

# Towards Optimal Copyright Protection Using Neural Networks Based Digital Image Watermarking

Mokhtar Hussein  
Computer Science Department  
Kakatiya University  
Warangal - India  
*msorori201201@gmail.com*

Dr. B. Manjula  
Computer Science Department  
Kakatiya University  
Warangal - India  
*manjulabairam@gmail.com*

**Abstract**—In the field of digital watermarking, digital image watermarking for copyright protection has attracted a lot of attention in the research community. Digital watermarking contains various techniques for protecting the digital content. Among all those techniques, Discrete Wavelet Transform (DWT) provides higher image imperceptibility and robustness. Over the years, researchers have been designing watermarking techniques with robustness in mind, in order for the watermark to be resistant against any image processing techniques. Furthermore, the requirements of a good watermarking technique include a tradeoff between robustness, image quality (imperceptibility) and capacity. In this paper, we have done an extensive literature review for the existing DWT techniques and those combined with other techniques such as Neural Networks. In addition to that, we have discussed the contribution of Neural Networks in copyright protection. Finally we reached our goal in which we identified the research gaps existed in the current watermarking schemes. So that, it will be easy to obtain an optimal technique to make the watermark object robust to attacks while maintaining the imperceptibility to enhance the copyright protection.

**Keywords**-Digital Image Watermarking DWT, Blind DWT, Non-Blind DWT, Neural Networks, SVD.

\*\*\*\*\*

## I. INTRODUCTION

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, similar to a paper containing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also carried along in the copy. In visible digital watermarking, the information is visible in the image or video. Typically, the information is text or a logo, which identifies the owner of the media. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such and it may be possible to detect that some amount of information is hidden in the signal itself. The watermark may be intended for general use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal.

Among all other watermarking, image watermarking particularly has special attention in the research community. Most of the research work is dedicated to image watermarking as compared to audio and video. The reasons for it, because of ready availability of the test images, secondly because it carries enough redundant information to provide an opportunity to embed watermarks easily, and, it may be assumed that any successful image watermarking algorithm may be upgraded for the video also.

Images are represented or stored in spatial domain as well as in transform domain. The transform domain image is represented in terms of its frequencies; whereas, in spatial domain it is represented by pixels. In simple terms, transform domain means the image is segmented into multiple frequency bands. To transfer an image to its frequency representation, we can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or

Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. called the transform domain coefficients. Generally, the embedding is performed after transforming the image in to other domain. Generally these techniques use DCT, DFT, or DWT. In case of spatial domain, simple watermarks could be embedded in the images by modifying the pixel values or the Least Significant Bit (LSB) values. In this type of techniques, the embedding is performed directly on image data. It is easy to implement on computational point of view but too fragile to withstand large varieties of external attacks, but still there are many available ways which minimize its drawbacks. However, more robust watermarks could be embedded in the transform domain of images by modifying the transform domain coefficients.

In transform domain watermarking schemes, the embedding is performed after transforming the image in to other domain. Generally these techniques use DCT, DFT, or DWT.

Among all the different techniques of transform domain, Discrete Wavelet Transform (DWT) typically provide higher image imperceptibility and are much more robust technique to image manipulation. In this domain watermark is placed in perceptually significant coefficients of the image. However, DWT has been used more frequently in digital image watermarking due to its time/frequency decomposition characteristics, which resemble to the theoretical models of the human visual system. In order to further performance improvements in DWT-based digital image watermarking algorithms could be obtained by joining DWT with DCT. The reason of applying two transform is based on the fact that jointed transform make up for the disadvantages of each other, so that effective watermark could be formed.

In this paper, we are going to state the literature review of the most important researches already done one the field of digital watermarking. The goal of this paper is to identify the

research gaps and existed issues to obtain an optimal techniques to make the watermark object robust to attacks while maintaining the imperceptibility to enhance the copyright protection using DWT along with Neural Networks. In order to achieve that, we are going to do an extensive literature review for the most important techniques uses DWT and Neural Networks based watermarking.

## II. DWT BASED WATERMARKING SCHEME

Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image. It gained widespread acceptance in signal processing, image compression and watermarking. It decomposes a signal into a set of functions, called wavelets. Wavelets are created by translation and dilations of a fixed function called mother wavelet. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Discrete Wavelet transformation is very suitable to identify the areas in the cover image where a secret image can be embedded effectively. This property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, it modifies only the region corresponding to that coefficient. The embedding watermark in the lower frequency sub-bands may degrade the image as generally most of the image energy is stored in these sub-bands. However it is more robust. The high frequency part contains information about the edge of the image so this frequency sub-bands are usually used for watermarking since the human eye is less sensitive to changes in edges to this frequency sub-bands.

