A Synthesis of State of the Art contributions in Digital Image Watermarking

Kamred Udham Singh, Achintya Singhal

ABSTRACT---The decision to include certain information into the concept of digital media has continually received attention, especially among participants in the research community. The aim of this paper is to examine some of the contributions that are deemed to be the state of the art. The paper gains insights from the perspective of the digital image watermarking process. In both spatial and transform domains, the watermarking concept has been proposed. The concept incorporates issues from different perspectives – in relation to image watermarking approaches. This study's chosen research article are from the web of science database, as well as those that the selected papers have cited highly.

Index Terms: Watermarking, Image, Transform domain, spatial domain.

I. INTRODUCTION

Communication ensures that feelings and ideas are expressed by the concerned parties. Also, information is given. The process has existed since the origin of man. Given different aspects of advancement, the need for secret communication has grown. The process of secret communication has also existed since the period of pigeon communication to the current digital era. Initially, one of the approaches used for secret communication entailed steganography, which reflected a state of covered writing. For thousands of years, this technique has been embraced. An example is a case in which the 5th century witnessed Herodotus, a Greek, provide writings concerning Histaeus. The aim was to deliver a message to a son-in-law in Greece. At first, information was tattooed on the scalp of a slave. Later, the slave's hair grew and would later be dispatched to deliver the hidden content on his scalp [1, 2]. Additional tricks were also used to communicate the intended ideas. Examples included the use of pencil marks, invisible inks, and the use of tiny pin structures on certain characters.

Notably, steganography refers to a technique through which digital data is hidden in different digital cover objects. Examples include video, audio, text, and image presentations; implying that only recipients tend to understand the intended messages [3]. The motivation is to ensure that messages that are covered are transmitted secretly via innocuous files. This concept has continually gained popularity and attention, coming in the wake of pressure towards data security. Also, the concept's central aim is to ensure that there is secure and complete communication between the sender and the receiver (without trace). Also, it strives to avoid suspicion in relation to the messages that are relayed [4]. According to Anderson and Petitcolas (1998) [5], steganography has had different forms of watermarking implemented to ensure that copyright data is hidden accordingly. In digital objects, serial numbers have also been used [4].

Imperative to note is that the process of image watermarking is not new. In the 14th century, aspects of cryptography and steganography played significant roles towards achieving image security [3]. However, there was significant development of steganography in the 15th and 16th centuries but era that followed witnessed deviations in which microdots and invisible inks were established. In the observation by Zhao (1997) [6], the watermarking technique strive to assure information security in different platforms; including audio and visual platforms.

Given the emergence of the Internet and other technological advancements, the current world has witnessed significant growth in digital media; especially in the past few years. Some of the developments accounting for these trends include online services and electronic commerce, which have had rapid expansion. With information and communication technology also improving, there has been faster and easier digital multimedia distribution. Also, digital data legalization implies that the need to secure the information could not be overstated. Some of the risks facing the data include malicious manipulation, counterfeiting, and piracy. The role of invisible watermarking is to ensure that the data is embedded in host images through unnoticeable modification. On the other hand, visible watermarking involves semi-transparent text overlaid or logos that are attacked to the host images. The intention of the watermarking procedure is to protect digital information. Hence, the concept has received growing attention due to the effectiveness with which it I associated – in relation to digital contents' copyright protection [5].

From the observation above, watermarking can be indivisible or visible. Imperceptible to human visual systems, the watermarks can only be detected via computer systems. Some of the information that they host includes the image, the logo, and the owner of the selected image. The aim is to prove the authentication copyright, upon which infringement is minimized. In digital images, different levels of energy are used to embed digital watermarks. Features to consider include the ability to avoid compromising image quality and the aspect of robustness in which it is expected that the embedded watermarks could not be removed by attackers easily [7].

Revised Manuscript Received on May15, 2019.

KamredUdham Singh, DST-CIMS, Institute of Science, Banaras Hindu University, Varanasi, 221005, India. (kamredudhamsingh@gmail.com)

AchintyaSinghal, Department of Computer Science, Institute of Science, Banaras Hindu University, Varanasi, 221005, India. (achintya.singhal@gmail.com)

II. MAJOR CHARACTERISTIC OF WATERMARKING TECHNIQUES

Watermarking techniques embed the watermark inside host image. Given the different demerits and merits with which the approach is associated, different applications account for varying degrees of importance of the digital watermarks. There are various important characteristics of watermarking [8], which are depicted in Fig. 1 and discussed below:

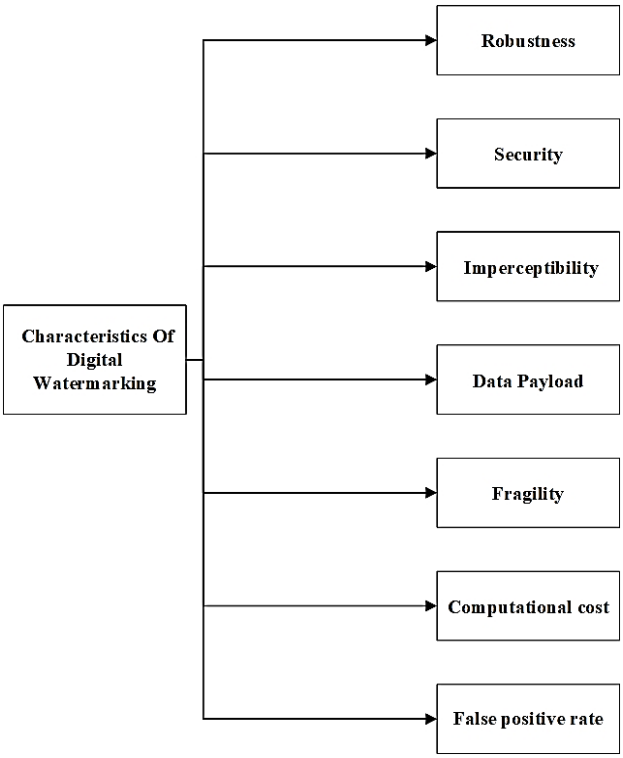

Fig. 1: Major characteristics of the watermarking Scheme

A. Robustness

This feature forms the chief motivation behind the watermarking procedure. The aspect constitutes the extent to which the determination of an image's presence of hidden data is difficult. In the field of copyright protection, watermarking becomes important whereby it bars malicious groups from filtering or destroying the watermarks that have been embedded on or in certain images. In relation to this concept of robustness, the two main issues that are worth considering include watermark detection and the possible presence or absence of a watermark – after an image is destroyed.

Based on the observations above, it becomes imperative to ensure that watermarking techniques are incorporated in such a way that they prove robust and guard against possible distortion or interference [9]. Determining the degree of robustness has witnessed growing use of Normalized Correlation (NC), a watermarking scheme that operates between the extracted watermark (W+) and the original watermark (W) the scheme holds that:

$$NC = \frac{\sum_{c=1}^{3}\sum_{x=1}^{p}\sum_{y=1}^{q}\left(W(x,y,c)\times W^{+}(x,y,c)\right)}{\sqrt{\sum_{c=1}^{3}\sum_{x=1}^{p}\sum_{y=1}^{q}(W(x,y,c)^{2})}\sqrt{\sum_{c=1}^{3}\sum_{x=1}^{p}\sum_{y=1}^{q}(W^{+}(x,y,c)^{2})}}$$

B. Security

In the practice of watermarking, attacks can be passive or active. If, utmost, random guessing is used to estimate the presence of a watermark, watermarking security becomes important due to the need to ensure that the selected or embedded watermark is guarded against distortion, which could extend to the hot image.

