# A Review on Data Hiding Based on Digital Watermarking Technique for Improving Secure data communication

By

***Aliu, D., E. A. Adedokun, M. B. Mu'azu, I. J. Umoh***
Department of Computer Engineering,
Ahmadu Bello University,
Zaria, Nigerian
Email: danfranali12@yahoo.com

**ABSTRACT**

*In recent years, the use of multimedia contents (image, audio, video and text) is rapidly increasing with the high growth and widespread use of the Internet and information technology. Due to this fact, tampering and illegal distribution of digital contents is inevitable because of their digital nature and as such it becomes imperative to devise mechanisms to protect such contents. Several mechanisms that have been proposed for data hiding are cryptography, steganography and watermarking. One of such mechanisms that have been attracting major interest is digital watermarking as it provides one of the best solutions among the proposed mechanisms. This is because watermarking has given an effective ways of data copyright protection or illegal duplication of digital data. Watermarking is a technique that is used to preclude duplicating or to shield digital data by imperceptibly hiding authorized sign information into the original data. The major challenge of watermarking technique is to optimally achieve a balance between imperceptibility and robustness. In order to attain this fit many researchers have proposed and developed different algorithms to this regards. This paper survey various watermarking algorithm for protection of digital data with a view to achieving optimal trade-off between imperceptibility and robustness. Performance and limitations some of the previous works are identified. Finally, future investigations to improve on some of the observed inadequacies are discussed.*

**Key** words: Watermarking, Steganography, Cryptography, Watermarking Embedding, Watermarking Extraction and Watermarking Scheme

## INTRODUCTION

The rising demand for the production, storage and transmission of multimedia contents (such as image, audio, video and text) over secured and unsecured communication media in recent years poses a lot of security and privacy concerns to both the sender and recipient. The use of these multimedia contents (image, audio, video and text) is rapidly increasing with the high growth and widespread use of the Internet and information technology. Due to this fact, tampering with and illegal distribution of digital contents is inevitable and as such it becomes imperative to devise mechanisms to protect the copyright of such media. It has been established that present copyright laws are insufficient for addressing the security of digital contents (Chandramouli *et al.,* 2002). Furthermore, simple transfer and manipulation of digital data also

institutes a real menace for information inventors, and copyright owners want to be recompensated every period their work is used. In addition, they want to be certain that their work is not deployed in an illegitimate means (for instance modified without their consent). The introduction of Internet has ensued in numerous chances for the creation and transfer of contents (electronic advertising, web publishing, digital repositories and libraries, real-time video and audio delivery, etc.) in digital form (Chandramouli *et al.,* 2002). A pertinent issue that arises in these applications is the protection of the rights of all participants, such as copyright enforcement and content verification because the present copyright acts are insufficient in transacting digital messages (Chandramouli *et al.,* 2002). One solution to this threat would be to curb access to the data based on encryption technique (Arnold *et al.,* 2003), even though it does not necessarily offer total protection. Once the encoded data are decoded, they can be easily circulated or manipulated (Arnold *et al.,* 2003). This has led to the fascination of researchers in developing copy deterrence and protection mechanisms (Kavitha & Shan, 2016). Several mechanisms have been proposed for the protection of multimedia contents based on data hiding techniques. These techniques are as follows (Harish *et al.,* 2013):

i. Cryptography,
ii. Steganography
iii. Watermarking

A comprehensive review of the development of data hiding can be found in (Tanaka, Nakamura & Matsui, 1990).