A discrete-wavelet transform based multiple watermarking algorithm (Tao et al., 1997) describes two important tools encryption and watermarking can be used to prevent unauthorized consumption and duplication. The watermark is embedded into LL and HH sub bands to improve the robustness. This approach is useful in such a way that embedding the watermark in lower frequencies is robust to a group of attacks such as JPEG compression, blurring, adding Gaussian noise, rescaling, rotation, cropping, pixelation, sharpening and embedding the watermark in higher frequencies is robust to another set of attacks such as histogram equalization, intensity adjustment, and gamma correction.

An integer wavelet based watermarking techniques (Luo et al., 2005) introduced to protect the copyright technique to enhance the security. This technique is useful for digital watermarking in DEM (Digital Elevation Mode) data, which effectively protects the copyright of DEM data and avoids the unauthorized user.

Recent researchers on secure digital watermarking techniques have revealed the fact that the content of the images could be used to improve the invisibility and robustness of a watermarking scheme. In this approach, watermark is created from the content of the host image and DWT is used for embedding watermarks, since it is an excellent time frequency analysis method which can be adapted well for extracting the information content of the image. Wand et al., adopt a key dependent wavelet transform. To take the advantage of localization and multi-resolution property of the wavelet transform, (Wang et al., 2002) proposed wavelet tree based watermarking algorithm. In this approach, the host image is transformed into wavelet coefficients using a discrete-time wavelet transform (DTWT). This technique is useful for removal of high-pass details in JPEG compression and robust

to time domain attacks such as pixel shifting and rotation. In addition to copyright protection, the proposed watermarking scheme can also be applied to data hiding or image authentication.

DWT based watermarking schemes follow the same guidelines as DCT based schemes, i.e. the underlying concept is the same; however, the process to transform the image into its transform domain varies and hence the resulting coefficients are different. Wavelet transform use wavelet filters to transform the image. There are many available filters, although the most commonly used filters for watermarking are Haar Wavelet Filter, Daubechies Orthogonal Filters and Daubechies Bi-Orthogonal. Each of these filters decomposes the image into several frequencies. Single level decomposition gives four frequency representations of the images. For that (Potdar et al., 2015), authors presented a survey of wavelet based watermarking algorithms. They classify algorithms based on decoder requirements as Blind Detection or Non-blind Detection. Blind detection doesn't require the original image for detecting the watermarks; however, non-blind detection requires the original image.

### A. DWT Based Blinded Watermark Detection

A DWT based blind watermarking scheme (Lie et al., 2009) defies by scrambling the watermark using chaos sequence. In addition, watermarking in DWT domain has drawn extensive attention for its good time-frequency features and its accurate matching of the HVS.

A novel watermarking technique called as "Cocktail Watermarking" (Lu et al., 2000) embeds dual watermarks which complement each other. This scheme is resistant to several attacks, and no matter what type of attack is applied; one of the watermarks can be detected. Furthermore, they enhance this technique for image authentication and protection by using the wavelet based Just Noticeable Distortion (JND) values. Hence this technique achieves copyright protection as well as content authentication simultaneously.

A multi-resolution watermarking scheme (Zhu et al., 2016) for watermarking video and images is embedded in all the high pass bands in a nested manner to multiple resolutions. This scheme doesn't consider the HVS aspect; however, this scheme is improved (Kaewkamnerd et al., 2000) by adding the HVS factor in account.

A blind image watermarking scheme (Peng Lie et al., 2009) based on wavelet tree quantization selects the largest two coefficients as significant coefficients and the difference between them is taken as significant difference. A watermark bit is embedded by comparing the significant difference with an average significant difference value and maximum difference coefficients are quantized.

A new robust fragile double image watermarking algorithm (Bo Chen et al., 2009) using improved pixel-wise masking model and a new bit substitution based on pseudorandom sequence. The method embeds robust and fragile watermark into the insensitive part and sensitive part of wavelet coefficients making two watermarks noninterfering.

### B. DWT Based Non-Blinded Watermark Detection

This technique requires the original image for detecting the watermark. Most of the schemes found in literature use a smaller image as a watermark and hence cannot use correlation based detectors for detecting the watermark; as a result they rely on the original image for informed detection. The size of

the watermark image (normally a logo) normally is smaller compared to the host image.

Another robust watermarking technique base on image fusion embedded (Lu et al., 2003) grayscale and binary watermark which is modulated using the "totalautomorphism". The novelty of this technique lies in the use of secret image instead of host image for watermark extraction and use of image dependent and image independent permutations to de-correlate the watermark logo.

A multiple watermarking scheme (Raval et al., 2003) argued that if the watermark is embedded in the low frequency components, it is robust against low pass filtering, lossy compression and geometric distortion. On the other hand, if the watermark is embedded in high frequency components, it is robust against contrast and brightness adjustment, gamma correction, histogram equalization and cropping and vice-versa. Thus, to achieve overall robustness against a large number of attacks, the authors proposed to embed multiple watermarks in low frequency and high frequency bands of DWT. Scheme was visible in some parts of the image especially in the low frequency areas, which reduced the commercial value of the image. Hence they generalized their scheme by using all the four sub bands and embedding the watermark in SVD domain.