C. Data Payload

This concept refers to the quantity of data housed by a given watermark. Indeed, an appropriate watermark is that which entails all the expected content in arbitrary and small portions.

D. Imperceptibility

The need for noise distortion in watermark embedding is also worth considering. Particularly, it is important to ensure that the hot image's perceptual quality is considered. The eventuality is that the original and the watermarked image ought to exhibit differences beyond an acceptable threshold; implying that the process needs to be so superior that the visual comparisons are unlikely to differentiate between the original and the watermarked image. In so doing, the hot image's integrity tends to be protected. Notably, watermark embedding is an important procedure whereby it promotes original data's conservation by guarding images against possible and malicious attacks. Hence, perceptual transparency entails the similarity between the original and the watermarked image. To determine the imperceptibility of certain images, the peak signal to noise ratio (PSNR) has gained increasing application. It i defined as:

$$PSNR = 10 * \log_{10}\frac{(Max)^2}{\frac{1}{m*n}\sum_{i=0}^{m}\sum_{j=0}^{n}\left(A_{ij}-B_{ij}\right)^2}$$

where

A_{ij}: Refers to the host image
B_{ij}: Refers to the watermarked-image
$m * n$: represent image dimensions .

Max: represent the maximum value of the colors which is 255

MSE refers to the Mean-Squared Error when the watermarked and the hot images are compared. It is expressed as:

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m}\sum_{j=0}^{n}\left(A_{ij}-B_{ij}\right)^2$$

where

A_{ij}: host image
B_{ij}: watermarked-image
$m * n$: represents dimension of the image.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

E. Fragility

The main motive of fragile watermarking is to cement content authentication, which is contradictory of robustness. It facilitates the endurance of various degrees of modification with great deal of flexibility on occurrence of distortions in the host image. On contrary to digital signature, which requires a perfect match, watermark provides reasonable relaxation.

F. Computational Cost

It is an important attribute, which refers to the overall cost of insertion and extraction of watermarking technique. Depending on various applications, it is of utter importance that the organization should motivate the embedding scheme to be fast along with preserving its simplicity, although it is not rare to observe that the extraction process may have more time complexity. However, the time complexity of extraction in some applications is very crucial, which shows that insertion and extraction time complexity of the watermark depends on the scheme applied.

G. The case of the false positive rate

It is the measure of the rate when there is no watermark embedding and still the embedded watermarks are identified by the system. Hence, it is very important to keep this rate to an optimum low level for ensuring the consistency of the watermarking technique.

III. DIGITAL WATERMARK APPLICATIONS

Image watermarking scheme is mainly application dependent i.e. its algorithm and constraints may vary in different scenarios. Image watermarking has proved its dominance over a vast class of real life applications and some of them discussed below:

A. Copyright Protection

In any given image, a watermark, which entails secret copyright data, can be embedded. The aim is to establish intellectual property [10, 11]. To achieve this process, the message is transformed into a complex structure to bar intruders from manipulating the information maliciously; especially because the intruder is unlikely to detect the copyright information. Also, the role of a watermark lies in the detection of possible modifications to a given image [12]. To achieve the watermarking process, some of the approaches that are employed include measuring certain quality features, conducting a similarity check, and through statistical correlation. Hence, growing interest in the subject of digital watermarking has evolved from the perceived role of the watermarks in ensuring that the copyrighted information or material i well protected against malicious attacks, theft, or manipulation.

B. Broadcast Monitoring

In broadcast monitoring, watermarking plays a major role in verification of the utilized airtime purchased from broadcasters to organizations [13]. For this purpose, storing identification codes of a broadcast is necessity of the system. Therefore, digital image watermarking technique is the most suitable for information monitoring in a broadcast system. The broadcast system that has the information contains a relevant watermark for its monitoring. However, it is not an easy task to embed and extract watermark using this watermarking scheme with reference to broadcast monitoring. Now days, research organizations are showing their great interest in refining and optimizing the watermarking scheme to overcome the above mentioned obstacle in broadcast monitoring.

C. Fingerprinting

In digital fingerprinting, the practice involves tracking the origin of certain copies that are deemed illegitimate. To ensure that materials or the data is authentic to the target audience, the copies have unique watermarks embedded on them. Therefore, fingerprinting complements the embedded serial numbers, which aid in customer identity. Hence, fingerprinting is beneficial to intellectual property owners in such a way that individuals who might attempt to manipulate the material are identified easily, having violated licences or agreement. In particular, the data is supplied to unauthorized parties for unauthorized access, making the fingerprinting procedure necessary.

D. Copy Protection

Copy protections of digital devices are controlled by the information encrypted in the watermark [14]. The copy prohibit bit in a watermark and the watermark detectors collectively ensures the authorized storing of the data. So the watermarking technique plays a great role in validation and justification of the data at the same time preserving its integrity.

E. Medical Safety

In modern era, medical safety is one of the most important issue as well as application of evolving watermarking techniques. The advance medical images contain patient's data along with the respective image, which hence arises the main problem of its safety. Watermarking techniques play a valiant role in avoiding patient's medical data from being compromised. It also helps medical practitioners to a great deal in performing scrumptious diagnosis of the medical images. There are watermarking schemes, which are very beneficial during the transmission of the medical images as they prevent from adulteration and privacy issues.

IV. GENERAL PROCEDURE OF IMAGE WATERMARKING

A watermarking scheme has three major steps:

- The generation of the watermark
- The embedding of the watermark
- The detection or extraction of the watermark

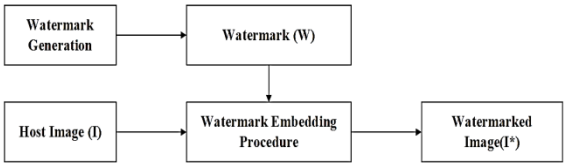

Fig. 2: Watermark Embedding Process

In Fig. 2, the basic process of watermarking is illustrated. The initial phase involves the input of the watermark and the host image. This process is followed by embedding, which involves the insertion of watermarks relative to the applied algorithm, eventually yielding watermarked images.

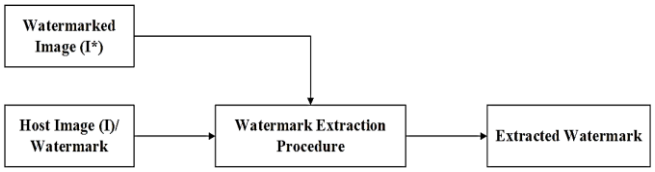

Fig. 3: Watermark Extraction Process

The process of extracting a watermark is commenced by comparative analysis of generated watermark image, original host image and inserted watermark. After the computational procedure, the watermark is extracted and further its qualitative analysis is performed.

V. TYPES OF DIGITAL WATERMARKING SCHEMES

Figure 4 illustrates the main techniques through which watermarking are achieved. The broad classification is done on the following basis viz. domain, digital documentation, human perception and application. The above mentioned bases are the major classes in which almost all the watermarking techniques are categorized. The techniques based on domain are further bifurcated in spatial and frequency domains. These two domains are connected through valid transformation criteria i.e. both of them can be obtained from each other using permissible transformation relations. Image, audio, video and text, which are the digital documents is another aspect of categorization of the watermarking scheme i.e. watermarking schemes may vary in their procedure for these digital documents. Both the non-blind and blind schemes aid in extracting the intended material. The schemes range from supervised and unsupervised to analogous procedures. Regarding the case of the non-blind scheme, the original image acts as reference to ensure that the watermarked image is compared. However, the blind scheme does not provide room for the comparative analysis exercised during the implementation of the non-blind scheme. Another notable aspect is that human perception plays an important role in such a way that the resultant observatory purpose seeks to add to the quality and quantity aspects of watermarking. In the category of human perception, watermarking can be invisible or visible. Given a host image, the visible aspect entails the overlaid secondary translucent watermark. Through careful and layman inspection, this watermark can be detected. For the case of the invisible watermark, perceptual observation is difficult – after the embedding procedure. Hence, the approach attracts the use of relevant algorithm through which information can be decoded. From the previous scholarly observations, invisible watermarks are classified further into robust and fragile watermarks. In the robust watermark, specific sub-categories include non-quasi invertible, quasi-invertible, public, private, non-invertible, and invertible invisible robust watermarks.