Cryptography is not particularly focused on concealing the presence of data, but is also regarded as encryption (Challita & Farhat, 2011). Cryptography can be defined as the study of mathematical systems for solving two types of challenges, privacy and authentication (Diffie & Hellman, 1976). A privacy scheme precludes the extraction of information by unauthorized parties from data transferred over public channel, hence ensuring the sent message is being read only by the designated receiver (Diffie & Hellman, 1976). An authentication scheme forestall an unauthorized injection of messages into public channel, ascertaining the receiver of a message of the legitimacy of its sender (Diffie & Hellman, 1976). Steganography means the study of techniques for concealing the existence of a secondary message in the presence of a primary message (Arnold *et al.,* 2003), that is, by inserting a private message in a cover image (Challita & Farhat, 2011). Where the carrier signal depicts the primary message and the secondary message is the payload signal or payload message. Steganography is a mechanism that is used for offering confidentiality and deniability, both of which can be satisfied exclusively through cryptographic ways (Arnold *et al.,* 2003). In steganography, messages which are secreted has no connection with the cover channel or image and the condition for steganography is that no intuition should arise that a channel is conveying any concealed data (Challita & Farhat, 2011). The aim of steganography is to have a covert communication between two parties, that is, presence of the communication is unknown to a potential assailant, and only a fruitful attack can notice the existence of this conversation. One of such mechanisms that have been attracting major interest is digital watermarking (Averkiou, 2002). Watermarking has provides one of the best solutions among the proposed mechanisms (Harish *et al.,* 2013). Watermarking have shown resilient that overcome covert communication as in steganography (Harish *et al.,* 2013).

The interest in watermarking actually started in 1990 with the development of the multimedia systems and the necessity of transferring data over the internet (Araghi *et al.,* 2016). Digital watermarking is a technique that is used to preclude duplicating or to shield digital data by invisibly hiding lawful mark message into the original data (Lai *et al.,* 2013). Digital watermarking can also be defined as the act of concealing information connected to a digital signal (which could be a video, song and image) inside the signal itself (Bajracharya & Koju, 2017). Watermarking attempts to hide a message interrelated to the actual content of the digital signal (Bajracharya & Koju, 2017). Such information is embedded for various reasons such as (Nin & Ricciardi, 2013): Copyright protection, Source tracking, broadcast monitoring, Telemedicine and Piracy deterrence etc. Watermark systems have a number of characteristics (Mehto & Mehra, 2015), however, it is the requirements of a particular watermarking system that decides the comparative importance of each characteristic (Chahal & Khurana, 2013). Different applications need different properties of watermarking. Before designing any watermarking system the attributes described in the following terms need to be taken into consideration (Tao *et al.,* 2014). Imperceptibility, capacity, robustness, security, computational complexity and verifiability. The categorization of watermarking scheme into four phases is based on the kind of information to be watermarked; this information can be any of (Sinha *et al.*, 2014): Video watermarking, Image watermarking, Text watermarking and Audio watermarking. A model of bits infixed into a digital audio, video, image, or text file that is unambiguously use to identifies the owner of a specific image is refer to as watermark and its main steps are embedding and extraction (Cherian & Mereena, 2016; Nyeem *et al.,* 2014).

1. Embedding Processing: Embedding is a method of inserting a watermark within the host image in order to create the watermarked image and the process is carried out at the sender's side (Navas *et al.,* 2008)

A typical watermark embedding is represented as follows (Chandramouli *et al.,* 2002):

$$X' = E_k(X, W) \quad (1)$$

where: *X* is the original image, *W* is the watermark information being embedded, k is the user's insertion key, *E* represents the watermark insertion function, X' depicts the watermark variant

2. Extracting Processing: Extracting is the method of recovering the watermark and the host image from the watermarked image and this process happened at the receiver's end

A generic watermark extraction is represented as follows (Chandramouli *et al.,* 2002):

$$\tilde{W} = D_{K'}(\tilde{X}') \quad (2)$$

Where: $\tilde{X}'$ represents the possible corrupted watermarked image, $K'$ denotes the extraction key, *D* depicts the watermark extraction /detection function, $\tilde{W}$ represents the extracted watermark information. The two processes are shown in Figures 1 and 2 respectively.