The core technique is to decompose an image into four sub band and then applying SVD to each band. The watermark is actually embedded by modifying the singular values from SVD.

Normalized correlation is used to evaluate the robustness of the extracted watermark. Another scheme proposed later and termed as FuseMark (Kundur D. et al., 2004) which includes minimum variance fusion for watermark extraction. Here, they propose to use a watermark image whose size is a factor of the host by  $2xy$ . The quality of the extracted watermark is determined by Similarity Ratio measurement for objective calculation.

### III. RECENT METHODOLOGIES COMBINED WITH SOFT COMPUTING TOOLS

Now-a-days, researchers are focusing on mixing of spatial and transformed domains (i.e. combinations of DFT, DWT and DCT) concepts and also applying more and more mathematical and statistical model, and other interdisciplinary approaches in watermarking: for example use of chaotic theory, fractal image coding, neural network etc. In this section we are presenting the brief of few recent watermarking algorithms.

A reversible watermarking scheme (Voigt M. et al., 2004) for the 2D-vector data (point coordinates), which are used in geographical information related applications, exploits the high correlation among points in the same polygon in a map and achieves the reversibility of the whole scheme by an 8-point integer DCT, which ensures that the original 2D-vector data can be watermarked during the watermark embedding process and then perfectly restored during the watermark extraction process. To alleviate the visual distortion in the watermarked map caused by the coefficient modification, they proposed an improved reversible watermarking scheme based on the original coefficient modification technique. Combined with this improved scheme, the embedding capacity could be greatly increased while the watermarking distortion is reduced as compared to the original coefficient modification scheme.

In (Pastoriza J.R.T. et al., 2006), authors presented zero-knowledge watermark detectors. Current detectors are based on a linear correlation between the asset features and a given secret sequence. This detection function is susceptible of being

attacked by sensitivity attacks for which zero-knowledge does not provide protection. In this work, a new zero-knowledge watermark detector robust to sensitivity attacks is presented, using the generalized Gaussian Maximum Likelihood (ML) detector as the basis.

A spread spectrum watermarking algorithm introduced (Piper A. et al., 2005) which had both resolution and quality scalability demonstrated through experimental testing using the JPEG2000 compression algorithm. To alleviate this trade off, they began with a non-adaptive resolution scalable algorithm and exploited the contrast sensitivity and texture masking characteristics of the HVS to construct an HVS adaptive algorithm that has good quality scalability. The algorithm is specifically designed to concentrate on textured regions only, avoiding the visible distortions, which may occur when strength increases are applied to edges. Furthermore, this texture algorithm is applied in the wavelet domain but uses only a single resolution for each coefficient to be watermarked.

A DWT-based image watermarking algorithm (Deng et al., 2012) in which the code-division multiple access (CDMA) encoded binary watermark, adaptively is embedded into the third level detail sub-band of DWT domain. It can be inferred from the literature survey that many of the algorithms proposed met the imperceptibility requirement quite easily but robustness to different image processing are mainly applied to content authentication attacks is the key challenge and the algorithms in literature addressed only a subset of attacks.

A new image adaptive watermarking scheme (Zhu X., et al., 2006) based on perceptually shaping watermark block wise. Instead of the global gain factor, a localized one is used for each block. Watson's DCT-based visual (Watson A.B., et al., 1992) model is adopted to measure the distortion of each block introduced by watermark, rather than the whole image. With the given distortion constraint, the maximum output value of linear correlation detector is derived in one block, which demonstrated the reachable maximum robustness in a sense.

An Independent Component Analysis (Bounkong S. et al., 2003) based watermarking method is domain-independent ICA-based approach. This approach can be used on images, music or video to embed either a robust or fragile watermark. In the case of robust watermarking, the method shows high information rate and robustness against malicious and non-malicious attacks while inducing low distortion. Another version of this scheme is a fragile watermarking scheme which shows high sensitivity to tampering attempts while keeping the requirement for high information rate and low distortion. The improved performance is achieved by employing a set of statistically independent sources (the independent components) as the feature space and principled statistical decoding methods.

A dual watermarking Scheme (Schlauweg M. et al., 2006) was presented. In general, the watermark embedding process affects the fidelity of the underlying host signal. Fidelity, robustness and the amount of data which can be embedded without visible artifacts, often conflict. Most of early watermarking schemes have focused on embedding the watermark information applying a global power constraint such as the Peak-Signal-to-Noise-Ratio (PSNR) to satisfy fidelity constraints. But, the PSNR value is reflecting human's visual system because local image properties such as edges or textures are not considered. The watermarking systems have been proposed that allowed the embedded signal to be locally varied in response to the local properties of the corresponding host signal.