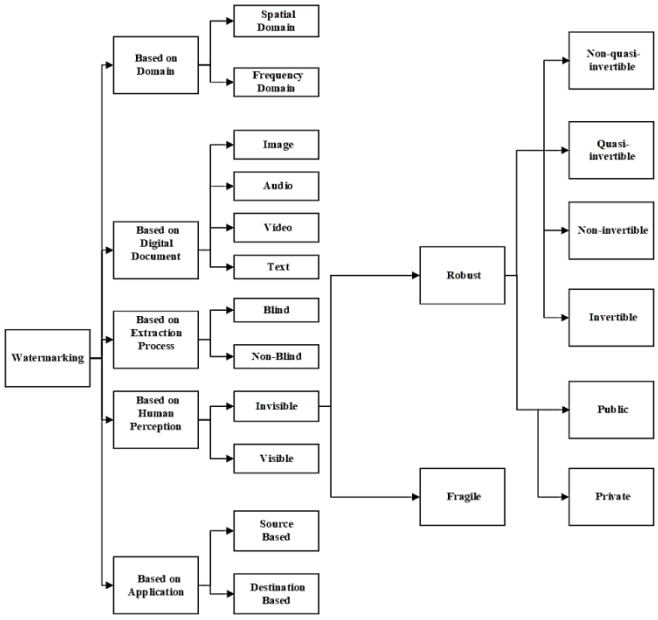

Fig. 4: Major Types of watermarking techniques [15]

VI. IMAGE WATERMARKING IN TRANSFORM DOMAIN

In transform domains, watermarking is associated with better performance – compared to situations involving the use of spatial domain approaches. Given the recent rapid advancement in information technology, the need to enhance digital content security could not be overemphasized. With the evolution of the LSB data embedding approach, the field of information security has witnessed a promising approach, especially due to the technique's ability to curb possible attacks. Indeed, the complexity of the algorithm reduces to a greater extent in transform domain than the spatial domain. The wavelet domain is advantageous over the other transform domains viz. Fourier, Laplace etc. as the computation is performed over a localized domain which hence reduces the computational complexity and loss of relevant information while reconstruction. It also proves its dominance over the other transform domains as it has a severe advantage of compact support system. The discretized version of the wavelet transform, if facilitated by multi-resolution analysis (MRA), provides a greater deal of flexibility over a range of resolutions thus enhancing the probability of perfect reconstruction. In transform-domain watermarking processes, three steps have been documented. The initial phase targets the host image before allowing for the embedding of watermarks in part of or all the coefficients that are transformed. The process culminates into the inverse transformation of the modified coefficients to regarding the image's original form. In the current literature, different watermarking techniques, which gain application to image watermarking, have been documented; with the transformed domain on focus.

In the study by Cox et al. (1997) [16], non-blind digital image watermarking was proposed. The discrete wavelet transform was emphasized, with the study indicating that

this technique operates in such a way that in a spread-spectrum, a Gaussian random vector is inserted. Indeed, it was established that the spread-spectrum plays an important role in any given data, and that the resultant scheme exhibits robustness relative to dithering distortion, geometric transformation, and cropping.

In another study, Barni et al. (1998a) [17] focused on a watermarking algorithm through which DCT coefficients' frequency embedding is achieved. In the proposed system, certain real numbers, having been generated randomly and in a sequence, were embedded in the selected DCT coefficients – before being inserted in gray scale watermarks within the host images. The process translated into a non-blind technique. In another study, Mauro Barni et. al. (1998b) [18] focused on a watermarking algorithm based on a pseudo-random sequence, with DCT coefficients fed with real numbers.

A study by Voyatzis and Pitas (1998) [19] targeted host images in relation to the use of a multiple watermark insertion scheme. The study indicated that the images have digital colors or be in gray scale. The algorithm relied on a mixing or chaotic system in which an 8-bit binary image processing aided in image watermarking, as well as the extraction of watermarks.

Also, Ruanaidh and Pun (1998) [20] proposed the use of a Fourier-Mellin-based algorithm in watermarking. This algorithm was observed to be better placed to minimize scale and rotation transformations. Through the introduction of the CDM spread spectrum, the study indicated that this approach requires users to provide secret keys before decoding the given material. In a related study, Delaigleet.al (1998) [21] emphasized the use of gray scale images that depend on the human visual model, with maximal length sequences aiding in the encoding of watermark bits. Additional insights form the study by Podilchuk and Zeng (1998) [22] demonstrated that when the multi-resolution wavelet framework and the block-based discrete cosine transform are used, the resultant visual model achieves desirable levels of robustness, proving better placed to curb rescaling, JPEG compression, and cropping attacks.

Another investigation by Hsu and Wu (1998) [23] emphasize the use of the multi-resolution signal composition technique as that which operates in such a way that multi-resolution representations characterize both the host image and the watermark; bearing varying structures. Hence, DWT aids in transforming the image to ensure that a multi-resolution representation is achieved before embedding watermarks of varying resolutions; having targeted and sought to align with the decomposed image's resolution. In the study by Wei et. al. (1998) [24], a proposed watermarking model constituted the Just-Noticeable Difference. Given a wavelet domain, the proposed system would operate in such a way that the human visual system determines the degree of image vulnerability, having embedded and watermarked the same. Wang et al. (1998) [25] conducted a related study in which the blind and adaptive watermarking criterion was proposed. This criterion relies on DWT's perceptually significant wavelet coefficients. From the study, it was noted that the approach operates via the initial determination of important wavelet sub-brands before establishing other significant wavelet coefficients, eventually ensuring that watermark sequences are embedded into the target coefficients.

Insights form Xia et al. (1998) [26] demonstrate further that pseudo-random codes and DWT could be used to achieve a hierarchical multi-resolution watermarking practice. In this approach, the study advocated for the embedding of the codes into selected coefficients, targeting medium and high frequency bands. Indeed, the study compared the results with those obtained via the DCT technique and concluded that the DWT approach yields a robust watermarking approach or outcome. In Borş and Pitas (1998) [27], DCT was proposed and was documented o operate via the initial choice or selection of pixels using the Gaussian network classifier – before embedding DCT coefficient constraints into the target blocks. Two approaches that were recommended included: the use of linear constraints in DCT coefficients and the definition of DCT coefficient space' circular zones. In another investigation, Hsu and Wu (1999) [28] emphasized the use of a non-blind watermarking algorithm, the DCT-based approach. Indeed, different binary watermarks, which exhibited visually identifiable patterns, were embedded into gray scale images, having modified the host image's middle-frequency zones selectively. In Kim et al. (1999) [29], a DWT-based multi-resolution watermarking scheme was embraced, with the host image embedded via a human visual system targeting different watermark. This study was similar to that which was conducted by Zhu et al. (1999) [30]. In the latter study, video and image-based digital watermarking was proposed relative to 3D and 2D discrete wavelet transform. Through the wavelet transform's hierarchical nature, the study stated that it provides room for digital watermark multi-resolution detection. Hence, it was observed to be better placed to be embedded into high-pass wavelet coefficients within the wavelet domain.