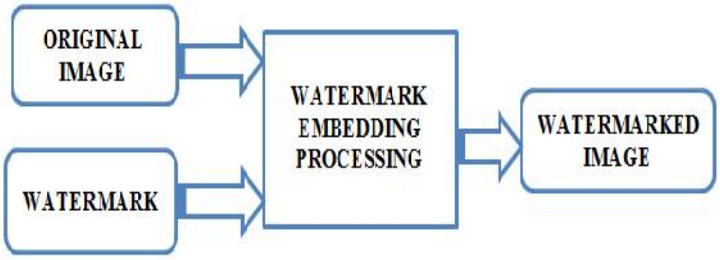



Figure 1: Watermark Embedding Process (Chanda & Choudhury, 2016)

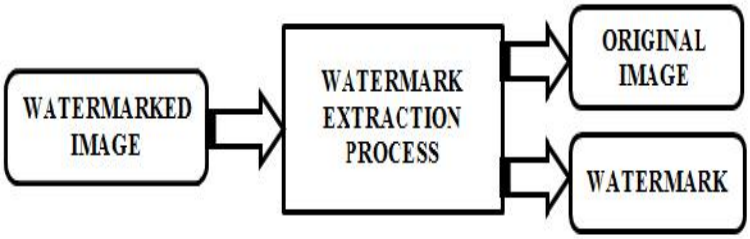
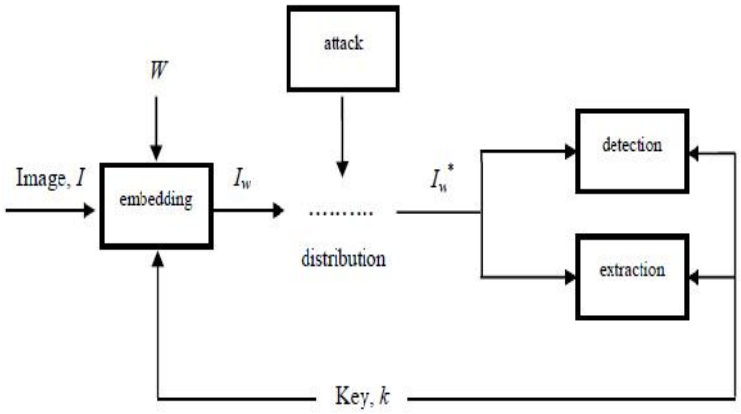



Figure 2: Watermark Extraction Process (Chahal & Khurana, 2013)

Figure 3 depicts the complete representation of the components of a watermarking process which comprises of embedding, detection and extraction




processes.

Figure 3: Watermarking System (Tao & Eskicioglu, 2004)

Where: $I$ depicts the host image, $W$ Denotes the watermark image, $I_W$ represents the watermarked image, $I_W^*$ *represents* the distorted image, $K$ depicts embedding and extraction key.

The two key groups of digital image watermarking are as follows (Sathik & Sujatha, 2012): Visible digital image watermarking technique and Invisible digital image watermarking technique. Information is perceptible in the multimedia content which identifies the owner of the document in detectible watermarking. The visible watermarking should be perceptible (easy to discern the concealed data) (Santhi & Arulmozhivarman, 2013). In undetectable watermarking information is summed as digital data to multimedia content, such that, it is imperceptible to observers. The invisible watermarking requirements are imperceptibility and robustness. The invisible watermarks are categorized as follows (Chandramouli *et al.,* 2002): Fragile watermarks, Semi fragile watermarks and robust watermarks.

Several techniques have been proposed for copyright protection of digital images and these are categorized into two domains as follows (Sathik & Sujatha, 2012): Spatial domain techniques and Transform domain techniques. In spatial domain techniques the pixel values of the host image are changed directly by inserting the watermark bits (Araghi *et al.,* 2016). These techniques are simply implemented with little cost of operation, quick, computationally uncomplicated and straightforward while there is no need for cover image to be transformed. Nevertheless, they are vulnerable to simple image processing operations such as noise, compression and filtering due to watermark insertion in selected locations of the image or other geometric attacks. The spatial domain techniques comprise of the following (Lai & Tsai, 2010; Zheng, Liu, Zhao, & Saddik, 2007): Least significant bit (LSB), Spread spectrum technique (SSM) and Correlation based technique (CBT).