Authors in their paper (Huang X.Y. et al., 2007) presented an improved invariant wavelet and designed a DCT based blind watermarking algorithm against Rotation-and Scaling-and Translation (RST) attacks by exploiting the affined invariance of the invariant wavelet. Surviving geometric attacks in image watermarking is considered to be of great importance. In the face of geometrical attacks, all shortcomings of almost all digital watermarking algorithms have been exposed. The experiments show that this novel watermarking algorithm is robust against filter, noise and arbitrary RST geometrical attacks, however, sensitive to local crop attacks.

An image watermarking scheme (Wang J., et al., 2006) based on 3-D DCT is decomposed into a 3-D sub-image sequence by sub sample of zigzag scanning order that is transformed using block-based 3-D DCT. Simultaneously, they proved that the distribution of 3-D DCT AC coefficients follows the generalized Gaussian density function using the distribution relative entropy theory. To satisfy the balance between the robustness and the imperceptivity, a 3-D HVS model is improved to adjust the embedding strength. In watermark detecting, the optimum detector is used to implement the blind detection. It is shown in experiments that the scheme is strongly robust against various attacks.

Digital watermarking scheme uses the properties of DCT and DWT (Tripathi S. et al., 2006) to achieve almost zero visible distortion in the watermarked images. These schemes use a unique method for spreading, embedding and extracting the watermark. Embedding using a linear relation between the transform coefficients of the watermark and a security matrix has been proposed with satisfactory results.

Algorithm is based on multistage Vector Quantization (VQ) (Lu Z.M., 2005) that embeds both robust watermark for copyright protection or ownership verification and fragile watermark for content authentication or integrity attestation. The method in combined DCT and VQ to simultaneously embed robust and fragile watermarks.

In the field of color images watermarking, many methods are accomplished by marking the image luminance, or by processing each color channel separately. Therefore (Li X. et al, 2004) introduced a new DCT domain watermarking expressly devised for RGB color images based on the diversity technique in communication system. Experimental results, as well as theoretical analysis, are presented to demonstrate the validity of the new approach with respect to algorithm operating on image luminance only.

Genetic watermarking based on transform-domain techniques. A genetic algorithm (Chin-Shiuh Shieha et al., 2004) is a search heuristic used for optimization. It generates solutions using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover. The evolution usually starts from a population of randomly generated individuals and happens in generations. In each generation, the fitness of every individual in the population is evaluated, multiple individuals are stochastically selected from the current population (based on their fitness), and modified (recombined and possibly randomly mutated) to form a new population. The new population is then used in the next iteration of the algorithm. Commonly, the algorithm terminates when either a maximum number of generations has been produced, or a satisfactory fitness level has been reached for the population. In case of watermarking, the singular values (SVs) of the host image are modified by multiple scaling factors to embed the watermark image. Modifications are

optimized using GA to obtain the highest possible robustness without losing the transparency.

#### IV. CONTRIBUTION OF NEURAL NETWORK IN COPYRIGHT PROTECTION

An artificial neural network (ANN) is a mathematical model or computational model that is inspired by the structure and/or functional aspects of biological neural networks. A neural network consists of an interconnected group of artificial neurons, and it processes information using a connectionist approach to computation. They are usually used to model complex relationships between inputs and outputs one algorithm (Chuan-Yu Chang et. al., 2010) introduced copyright protection for images with a full counter-propagation neural network (FCNN). Most attacks do not degrade the quality of detected watermark image as FCNN has storage and fault tolerance. Authors (Quan Liu et. al., 2005) designed and realized meaningful digital watermarking algorithm based on Radial Basis Function (RBF) neural network. RBF Neural network is used to simulate human visual system to determine watermark embedding intensity.

An adaptive digital watermarking scheme (Zhang Zhi-Ming et al., 2014) with RBF neural networks, in which a visually recognizable binary image watermark is embedded into the DCT domain of the cover image. The watermark was encrypted by chaotic series and inserted into the middle frequency coefficients of the cover image's blocked DCT based transform domain. According to authors, to make the watermark stronger to resist different types of attacks, it is important to adapt the embedding maximum amount of interested watermark before the watermark becomes visible. For that, RBF neural networks are used to achieve maximum-strength watermark according to the frequency component feature of the cover image. Experimental results show that the proposed techniques have good imperceptibility and can survive of common image processing operations and JPEG lossy compression with high robustness. They do not compute processing time spans of any process utilized in this algorithm.

In 2013, M. Vafaei et al presents, a blind watermarking method based on neural networks in discrete wavelet transform domain. Robustness and imperceptibility are main contradictory requirements of a watermark. In the proposed method, better compromises are achieved using artificial neural networks to adjust the watermark strength. A binary image is used as the watermark and embedded repetitively into the selected wavelet coefficients, which also improves the watermark robustness. Experimental results demonstrate that the proposed scheme has a simultaneous good imperceptibility and high robustness against several types of attacks, such as Gaussian and salt and pepper noise addition, cropping, mean and median filtering and JPEG compression.