In a study by Suthaharan et al. (2000) [31], statistical properties, HVS and DCT properties were considered before proposing a model through which the effect of the watermark would be spread on an image in the entirety. The scheme was observed to operate in such a way that the lower low-frequency AC components would have the watermark embedded on them; with the hot image forming the platform for the watermarking procedure. To ensure that the imperceptibility requirement was reduced, the author employed the bounded normal distribution. The proposed scheme yielded superior outcomes compared to that in which the spread spectrum scheme had been employed (Podilchuk & Zeng [22] and P&Z's [16]). The performance and inferences were observed and made (respectively) based on factors such as maximal capacity requirement, imperceptibility, transparency, and robustness.

In Wu and Hsieh (2000) [32], a blind watermarking scheme was proposed. DCT and the Reed Solomon Codewords coding methods guided the investigation. Given the host image, the DCT-based transformed block's RS code was used for watermarking and embedding processes. A similar investigation was conducted by Niu et al. (2000)

[33], who advocated for the use of DCT and the stack filter threshold decomposition for watermarking. On the host image, various watermarks were embedded based on the use of gray-level digital watermarks. Indeed, the proposed scheme entailed a non-blind watermarking approach. Form the results, the proposed approach was deemed robust and better placed to prevent compressing and cropping attacks, as well as other ordinary image-processing attacks.

A non-blind watermarking technique was proposed in the study by Falkowski and Lim (2000) [34]. In this study, the Complex Hadamard Transform (CHT) and the multi-resolution transformed were applied to gray-scale images. During the initial phase, the researchers relied on the Multi-resolution integer-valued Hadamard transform for the decomposition of the host image. This decomposition sought to transform it into a pyramid structure exhibiting bands such as LH, HL, HH, and LL. Notably, the least frequency band aide din the insertion of watermarks to ensure that the LL band was segmented into the 8x8 blocks; with the 2D CHT applied eventually. Findings demonstrated that the proposed scheme was robust and capable of minimizing dithering, compression and cropping attacks or distortions. In the investigation by Pereira and Pun (2000) [35], the proposed watermarking approach was that which relied on template matching and Fourier transform, targeting color images. The proposed scheme operated in such a way that the template and the watermark were embedded into DFT domains with mid-frequency ranges. The process of extracting the watermark was divided into two main stages. The initial stage constituted the extraction of the template while the second stage involves extracting the watermark. The template was extracted firstly because it contained data regarding the process of embedding the watermark. In the findings, the study demonstrated that the proposed scheme was robust whereby it minimized general linear transformations, as well as aspect ratio changes, compression, scaling, rotation, and other attacks targeting image processing.

In the investigation by Huang et al. (2000) [36], a watermarking technique that relied on DCT component magnitude's quantitative analysis was proposed. The target platform involved the host images. With the DC component on target, the watermark was embedded, with this context observed to exhibit superior perceptual capacity than the case of the host image's AC component. Indeed, it was concluded that the proposed scheme was robust against attacks that target image processing. A similar study was conducted by Lu et al. (2000a) [37]. In the latter study, a non-blind watermarking criterion was employed. This scheme was deemed "Cocktail watermarking." The scheme relied on the visual model-based technique, as well as the spread spectrum watermarking approach; with gray scale images on focus. The objective was to analyze the modulation techniques' efficiency and also ensure that the deficiency problem was addressed. Also, the approach introduced a modulation strategy constituting negative and positive modulation. In this case, positive modulation constituted the transformed coefficients' increase in magnitude while negative modulation constituted their decrease in magnitude. With the negative and positive modulations embedded into the host image's complementary watermarks simultaneously, it was concluded that given a host image, watermark extraction could be achieved via the proposed scheme.

In Lin et al. (2011) [38], the target component entailed a non-blind watermarking algorithm. The study relied on the discrete Fourier transform to apply on the host image, especially with the motivation of ensuring that the 1-D signal on the host image was not only converted but also had a watermark embedded. Also, the study strived to determine the level of the proposed scheme's robustness against translation, scaling, and geometric rotation – compared to situations in which other algorithms might have been applied. Results demonstrated that watermarking poses superior results in relation to the resistance to image processing attacks – such as JPEG compression and cropping. A similar investigation was conducted by Wang et al. (2002a) [39]. In the latter study, the proposed scheme constituted a Filter-bank technique in which wavelet filter-banking was implemented. The target platform entailed the host image. The scrambled watermark would later be embedded onto the hot image's medium-frequency band. In another scholarly investigation, Barni et al. (2002) [40] targeting a watermarking scheme in which DCT was applied to the hot image before inserting a watermark. The process involved the modification of a full-frame DCT coefficient subset in the respective color channels.

Additional insights were gained from the study by Chen and Lin (2003) [41, who emphasized the use of mean quantization and DWT. Initially, the DWT was applied to the host image before comparing the outcomes to those that had been reported after applying JND values in various HL and LL coefficients. In turn, the coefficients were modified relative to the bits of the watermark.

In an additional investigation, Hsieh et al. (2005) [42] relied on the DWT transform and secret sharing, with the target platform being a color image. The technique that was embraced involved two phases. The initial stage constituted the sharing of the image generation process while the second stage constituted the retrieval of the image. During the process of image generation, the host image was transformed to yield the YCbCr color space. In turn, an image was generated by employing a special sampling technique. After feature extraction from the selected image's sampling plane (by using DWT), the resultant scheme yielded a principal share image through watermarking. From the results, the proposed scheme was avowed to yield superior results whereby it was found to be better placed to minimize image processing attacks such as those involving JPEG compression, sharpening, cropping, and scaling.

Other insights were gained from the investigation by Jane et al. (2013) [43]. In this study, the proposed scheme entailed a hybrid image-watermarking procedure; targeting LU, Arnold's Cat Map, SVD, and DWT decomposition. Initially, the DWT was applied on the selected host image. The role of the algorithm was to ensure that the image is decomposed to yield four distinct frequency sub-bands. In turn, LU factorization was applied on the LL band. The aim was to decompose the latter to

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

form U, D and L – before applying the SVD on the selected D component. In turn, the D's diagonal singular value coefficients were modified relative to the chaotic mapped watermark's diagonal singular value coefficients. In the additional investigation by Jane and Elbaşi (2014a) [44], a non-blind hybrid image watermarking technique was proposed. The proposed scheme was based on the LU, SVD and DWT matrix decomposition. In the proposed technique, the researchers embedded the binary watermark into the host image, having employed the DWT algorithm on the same. In turn, LU composition was applied on the LL band before ensuring that it is decomposed to obtain three matrices; D, V and S. Eventually, the watermark was embedded into S, a singular value matrix. From the results, the proposed scheme was found to be robust and capable of minimizing attacks that target image processing; including rotation, filtering, and scaling. However, it was noted that the proposed scheme exhibited a limitation whereby it was highly complex. These results concurred with most of the findings documented by studies such as Wang et al. (2016) [45, 46-59]. Also, Fazli and Moeini (2016) [60] proposed a hybrid scheme. Authors initially applied DWT on host image and the partitioned the LH and HL into 8 X 8 block and then applied the DCT on these blocks. Finally authors, applied the SVD on those blocks. Singular values of SVD are used to embed the watermark.