The transform domain techniques comprise of the following (Rahman, 2013 and Cherian & Mereena, 2016): Discrete Orthonormal Stockwell Transform (DOST), Singular Value Decomposition (SVD), Lifting Wavelet Transform (LWT), Discrete Stockwell Transform (DST), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) and Fast Fourier Transform (FFT). The information concealing and recovery operations of these transform algorithms are comparatively complicated, however, due to their strong anti-attack abilities, they are suitable for the copyright protection of multimedia data (Araghi *et al.,* 2016). These methods in handling image and common signal processing attacks achieve higher imperceptibility and robustness, although, the cost of computation is higher than that of the spatial domain watermarking schemes (Cherian & Mereena, 2016). The conditions of robustness, imperceptibility and capacity are conflicted and limited by each other. One may want to increase the watermarking strength in order to increase the robustness but this can result in a more perceptible watermark (Tao *et al.,* 2014). Consequently, one can decrease the capacity by decreasing the number of samples allocated to each hidden bit but this is counterpoised by a loss of robustness. In other words, for any watermarking scheme, it is impossible to meet these three requirements simultaneously (Tao *et al.,* 2014). In order to ascertain a direction to address this challenge in watermarking technique, a review of related works is carried out.

## *REVIEW OF RELATED WORKS*

Several researches have been undertaken in the area of watermarking and mechanisms to improve its imperceptibility, payload, security and robustness and some of the more relevant ones are presented:

Shieh *et al.* (2004) developed an innovative robust watermarking technique using DCT based on genetic algorithm (GA). In this work, the GA was used to optimally select the frequency bands for embedding watermark into DCT based watermarking system. The algorithm was tested on Lena image as cover image of size 512 x 512 and rose of size 128 x128 as the watermark. The performance of the algorithm was measured using PSNR and normalized correlation NC to simultaneously evaluate imperceptibility and robustness. However, the proposed algorithm was susceptible to geometric attacks such as rotation and histogram equalization to fully establish the strength of its robustness.

Tao & Eskicioglu (2004) implemented a generation algorithm by inserting visual secret messages in all four sub-bands at two different decomposition levels of DWT. The first level decomposition of the algorithm was examined on a gray scale goldhill (cover image) of size 512 x 512 and binary visual messages BC and A of size 256 x 256. The second level of decomposition was tested on same size of cover image in first level of decomposition and binary visual watermarks BC and A of size 128 x 128. The algorithm was tested against fifteen different attacks. It was shown that the watermark embedded in low frequencies was resilience to attacks which includes JPEG compression, blurring, inclusion of Gaussians noise and rescaling, while those embedded in high frequencies were robust to attacks such as gamma correction, intensity adjustment and histogram equalization. It was established that watermark embedded in at least two sub-bands at a certain DWT decomposition level made the algorithm tremendously withstand to most of the malicious attempts or normal A/V processing. However, the scale factor was manually determined for each sub-band, which affected the embedding speed of the algorithm.

Navas *et al.* (2008) developed a non-blind transform domain watermarking based DWT-DCT-SVD. In this approach, DWT was used to decompose a gray scale (cover image) into four sub-bands, LL, HL, LH and HH. The DCT is employed to the selected coefficients obtained from DWT operation (LL and HH were selected). SVD was used to modified the DCT coefficients obtained from it applications. The watermark also undergoes the same processes that were used to process the cover image. The watermark was inserted in the host image by the addition of both the modified cover image and watermark together. Inverse DCT was performed follow by inverse DWT to obtain the watermarked image. The algorithm was tested on a gray scale cover image (Cameraman) of size 256 X256 and watermark (Lena) of size 128 X 128. The evaluation of the algorithm was examined using PSNR and MSE. It was founded that the algorithm was resistance against attacks such as average filtering, Gaussian blur and JPEG compression. However, the performance of the algorithm degraded when applied on colour images and digital imaging and communications in medicine DICOM images.

Al-Mansoori & Kunhu (2012), developed a robust image watermarking algorithm for inserting logo information into all DubaiSat-1 satellite images based on DCT. The odd and even technique was used to embed the watermark into the decomposed 2-D DCT coefficients of the cover image. The proposed algorithm comprises of three modules; for the first module, two bits of binary watermark logo are embedded inside the block based image with a secret key, while for the second module, two copies of two bits of binary watermark logo are embedded inside the block based image with a secret key and for the third module, three copies of two bits of binary watermark logo are embedded inside the block based image with a secret key. The performances of the three modules of the algorithm were evaluated based on their PSNR values using the following attacks: flipping, noise, resize and rotations. However, the performance evaluation of the algorithm when subjected to rotation, resize, translation and cropping attacks decreased in performance.

