochi India*, pp. 1770–1777.

WOO, C. (2007). Digital image watermarking methods for copyright protection and authentication. A Thesis submitted in accordance with the regulations for Degree of Doctor of Philosophy, Information Security Institute Faculty of Information Technology Queensland University of Technology, 197p

Wu, X., Hu, J., Gu, Z. and Huang, J. A. (2020). Secure Semi-fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters. Available online: https://dl.acm.org/doi/10.5555/1082290.1082302 (accessed on 8 February 2022).

Yeo, In and Kim, H.J. (2003). Generalized patchwork algorithm for image watermarking. *Multimedia Systems*, 9:261–265.

Zeki, A., Abubakar, A. and Chiroma, H. (2020). An intermediate significant bit (ISB) watermarking technique using neural networks. Available online: https://link.springer.com/article/10.1186/s40064-016-2371-6#citeas (accessed on 16 February 2022).

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Zhang, Y., Li, Y. and Sun, Y. (2019). Digital watermarking based on Joint DWT–DCT and OMP reconstruction. *Circuits, Systems and Signal Processing*, 38:5135-5148.