In the study by Singh et al. (2017) [61], some of the codes that were employed involved QR, SVD and DWT. The role of the QR code entailed image watermarking. During the first stages, the DWT was applied to low-frequency bands and the host image. In turn, the frequency band was divided to obtain n x n block sizes through which the RGB component was established for the respective blocks. Eventually, SVD was applied on the respective RGB components to obtain singular values through which watermarking was implemented. In another investigation, Ni et al. (2006) [62] focused on the LWT as a watermarking scheme targeting images. Also, spatial tampering location was estimated using the chaotic sequence. Firstly, the LWT was applied on the host image. Secondly, the watermark was embedded into different sub-bands. Form the results, the proposed scheme were observed to stretch beyond spatial tampering localization to promote the process of estimating the forms of frequency operations. In a further investigation, Gao and Gu (2007) [63] advocated for the use of reversible image watermarking technique, relying on the chaotic system and LWT. Initially, the host image was split to form non-overlapping blocks. Later, the LWT was applied on the respective blocks before ensuring that the watermark was embedded into each block, as well as LL. The role of the chaotic system was to ensure that the blocks' positions were shuffled. Results demonstrated that the proposed scheme was robust and better placed to shun possible cropping attacks.

In Lizonget al. (2010) [64], the main objective was to determine the feasibility of implementing the blind-image watermarking scheme. The chaotic system and LWT were applied. Indeed, the binary watermark was inserted into a chosen gray scale image. From the findings, it was concluded that the proposed scheme was robust and would guard against attacks such as JPEG compression, salt and pepper noise, rotation, sharpening, and cropping. It is also worth indicating that the study by Ghaderiet al. (2013) [65] aimed at applying SVD and LWT to determine the degree of roobustness of the proposed scheme. During the initial phase, a 4-level LWT was applied, followed by SVD implementation on LH and HL sub-bands. Also, the watermark image was converted to obtain a binary image before embedding a watermark through the bands' singular value modification. Form the outcomes, the authros noted that the proposed scheme was robust and capable of guarding against attacks such as cropping, JPEG compression, resizing, scaling, rotation, and contrast adjustment. In Sarkar and Senthilkumar (2012) [66], SVD and LWT were also applied. Initially, the host image was targeted via the use of LWT whereby the LL band was split into 2X2-sized blocks. Eventually, SVD was applied before ensuring that the binary watermark was embedded via the blocks' singular value modification. Chamlawi and Khan (2010) [67] conducted a similar study whereby an LWT-based novel semi-fragile watermarking scheme was proposed. Indeed, two watermarks constituting the recovery watermark and the authentication watermark were inserted into the target bands. With the selected scheme seeking to give insight into the subject of image authenticity and recovery, findings demonstrated that the proposed scheme was secure and efficient, capable of preventing JPEG compression attacks.

It is also worth noting that Mehta et al. (2016) [68] sought to apply LSVR, QR and LWT algorithms to discern the degree of robustness of the proposed scheme. Given the host image, the LWT was applied before ensuring that low-frequency bands were divided into 4X4-sized non-overlapping blocks. In turn, QR decomposition was implemented, culminating into the embedding of a watermark in the first row of the respective blocks' R matrix. Indeed, findings demonstrated that the proposed scheme was robust and capable of preventing attacks such as JPEG compression, salt and pepper noise, scaling, and cropping. In another documentation, Su et al. (2012) [69] strived to apply LWT and how it could prove robust when implemented on color image. The initial stage entailed the convention of the mage into YCrCb color space, followed by LWT implementation on the resultant image. Also, the RGB component was used to embed the watermark into the color host image's frequency components constituting Cb, Cr and Y. Another study by Verma&Jha (2015a) [70] embraced the LWT algorithm in such a way that the LH sub-band was divided into non-overlapping blocks. In turn, there was a random shuffling of the blocks. The process paved the way for the embedding of the binary watermark into the selected blocks. Indeed, the study affirmed that a notable limitation associated with the proposed scheme was that it would not sustain attacks such as rotation, salt and pepper noise, and filtering. Hence, another scholarly investigation [71] was proposed. The proposed scheme employed the 3-level LWT on a given host image – before embedding the binary watermark into the target HL sub-band.

VII. IMAGE WATERMARKING IN THE TRANSFORM DOMAIN

In the spatial domain watermarking techniques researcher directly modify the pixel values of the host image to embed the watermark's bits. Many watermarking techniques have been developed till now. These techniques modifies the Least Significant Bit (LSB) of the host image. LSB watermarking technique is one of the traditional techniques of image watermarking that embed the watermark without introducing many perceptible distortions. In spatial domain watermarking, the watermark is commonly recovered using knowledge of the pseudo noise (PN) sequence and the statistical properties of the watermark embedding process.

Nikolaidis& Pitas (1998) [72] proposed a spatial domain watermarking scheme, watermarking is performed in the spatial domain by minor modification in the intensity of random selected pixels of host image.

Hernandez et al. (1998) [73] proposed an algorithm for grayscale images for performance analysis of a 2-D multiplulse amplitude modulation scheme.

Pitas (1998) [74] proposed method for grayscale digital image watermarking which is based on statistical detection theory. In this method author embedded predetermined small luminance value to randomly selected image pixels.

Lee & Won (1999) [75] proposed watermarking scheme based on error control coding (EEC) technique for grayscale image. Authors first use RS (Reed-Solomon) coding technique to generate the ECC code word of watermark, after that these generated ECC code words of watermark is embedded into two LSBs of the gray levels by randomly visiting the pixels in the host image.

Lee & Lee (1999) [76] proposed an adaptive watermarking technique that adaptively modified the intensities of some selected pixel and modification is not noticeable to human visual system. Authors firstpermute the watermark using two-dimensional pseudo-random number traversing method and decompose the host image in blocks before the watermark insertion. Authors also use a DES algorithm for secret key generation at the watermark insertion stage.

Lin (2000) [77] proposed a spatial domain watermarking approach for grayscale images which is based on block-oriented and modular-arithmetic. Authors first generate a unique watermark for each distribution and embedded it into the grayscale image. Authors also stated in this paper that the approach is much better than the Voyatazis& Pitas (1998) [19] scheme and more secure than the Cox et al. (1997) [16] method, this scheme is robust against JPEG compression and difficult for collusion attack.

Hernandezet al. (2000) [78] introduced a spatial domain watermarking scheme based on channel coding for still images. Authors stated in this theoretical model that scheme is robust against cropping, space-variant linear filtering processes and additive noise attacks and performance of this scheme under JPEG compression can be analyzed through a combination of quantization noise and block filtering.

Lu & Sun (2000b) [79] proposed a non-blind watermarking based on vector quantization **(**low-bit rate image compression scheme**)** and code word. Authors stated that, this scheme is robust against vector quantization attack.

Nikolaidis& Pitas (2000) [80] proposed a watermarking scheme based on chaotic theory and region based image segmentation for color facial images. In this scheme facial area of image is adopted for watermark insertion which is segmented from the host image. This watermarking scheme is robust against the geometric transformations viz. scaling, cropping and rotation, filtering, noise addition and compression attacks.

Yu et al. (2001) [81] proposed a blind watermarking scheme based on neural networks for color image. Authors use Blum-Blum-Blum pseudorandom number generators (PRNGs) for selection of a sub set of pixels of host image because two distinct sequences of random numbers are required to access any location of image (**x**-coordinate and **y**-coordinate). Authors stated that trained neural networks almost recover the exact watermark from host image against the various image processing attacks. So this scheme is much robust than other technique.