In 2014 Hieu V. Dang et al deals with the problem of robust and perceptual logo watermarking for color images. In particular, they investigated trade-off factors in designing efficient watermarking techniques to maximize the quality of watermarked images and the robustness of watermark. With the fixed size of a logo watermark, there is a conflict between these two objectives, thus a multi objective optimization problem is introduced. They proposed to use a hybrid between general regression neural networks (GRNNs) and multi objective memetic algorithms (MOMA) to solve this challenging problem. Specifically, a GRNN is used for efficient watermark embedding and extraction in the wavelet domain. Optimal watermark embedding factors and the smooth parameter of the

GRNN are searched by a MOMA for optimally embedding watermark bits into wavelet coefficients. The experimental results show that the proposed approach achieves robustness and imperceptibility in watermarking.

The GRNN, proposed by Specht, is a special network in the category of probabilistic neural networks (PNN). GRNN is a one-pass learning algorithm with a highly parallel structure. Different from other probabilistic neural networks, GRNNs provide estimates of continuous variables and converges to the underlying (linear or nonlinear) regression surface. This makes GRNN a powerful tool to do predictions, approximation, and comparisons of large data sets. It also allows having fast training and simple implementation. GRNN is successfully applied for image quality assessment, function approximation, and web-site analysis and categorization. For that, watermarking for color images is formulated as a multi objective optimization problem of finding the watermarking parameters to maximize the quality of watermarked image and the robustness of the watermark under different attacks. A novel intelligent and robust watermarking method based on the general regression neural networks and multi objective memetic algorithms is proposed to solve this challenging problem. Specifically, the embedding factors and the smooth parameter of the GRNN are searched optimally by the multi objective memetic optimization to maximize the PSNR and the averaged WARs objectives. The proposed algorithm obtains better results in transparency and robustness against classes of additive noise, and signal processing attacks than previous approaches.

However, the proposed algorithm has its own disadvantages and needs further improvements. For example, since it needs a sufficient time for the evolutionary and local refining searches to find the best local and global solutions, it is not fast enough for the real-time applications at this stage.

Over the years, researchers have been designing watermarking techniques with robustness in mind, in order for the watermark to be resistant against any image processing technique, although a necessary condition for the robust watermarking technique still remains with the quality of the technique itself (Matt and Jeffrey 1999). Furthermore, the requirement of a good watermarking technique includes a tradeoff between robustness, image quality (imperceptibility) and capacity. It has been found that when the robustness of the watermarking method improves, the imperceptibility decreases, and the capacity increases (Rahman et al. 2011; Yalman and Erturk 2013; Ji et al. 2013; Akar et al. 2013; Duda et al. 2001).

Different parameters are used to assess the robustness of watermarking, namely bit correct ratio (BCR) (Maity and Kundu 2002; Hua et al. 2016), or the bit error ratio (BER) (Parameswaran and Anbumani 2006; Zhang et al. 1998). In some cases, similarity was used to draw some conclusion (Bishop 2006), whereas the probability approach is also considered as a robustness measure. Robustness measures through these methods give almost the same result. Consistent with this, normalized cross correlation (NCC) has been used in the current study. This famous technique is mostly used as a parameter for testing the robustness of the watermarking (Kiani and Ebrahimi 2011; Braudaway et al. 1996). The issue raised by this researcher is the extent to which these quality measures relate to determining the quality of a watermarked file after embedding and after it has undergone an attack.

The watermarking technique used involves the embedding of a watermark in intermediate significant bits (ISB) (Hal 1997). There are several types of NN, including the recurrent,

generalized regression. Multi-layer perceptron NN (MLPNN) is the most widely used NN for prediction (Yeung and Mintzer 1997), and it performs better than other NNs in terms of its accuracy in recognizing patterns (Bender et al. 1996); therefore the study has chosen to use it. The neural network model used the image quality metric (PSNR and NCC) values obtained from the watermarking of six grey-scale images that used ISB as the desired output and trained the network to predict future values when some output of the same or different type of image quality metrics (PSNR and NCC) were obtained.

## V. ROBUSTNESS OF THE WATERMARKING TECHNIQUES

Many image watermarking algorithms (Akram Zeki et al. 2016) have been presented by various researchers with the aim of preventing the ownership of the image and for copyright protection. Digital watermarking in general is a special case of the general information-hiding problem (Wojtowicz and Ogiela 2016). A digital watermark is a signal that is temporarily or permanently embedded into digital data (audio, images, videos and text), which can be detected or extracted later by means of a computing operation, to make an assertion about the ownership of the data. The watermark is hidden in the host data, in such a way that it is inseparable from the data and resistant to image processing operations, and it does not degrade the host file. Thus, by means of watermarking, the real image is still accessible but is permanently marked (Caronni 1995; Liu et al. 2016).