Makur&Selvi (2001) [82] proposed a blind watermarking scheme based on variable dimension vector quantization. Authors explored the both blind and non-blind versions of the proposed algorithm. Authors stated that blind version of algorithm is much robust than non-blind.

Liu & Chen (2001) [83] proposed a two-layer blind watermarking scheme for grayscale image both layer watermark insertion is done in spatial domain. In this scheme watermark is a serial number. Proposed scheme implemented by little intensity of most pixels. Authors stated that scheme is resistant to various attacks but not robust against geometric attack viz. scaling, rotation etc. but proposed scheme is fast and easy to implement.

Tsai et al. (2004) [84] proposed a new color image watermarking scheme based on the color quantization. Authors initially applied the DES algorithm on the watermark for encryption and perform the pixel mapping procedure on the host image to find the appropriate pixel. Finally insert the encrypted watermark in these selected pixels.

Simitopoulos et al. (2003) [85] proposed a watermarking scheme for color images based on Generalized Radon Transformations; authors initially generates the watermark, which is the random 2D sequence of +1 and -1. Now Harris corner detector technique is applied for detection of corner points of the host image preceded by radial integration transform (RIT) and circular integration transform (CIT) for robustness against geometrical transformation attacks. Then the additive watermark embedding is performed in spatial domain.

Seo&Yoo (2004) [86] proposed a scheme based on feature points. In this scheme authors initially extract the feature points of scale-space of the image and select the strongest scale-normalized corner. Now watermark is embedded in the host image on the basis of the characteristic scale at the selected feature points.

In the study by Chang et al. (2005) [87],the watermarking scheme that was investigated entailed gray level image. The watermark that was developed relied on a binary image in

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

SVD. During the irst stages, the host image was divided into different blocks before applying AVD for transformation. In turn, the watermark was embedded into the U and D components, having modified them.

VIII. RESULT AND DISCUSSION

The study of state of art contributions in the area of digital image watermarking reveals that robustness, security and imperceptibility are the main challenges of the watermarking scheme and there always exists a trade-off between robustness and imperceptibility. Over the years, researchers have focused on this trade-off and proposed various image watermarking schemes but with the advancement in technology especially imaging, need for more efficient algorithms arise. Moreover, with advancements, new high resolution digital imaging formats containing highly sensitive metadata needs protection too. Hence, this challenge remains, i.e. to have an algorithm that efficiently handles all the three factors together, in the area of image watermarking and the expectation to have a watermarked image equivalent (quality based) to the original image is increasing day-by-day. The research issues concluded based on the study of state of art contributions are:

- Most of the researchers have proposed watermarking scheme for either grayscale images or they used binary or grayscale watermark. Majority of these algorithms embedded single watermark in the host image. It has been realized that because of single watermark embedding major portions of the host image remain unsecured. Also, due to ease of color photography and imaging, organizations readily have high resolution colored images and color logo. Therefore, there is a need to have a scheme that support multiple watermark insertion in colored host image and preferably the watermark should also be either colored or holographic.
- Also, with the prominent development in the area of digital medical imaging and increase of frequency of communicating these medical images across the globe for different medical purposes, the need to protect these images became significant. To address this, Parah et al. (2015a) [53], Thakkar & Srivastava (2017) [52] and BW &Permana (2012) [88] proposed the watermarking scheme for medical images. But all these schemes were for grayscale .bmp format medical images and inserted grayscale watermark. But, current advanced medical imaging technologies used in sensitive medical equipment like Color Doppler, X-Ray, CT-Scan etc., generates high resolution digital imaging formats containing highly sensitive meta data like colored DICOM images. These images are highly susceptible to noise, hence the security of these images is a great challenge. Therefore, there is a need to have a scheme that can be applied these sensitive medical images.

IX. CONCLUSION

The process of incorporating certain digital information into the media o become part of the latter has gained growing interest in the research community. This paper has examined the background data regarding major factors contributing to and shaping trends in the subject of digital image watermarking. In most cases, the spatial and transform domains have gained growing attention in relation to the image watermarking practice. The study has also examined different methods of watermarking, especially in relation to the literature regarding various scholarly insights and investigations that have been conducted and the findings reported previously. The web of science has been used as an ideal database from which the research articles have been selected. Findings demonstrate that most of the watermarking techniques are yet to achieve desirable levels of imperceptibility, security, and robustness. Hence, the study recommends that in the medical field, robust techniques of image watermarking are designed to respond to the ever-changing and growing needs of the target audiences.

REFERENCES

1. Johnson, N. F., & Jajodia, S. (1998), "Exploring steganography: Seeing the unseen", *IEEE Computer*, vol. 31(2) pp. 26-34.
2. Judge, J. C. (2001), "Steganography: Past, present and future", (No. UCRL-ID-151879). Lawrence Livermore National Lab., CA (US). 2001.
3. Chandramouli, R., & Memon, N. (2001), "Analysis of LSB Based Image Steganography", *IEEE International Conference on Image Processing*, Vol. 3, pp. 1019-1022.
4. Kahn, D. (1996b), "The history of steganography", *Proceedings of the 1st international workshop on Information Hiding*, pp 1-5.
5. Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999), "Information hiding – a survey", *Proceedings of the IEEE (USA*), vol. 87(7), pp. 1062–1078.
6. Zhao, J. (1997), "Look, it's Not There – Digital watermarking is the best way to protect intellectual property from illicit copying". *byte.com.* http://www.byte.com/art/9701/sec18/art1.htm
7. Aggarwal, A., & Singla, M. (2011), "Image Watermarking Techniques in Spatial Domain: A Review", *International Journal of Computer Technology and Applications*, vol. 2(5), pp. 1357–1363.
8. Singh, A. K., Dave, M., & Mohan, A. (2014), "Wavelet based image watermarking: futuristic Concepts in information security". *Proc. Natl Acad. Sci*., India, Sect A 84(3) pp.345-359.
9. Shih, F. Y., & Wu, Y. T. (2005), "Robust watermarking and compression for medical images based on genetic algorithms", *Information Sciences*, vol. 175, no. 3, pp. 200 - 216.
10. Swanson, M. D., Kobayashi, M., & Tewfik, A. H. (1998), "Multimedia data embedding and watermarking technologies", *Proceedings of the IEEE*, Vol. 86, No. 6, pp. 1064-1087.
11. Wolfgang, R. B., Podilchuk, C. I., & Delp, E. J. (1999), "Perceptual watermarks for digital images and video," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1108-1126.
12. Wolfgang, R. B., & Delp, E. J. (1999), "Fragile watermarking using the VW2D watermark ", *Proceedings of the SPIE/IS&T Conference on Security and Watermarking of Multimedia Contents, SPIE* , San Jose, CA, vol. 3657, pp. 204-213.

13. Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007), "*Digital Watermarking and Steganography, 2nd ed. San Francisco*", CA, USA: Morgan Kaufmann Publishers Inc., ISBN: 9780080555805.
14. Langelaar, G. C., Lagendijk, R. L., & Biemond, J. (1998), "Real-time labeling of MPEG-2 compressed video," *J. Visual Commun. Image Representation*, vol. 9, no. 4, pp. 256-270.
15. Mohanty, S. P. (1999), "Digital Watermarking: A Tutorial Review", URL: www.csee.usf.edu/~smohanty/research/Reports/ WMSurvey1999Mohanty.pdf
16. Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997), "Secure spread spectrum watermarking for multimedia," in *IEEE Transactions on Image Processing*, Vol. 6(12), pp. 1673-1687.
17. Barni, M., Bartolini, F., Cappellini, V., & Piva, A. (1998a), "Copyright protection of digital images by embedded unperceivable marks", *Image and Vision Computing*, Vol. 16(12–13), pp. 897-906.
18. Barni, M., Bartolini, F., Cappellini, V., & Piva, A. (1998b), "A DCT-domain system for robust image watermarking", *Signal Processing*, Vol. 66(3), pp. 357-372.
19. Voyatzis, G., & Pitas, I. (1998), "Digital image watermarking using mixing systems", *Computers & Graphics*, vol. 22, Issue 4, pp. 405-416.
20. Ruanaidh, J. J. O., & Pun, T. (1998), "Rotation, scale and translation invariant spread spectrum digital image watermarking", *Signal Processing*, Volume 66, Issue 3, pp. 303-317.
21. Delaigle, J. F., De Vleeschouwer, C., & Macq, B. (1998, "Watermarking algorithm based on a human visual model", *Signal Processing*, Vol. 66(3), pp. 319-335, ISSN 0165-1684
22. Podilchuk, C. I., & Zeng, W. (1998), Image-adaptive watermarking using visual models, in *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525-539.
23. Hsu, C. T., & Wu, J. L. (1998), Multiresolution Watermarking for Digital Images,*IEEE Transactions On Circuits and Systems—Ii: Analog and Digital Signal Processing*, Vol. 45(8), pp. 1097-1101.
24. Wei, Z. H., Qin, P., & Fu, Y. Q. (1998), "Perceptual digital watermark of images using wavelet transform" *IEEE Transactions on Consumer Electronics*, vol. 44(4), pp. 1267 - 1272.
25. Wang, H. J. M., Su, P. C., & Kuo, C. C. J. (1998), "Wavelet-based digital image watermarking," *Opt. Express 3*, pp. 491-496.
26. Xia, X. G., Boncelet, C. G., & Arce, G. R. (1998), "Wavelet transform based watermark for digital images," *Opt. Express 3*, pp. 497-511.
27. Borş, A. G., & Pitas, I. (1998), "Image watermarking using block site selection and DCT domain constraints," *Opt. Express*, 3, 512-523.
28. Hsu, C. T., & Wu, J. L. (1999), "Hidden digital watermarks in images," in *IEEE Transactions on Image Processing*, Vol. 8(1), pp. 58-68.
29. Kim, Y. S., Kwon, O. H., & Park, R. H. (1999), "Wavelet based watermarking method for digital images using the human visual system," *Circuits and Systems,. ISCAS '99. Proceedings of the 1999 IEEE International Symposium on*, Orlando, FL, pp. 80-83 vol.4.
30. Zhu, W., Xiong, Z., & Zhang, Y. Q. (1999), "Multiresolution watermarking for images and video," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 9, no. 4, pp. 545-550, Jun.
31. Suthaharan, S., Kim, S. W., Lee, H. K., & Sathananthan, S. (2000), "Perceptually tuned robust watermarking scheme for digital images", *Pattern Recognition Letters*, Volume 21, Issue 2, pp.145-149.
32. Wu, C. F., & Hsieh, W. S. (2000), "Image refining technique using digital watermarking," in *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 1-5.
33. 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*, vol. 46, no. 1, pp. 137-145.
34. Falkowski, B. J., & Lim, L. S. (2000), "Image watermarking using Hadamard transforms", *Electronics Letters*, Vol. 36(3), pp. 211-213.
35. Pereira, S., & Pun, T. (2000), "Robust template matching for affine resistant image watermarks", *IEEE Transactions on Image Processing*, vol. 9, no. 6, pp. 1123-1129.
36. Huang, J., Shi, Y. Q., & Shi, Y. (2000), "Embedding image watermarks in dc components," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, no. 6, pp. 974-979.
37. Lu, C. S., Huang, S. K., Sze, C. J., & Liao, H. Y. M. (2000a), "Cocktail watermarking for digital image protection," in *IEEE Transactions on Multimedia*, vol. 2, no. 4, pp. 209-224.
38. Lin, N., Shen, J., Guo, X., & Zhou, J. (2011), "A robust image watermarking based on DWT-QR decomposition," IEEE 3rd International Conference on Communication Software and Networks, Xi'an, pp. 684-688.
39. Wang, Y., Doherty, J. F., & Van Dyck, R. E. (2002a), "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Transactions *on Image Processing*, vol. 11, no. 2, pp. 77-88
40. Barni, M., Bartolini, F., & Piva, A. (2002), "Multichannel watermarking of color images," in *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 12(3), pp. 142-156.
41. Chen, L. H., & Lin, J. J. (2003), "Mean quantization based image watermarking", *Image and Vision Computing*, Vol. 21(8), pp. 717-727.
42. Hsieh, S. L., Hsu, L. Y., & Tsai, I. J. (2005), "A Copyright Protection Scheme for Color Images using Secret Sharing and Wavelet Transform", *Proceedings of World Academy of Science, Engineering and Technology*, Vol. 10, 3159-3165.
43. Jane, O., Ilk, H. G., & Elbasi, E. (2013), "A secure and robust watermarking algorithm based on the combination of DWT, SVD, and LU decomposition with Arnold's Cat Map approach,"*8th International Conference on Electrical and Electronics Engineering (ELECO)*, Bursa, pp. 306-310.
44. Jane, O., & Elbaşi, E. (2014a), "A new approach of non-blind watermarking methods based on DWT and SVD via LU Decomposition" *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 22, no. 5, pp. 1354-1366.
45. Wang, D., Yang, F., & Zhang, H. (2016), "Blind Color Image Watermarking Based on DWT and LU Decomposition," *Journal of Information Processing Systems*, vol. 12, no. 4, pp. 765-778.
46. Lin, N., Shen, J., Guo, X., & Zhou, J. (2011), "A robust image watermarking based on DWT-QR decomposition," *IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, pp. 684-688.
47. Su, Q., Niu, Y., Wang, G., Jia, S., & Yue, J. (2014a). "Color image blind watermarking scheme based on QR decomposition", *Signal Processing*, vol. *94*(1), pp. 219-235.
48. Su, Q., Niu, Y., Zou, H., Zhao, Y., & Yao, T. (2014b). "A blind double color image watermarking algorithm based on QR decomposition", *Multimedia Tools and Applications*, vol. *72*(1), pp. 987–1009.
49. Kuobin, D. (2011), "Singular Value Decomposition Watermarking Method for Medical Image," *International Conference on Intelligence Science and Information Engineering*, Wuhan, 2011, pp. 546-548.