The robustness of watermarking techniques has received a large amount of attention among researchers because it reflects good performance of certain techniques and shows how resistant to attack a technique can be. A robust watermarking technique prevents a watermark attack against geometric distortions, ensures the synchronization of the watermark before and after embedding, and ensures watermark resilience to common image processing attacks as well as desynchronization attacks (Huo-Chong et al. 2011; Mardanpour and Chahooki 2016). Robust watermarking ensures self-synchronizing schemes, which will certainly permit the recovery of the watermark after geometrical attacks (Li et al. 2006). A robust watermarking technique can ensure the mapping of original watermark image features with the watermarked image features to be resilient against the image processing, such as affine transformations (Hong-ying et al. 2013; Liu et al. 2006).

Although there are other watermarking techniques that are not robust, which are affected by many attacks, the intention might clearly be that any attempt to make an alteration should damage the image. In that case, the technique serves its purpose. Any watermarking technique with robustness in mind should tend to be resistant against image processing operations, utilizing any concept that is necessary. For example, a mathematical remainder operation might be used to build a robust watermarking technique that will modify the low-frequency coefficients in the DCT frequency domain (Rafi et al. 2013).

The robustness of watermarking techniques is essential in hardware-based watermarking techniques. The correlation of the original watermark image and the watermarked image makes it capable of detecting the inserted bits (Hartung and Kutter 1999; Jiao et al. 2015). For this reason, it can be implemented in a hardware-oriented image coding processing scheme (Kougianos et al. 2009), while using any transformation technique. At the same time, the relationship

between the capacity and the bit error rate will maintain at a lower level (Juergen 2005; Abbasi et al. 2015).

Various transforms as well as their hybrids have been used for getting better robustness than each other comparatively. Here SVD has been used along with error control and back propagation neural networks to enhance the performance at the cost of algorithmic complexity.

The singular value decomposition (SVD) technique is a generalization of the Eigen value decomposition used to analyze rectangular matrices. This mathematical technique has been used in various fields of image processing. The main idea of the SVD is to decompose a rectangular matrix into three simple matrices. It has been widely studied and used for watermarking by researchers for long.

SVD is used to hide the logo for watermarking in its Eigen values. To improve the robustness error control coding scheme the next important technique employed is the back propagation algorithm based neural network. This is because among different learning algorithms, back propagation algorithm is widely used learning algorithm in artificial neural networks. The feed forward neural network architecture is capable of approximating most problems with high accuracy and generalization ability. This algorithm is based on the error correction learning rule. Error propagation consists of two passes through the different layers of the network, a forward pass and a backward pass. In the forward pass the input vector is applied to the sensory nodes of the network and its effect propagates through the network layer by layer. Finally a set of outputs is produced as the actual response of the network.

During the forward pass the synaptic weight of the networks are all fixed. During the back pass the synaptic weights are all adjusted in accordance with an error correction rule. The actual response of the network is subtracted from the desired response to produce an error signal. This error signal is then propagated backward through the network against the direction of synaptic conditions. The synaptic weights are adjusted to make the actual response of the network move closer to the desired response.

## VI. RESEARCH GAP IDENTIFIED

In the field of digital watermarking, digital image watermarking for copyright protection has attracted a lot of attention in the research community. Digital watermarking contains various techniques for protecting the digital content.

As we have already seen in the previous sections of this paper, the previous approaches of digital water marking. According to those researches we got lots of research gaps.

On the basis of the extensive literature review we have done, it can be stated that the main issue with the image watermarking and watermarking schemes which used to make the watermarked object robust to attacks while maintaining the imperceptibility. Basically there are mainly three challenges being faced by the currently available Watermarking schemes and those challenges are: 1) Time Complexity 2) Quality Complexity 3) Watermarking Standards. Some additional issues are identified which are as follows:

- In existing methods the watermarked image is almost the same as the original cover image. Most of the attacks would degrade the quality of the extracted watermark image. A robust watermarking technique should prevent a watermark attack against geometric distortions, ensure the synchronization of the watermark before and after embedding, and ensure

watermark resilience to common image processing attacks as well as desynchronization attacks.

- The existing methods have been able to achieve good visual quality of the signed and attacked images and high normalized correlation value indicates good robustness of the embedding scheme. However, the existing methods do not compute any processing time spans consumed by their algorithm. The existing methods need a sufficient time for the evolutionary and local refining searches to find the best local and global solutions, it is not fast enough for the real-time applications at this stage.
- Embedding watermark on a single coefficient may not sustain robustness against attacks but group of coefficients when used for data embedding has higher probability to show robustness. Also, improvement on these watermarking schemes is required to carry variable payloads for adjustability requirement with imposed security.
- In most of the research papers, once the watermarking scheme is finalized, it is applied to all test images. Since each image is different and has certain characteristics and after embedding the watermark data by a particular watermarking scheme, its performance against a particular attack may not be similar with other image. No study is conducted to make the embedding scheme based on some image characteristics. Thus, the issue is to explore the relationship between the performance of watermarking scheme and the cover image characteristics itself.

## VII. CONCLUSION

From the literature review, it is clear that research in the area of image watermarking is strongly motivated due to an increasing need from the copyright owners to reliably protect their rights. Because of large economic stake, heavy usage of images in social media domain requires ample research opportunities as well as a great future. New applications are likely to emerge and may combine existing approaches. As a conclusion, spatial domain methods are simple and fast, but are not robust against attacks. In comparison, transform domain watermarking techniques with fusion on other techniques like neural network are more robust. Many more investigations and novel algorithms are required to improve the process of image watermarking.

## REFERENCES

- [1] P.Tao, and A.M.Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol.5601, pp.133-144, 2004.
- [2] Y.Luo, L.Z.Cheng, B.Chen, and Y.Wu, "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp.1096-1103, 2005.
- [3] S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection for watermarking," IEEE Transactions on Image Process, pp. 154-165, 2002
- [4] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," IEEE Trans. on Image Process, vol.11, pp. 77 88, 2002.
- [5] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques." In Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on, pp. 709-716. IEEE, 2005.

- [6] C-S. Lu, H-Y. Liao, H-Y., M. Huang and S-K. Sze Combined Watermarking for Images Authentication and Protection, Proc. 1st IEEE Int'l Conf. on Multimedia and Expo 3:30 (2000) pp. 1415-1418.
- [7] C-S. Lu, S-K. Huang, C-J. Sze and H-Y. Liao A new watermarking technique for multimedia protection, *Multimedia Image and Video Processing* (2001) pp. 507-530.
- [8] ZHU Chang-qing, YANG Cheng-song, LI Zhong-yuan. An Anti-compression Watermarking Algorithm for Vector Map Data. *Journal of Zhengzhou Institute of Surveying and Mapping*, 2006, 23(4):281-283.
- [9] N. Kaewkamnerd and K.R. Rao Multiresolution based image adaptive watermarking scheme EUSIPCO online at [www.ee.uta.edu/dip/paper/EUSIPCO\\_water.pdf](http://www.ee.uta.edu/dip/paper/EUSIPCO_water.pdf) (2000).
- [10] Chen Yongqinang, Zhang Yanqing, and Peng Lihua, "A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural Network", *Academy Publisher*, pp. 298-301, 2009.
- [11] heng-Ri Piao, Seunghwa Beack, Dong-Min Woo, and Seung-Soo Han, "A Blind Watermarking algorithm Based on HVS and RBF Neural Network for Digital Image", *Springer-Verlag Berlin Heidelberg*, pp. 493-496, 2006.
- [12] M.S. Raval and P.P. Rege, Discrete wavelet transform based multiple watermarking scheme, *Conference on Convergent Technologies for Asia-Pac Region (TENCON'03) 3* (2003) pp.935-938.
- [13] Y. Zhao, P. Campisi and D. Kundur, Dual domain watermarking for authentication and compression of cultural heritage images *Proc. IEEE Transactions on Image Processing* 13:3 (2004) pp. 430-448.
- [14] M Voigt , Bian Yang , Christoph Busch. Reversible Watermarking of 2D-vector Data. *Proceedings of the 2004 ACM International Workshop on Multimedia and security*, Magdeburg, Germany, Aug., 2004:160-165.
- [15] Deng, N., Jiang, C.S., 'CDMA watermarking algorithm based on wavelet basis'. *Proc. 9th Int. Con. Fuzzy Systems and Knowledge Discovery*, May 2012, pp. 2148– 2152.
- [16] A.B. Watson, DCT Quantization Matrices Visually Optimized for Individual Images, *Proc. Human Vision, Visual Processing, and Digital Display IV* (1992) pp. 202-216.
- [17] S. Bounkong, B. Toch, David Saad, David Lowe, "ICA for Watermarking Digital Images", *Journal of Machine Learning Research* 4 (2003) 1471-1498.
- [18] X.Y. Huang, M.S. Tan, Y. Luo and D.Z. Lin, An image digital watermarking based on DCT in invariant wavelet domain, *IEEE 1st Int'l Conf. on Wavelet Analysis and Pattern Recognition* (2007) pp. 458-463.
- [19] J. Wang, S. Lian, Z. Liu, Z. Ren, Y. Dai and H. Wang, Image Watermarking Scheme Based on 3-D DCT, *Proc. 1st IEEE Int'l Conf. on Industrial Electronics and Applications* (2006) pp. 1-6.
- [20] X. Li and X. Xue, Improved robust watermarking in DCT domain for color images, *Proc. IEEE 1st Int'l Conf. on Advanced Information Networking and Applications (IEEE-AINA'04)* (2004) pp. 53-58.