50. Çetinel, G., & Çerkezi, L. (2016), "Wavelet Based Medical Image Watermarking Scheme for Patient Information Authenticity" *International Journal of Applied Mathematics, Electronics and Computers*", Vol. 4(Special Issue), pp.220–223.
51. Parah, S. A., Sheikh, J. A., Assad, U. I., & Bhat, G. M. (2015b), "Hiding in encrypted images: a three tier security data hiding technique", *Multidim Syst Sign*, vol. 28, Issue 2, pp 549–572.
52. Thakkar, F. N., & Srivastava, V. K. (2017), "A blind medical image watermarking: DWT-SVD based robust and she cure approach for telemedicine applications", *Multimedia Tools Appl.* Vol.76, pp. 3669–3697.
53. Parah, S. A., Sheikh, J. A., Ahad, F., Loan, N. A., & Bhat, G. M. (2015a), "Information hiding in medical images: a robust medical image watermarking system for E-healthcare", *Multimedia Tools and Applications*, vol.76, no.8, pp. 10599-10633.
54. Naderahmadian, Y., & Hosseini-Khayat, S. (2010). "Fast watermarking based on QR decomposition in Wavelet domain", *Sixth international conference on intelligent information hiding and multimedia signal processing*, pp. 127–130.
55. Song, W., Hou, J. J., Li, Z. H., & Huang, L. (2011), "Chaotic system and QR factorization based robust digital image watermarking algorithm". *Journal of Central South University of Technology*, 18(1), 116–124.
56. Su, Q., Wang, G., Zhang, X., Lv, G., & Chen, B. (2017), "An improved color image watermarking algorithm based on QR decomposition," *Multimed. Tools Appl*., vol. 76, Issue 1, pp 707–729.
57. Bhatnagar, G., & Raman, B. (2009), "A new robust reference watermarking scheme based on DWT-SVD", *Computer Standards & Interfaces*, Vol. 31(5), pp. 1002-1013.
58. Sleit, A., Abusharkh, S., Etoom, R., & Khero, Y. (2012), "An enhanced semi-blind DWT-SVD-based watermarking technique for digital images", *The Imaging Science Journal*, vol. 60, no. 1, pp. 29-38.
59. Golshan, F., & Mohammadi, K. (2013), "A hybrid intelligent SVD-based perceptual shaping of a digital image watermark in DCT and DWT domain", *Imaging Sci. J.*, Vol. 61(1), pp. 35-46.
60. Fazli, S., & Moeini, M. (2016), "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks", *Optik - International Journal for Light and Electron Optics*, Vol. 127(2), pp. 964-972.
61. Singh, R. K., Shaw, D. K., & Sahoo, J. (2017), "A secure and robust block based DWT-SVD image watermarking approach", *Journal of Information & Optimization Sciences*, vol. 38, issue. 6, pp. 911-925.
62. Ni, R., Ruan, Q., & Liu, J. (2006), "Tampering estimation watermarking based on lifting wavelet and chaotic sequence," *2006 8th international Conference on Signal Processing*, Beijing.
63. Gao, T. G., &Gu, Q. L. (2007), "Reversible watermarking algorithm based on wavelet lifting scheme," *2007 International Conference on Wavelet Analysis and Pattern Recognition*, Beijing, pp. 1771-1775.
64. Lizong, L., Tiegang, G., Qiaolun, G., & Lei, B. (2010), "A Verifiable Copyright-Proving Scheme Based on Lifting Wavelet Transformation,"*Third International Symposium on Intelligent Information Technology and Security Informatics*, Jinggangshan, pp. 68-72.
65. Ghaderi, K., Akhlaghian, F., & Moradi, P. (2013), "A new robust semi-blind digital image watermarking approach based on LWT-SVD and fractal images,"*21st Iranian Conference on Electrical Engineering (ICEE)*, Mashhad, pp. 1-5.
66. Sarkar, S., & Senthilkumar, K. (2012), "A highly secured Digital Watermarking Algorithm for Binary Watermark using Lifting Wavelet Transform and Singular Value Decomposition", *IET Chennai 3rd International on Sustainable Energy and Intelligent Systems (SEISCON 2012)*, Tiruchengode, pp. 1-5.
67. Chamlawi, R., & Khan, A. (2010), " Digital image authentication and recovery: Employing integer transform based information embedding and extraction", *Information Sciences*, Vol. 180(24), pp. 4909-4928.
68. Mehta, R., Rajpal, N., & Vishwakarma, V. P. (2016), V.P.,"LWT- QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR", *Multimed Tools Appl*, vol. 75, pp. 4129-4150.
69. Su, Q., Niu, Y., Liu, X., & Zhu, Y. (2012), "A blind dual color images watermarking based on IWT and state coding," *Optics Commun.*, vol. 285, no. 7, pp. 1717 – 1724.
70. Verma, V. S., & Jha, R. K. (2015b), "Improved watermarking technique based on significant difference of lifting wavelet coefficients," *Signal, Image and Video Process.*, vol. 9, no. 6, pp. 1443-1450.
71. Verma, V. S., & Jha, R. K. (2015a), Aparajita Ojha,"*Significant region based robust watermarking scheme in lifting wavelet transform domain " Expert Systems with Applications*, vol. 42, Issue 21, pp. 8184-8197.
72. Nikolaidis, N., & Pitas, I. (1998), "Robust image watermarking in the spatial domain", Signal Processing, Volume 66, Issue 3, pp.385-403.
73. Hernández, J. R., Perez-Gonzalez, F., Rodriguez, J. M., & Nieto, G. (1998), "Performance analysis of a 2-D-multipulse amplitude modulation scheme for data hiding and watermarking of still images". *IEEE Journal on Selected areas in Communications*, 16(4), 510-524.
74. Pitas, I. (1998), "A method for watermark casting on digital image," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 8, no. 6, pp. 775-780.
75. Lee, J., & Won, C. S. (1999), "Authentication and correction of digital watermarking images," in *Electronics Letters*, vol. 35, no. 11, pp. 886-887.
76. Lee, C. H., & Lee, Y. K. (1999), "An adaptive digital image watermarking technique for copyright protection,"*IEEE Transactions on Consumer Electronics*, vol. 45, no. 4, pp. 1005-1015.
77. Lin, P. L. (2000), Robust transparent image watermarking system with spatial mechanisms, Journal of Systems and Software, Volume 50, Issue 2, pp. 107-116.
78. Hernández, J. R., Rodrıguez, J. M., & Pérez-González, F. (2000). Improving the performance of spatial watermarking of images using channel coding. Signal Processing, 80(7), 1261-1279.
79. Lu, Z. M., & Sun, S. H. (2000b), "Digital image watermarking technique based on vector quantisation," in *Electronics Letters*, vol. 36, no. 4, pp. 303-305.
80. Nikolaidis, N., & Pitas, I. (1998), "Robust image watermarking in the spatial domain", *Signal Processing*, Volume 66, Issue 3, pp.385-403.
81. Yu, P. T., Tsai, H. H., & Lin, J. S. (2001), "Digital watermarking based on neural networks for color images", *Signal Processing*, vol. 81, Issue 3, ISSN 0165-1684, pp. 663-671.
82. Makur, A., & Selvi, S. S. (2001), "Variable dimension vector quantization based image watermarking, *Signal Processing*", Volume 81, Issue 4, ISSN 0165-1684, pp. 889-893, April 2001.
83. Liu, J. C., & Chen, S. Y. (2001), "Fast two-layer image watermarking without referring to the original image and watermark", *Image and Vision Computing*, Volume 19, Issue 14, 1, pp. 1083-1097, Dec 2001.

84. Tsai, P., Hu, Y. C., & Chang, C. C. (2004), "A color image watermarking scheme based on color quantization", *Signal Processing*, Volume 84, Issue 1, pp. 95-106, ISSN 0165-1684.
85. Simitopoulos, D., Koutsonanos, D. E., & Strintzis, M. G. (2003), "Robust image watermarking based on generalized Radon transformations," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 732-745.
86. Seo, J. S., &Yoo, C. D. (2004), "Localized image watermarking based on feature points of scale-space representation", *Pattern Recognition*, Volume 37, Issue 7, pp. 1365-1375.
87. Chang, C. C., Tsai, P., & Lin, C. C. (2005), "SVD-based digital image watermarking scheme", *Pattern Recognition Letters*, Vol. 26(10), pp. 1577-1586.
88. BW, T. A., & Permana, F. P. (2012), "Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and Run Length Encoding(RLE) compression", *Proceedings of the IEEE International Conference on Communication, Networks and Satellite* (COMNETSAT '12) Bali, Indonesia, pp. 167–171.