- [21] Chin-Shiuh S. et al. Genetic watermarking based on transform domain techniques. *Pattern Recognition*. 2004. 37. 555–565p.
- [22] Quan, L.; Jiang, X.: Design and Realization of a Meaningful Digital Watermarking Algorithm Based on RBF Neural Network. *Proceedings of the Sixth World Congress on Intelligent Control and Automation, WCICA*. vol. 1, pp. 2878-2881, 2006.
- [23] Ren Shuai, Lei Jingxiang, Zhang Tao, Duan Zongtao Fast Watermarking of Traffic Images Secure Transmission in Effective Representation Mode, *J. Appl. Math* 8, 2565-2569, (2014).
- [24] Mohamad Vafaei, and Homayoun Mahdavi-Nasab, "A Novel Digital Watermarking Scheme Using Neural Networks with Tamper Detection Capability", *J. Basic. Appl. Sci. Res.*, 3(4)577-587, 2013.
- [25] Hieu V. Dang and Witold Kinsner, "An intelligent digital color image watermarking approach based on wavelet transform and general regression neural network," in *Proc. of the 11th IEEE Intern. Conf. on Cognitive Informatics and Cognitive Computing, ICCI\*CC 2012*, (Kyoto, Japan; August 22-24, 2012), pp. 115-123, 2012.
- [26] Matt ML, Jeffrey AB (1999) Computing the probability of false watermark detection. In: *Third international workshop on information hiding*, Dresden, Germany
- [27] Rahman Z, Jobson DJ, Woodell GA (2011) Investigating the relationship between image enhancement and image compression in the context of the multi-scale retinex. *J Vis Commun Image Represent* 22:237–250.
- [28] Yalman Y, Erturk I (2013) A new color image quality measure based on YUV transformation and PSNR for human vision system. *Turk J Electr Eng Comput Sci* 21(2):603–612.
- [29] Ji F, Deng C, An L, Huang D (2013) Desynchronization attacks resilient image watermarking scheme based on global restoration and local embedding. *Neurocomputing* 106:42–50.
- [30] Akar F, Yalman Y, Varol HS (2013) Data hiding in digital images using a partial optimization technique based on classical LSB method. *Turk J Electr Eng Comput Sci* 21(Sup. 1):2037–2047.
- [31] Duda RO, Hart PE, Stork DG (2001) *Pattern classification*, 2nd edn. Wiley, New York
- [32] Maity SP, Kundu MK (2002) Robust and blind spatial watermarking in digital image. In: *Proceedings of 3rd Indian conference on computer vision, graphics and image processing (ICVGIP '2002)*. 16–18th December 2002. Ahmedabad, India, pp 388–393.
- [33] Hua G, Huang J, Shi YQ, Goh J, Thing VL (2016) Twenty years of digital audio watermarking—a comprehensive review. *Sig Process* 128:222–242.
- [34] Parameswaran L, Anbumani K (2006) A robust image watermarking scheme using image moment normalization. In: *Transactions on engineering, computing and technology*. May 13, pp 1305–5313.
- [35] Zhang G, Patuwo BE, Hu MY (1998) Forecasting with artificial neural networks: the state of the art. *Int J Forecast* 14:35–62.
- [36] Kiani S, Ebrahimi MM (2011) A multi-purpose digital image watermarking using fractal block coding. *J Syst Softw* 84:1550–1562.
- [37] Bender W, Gruhl D, Morimoto N, Lu A (1996) Techniques for data hiding. *IBM Syst J* 35:313–336.
- [38] Wójtowicz W, Ogiela MR (2016) Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. *J Vis Commun Image Represent* 38:1–10.
- [39] Akram Zeki, Adamu Abubakar and Haruna Chiroma, "An intermediate significant bit (ISB) watermarking technique using neural networks", *SpringerPlus* (2016) 5:868 DOI 10.1186/s40064-016-2371-6.
- [40] Caronni G (1995) Assuring ownership rights for digital images. In: *Proceedings of reliable IT systems (VIS 95)*. June. Germany, 1995.
- [41] Liu H, Xiao D, Zhang R, Zhang Y, Bai S (2016) Robust and hierarchical watermarking of encrypted images based on compressive sensing. *Sig Process Image Commun* 45:41–51
- [42] Huo-Chong L, Raphael C, Phan W, Swee-Huay H (2011) On an optimal robust digital image watermarking based on SVD using differential evolution algorithm. *Opt Commun* 284:4458–4459.
- [43] Mardanpour M, Chahooki MAZ (2016) Robust transparent image watermarking with Shearlet transform and bidiagonal singular value decomposition. *AEU Int J Electron Commun* 70(6):790–798
- [44] Rafi U, Asifullah K, Aamir SM (2013) Dual-purpose semi-fragile watermark: authentication and recovery of digital images. *Comput Electr Eng* 39(7):2019–2030.