Anitha & Velusamy (2012), developed an efficient technique for digitizing the authoritative documents of an individual based on secret key biometric watermarking. Biometric watermark for five different persons were generated from their iris and a total of 25 documents that belonged to these five people were selected. Each biometric watermark was embedded in all the 25

documents, that is, a person's biometric watermark was embedded in the person's documents. The embedding and extracting process were done with the aid of a secret key generated from cryptographic hash function. It was found that the technique showed accuracy in authenticating the genuine documents and was resistant against signal processing attacks. However, the performance analysis of the technique was evaluated under geometric attacks in order to ascertain the reliability of the model, which was discovered to be susceptible to geometric attacks.

Kashyap & Sinha (2012), Implemented 2-level 2-D DWT based digital mage watermarking technique, whereby alpha blending technique was applied to insert the watermark in the original image. A gray scale (original image) was decomposed using the second level 2-D DWT to obtain second level (low and high frequency) sub-bands. Watermark image was also decomposed using 2-level 2-D DWT to obtain 2-level (low and high frequency) sub-bands. The decomposed 2-level low-low (LL) frequency constituents of the host image and that of watermark image are manifold by scaling factors and then added using alpha blending formula. The watermarked image was created by performing inverse second level 2-D DWT. The performance of the algorithm was tested using gray scale images (Lena image) as original image and (cameraman) as the watermark. The images are of equal size of 256 x 256. The values of MSE and PSNR were calculated for different values of the scaling factors. Investigational results showed that the quality of the processed image was dependent on the scaling factors. However, robustness of the technique was trade-off for imperceptibility against intentional and unintentional attacks. This was due to the fact that the scaling factor was manually selected.

Kejgir & Kokare (2012) developed a robust digital image watermarking method based on lifting wavelet transform (LWT) and SVD. The LWT transformed the image into sub-bands with energy greater than a given threshold is selected for watermark embedding. The SVD is applied on the selected sub-band, where the selected sub-band is decomposed into three matrices and used to insert the watermark. The proposed algorithm was tested on five different host images (pepper, rose, Mandrill) of size 512 x 512 and cameraman of size 256 x 256 and watermark of digital signature of size 256 x 256. The technique was examined for robustness against eight different attacks on each of the five images. The performance of the algorithm was evaluated using PSNR and CRC to show the simultaneous improvement of watermarked image quality and robustness respectively. The algorithm outperformed DWT and SVD when compared in terms of robustness and speed in real life applications. Nevertheless, the imperceptibility of the watermarked image which plays a vital role in digital watermarking was sacrifice for robustness.

Singh *et al.*, (2012), developed a DWT based digital image watermarking algorithm. A 4-level 2-D DWT was used to decompose cover image and the watermarks bits are then embedded into the mid frequencies of the decomposed cover image by modifying the coefficients in the block according to the embedding process. Inverse 4-level 2-D DWT was performed to obtain the watermarked image. The algorithm was examined on four different images (baboon, satellite, Lena and medical) as cover images and binary image as watermark information. The performance of the algorithm was measured using PSNR. The PSNR values were computed at different scaling factors and as the scaling factor value is increased, the PSNR value of the image decreased. However, evaluation of robustness of the proposed algorithm was vulnerable to poisson noise, filtering and JPEG compression attacks.

Lai *et al.* (2013), developed a robust feature-based image watermarking technique which hybridized DWT and SVD using PSO. The edge image information was utilized to embed the watermark. The PSO was used to optimally select a suitable scaling factor which was used to ascertain the robustness of the watermark. The watermarked image was obtained by applying inverse DWT. The technique was tested on the image of a boat of size 512 x 512 as cover image and a gray scale image (cameraman) of size 128 x 128 as watermark. The proposed algorithm was subjected to several attacks such as geometric attack, noise attack, denoising attack and image processing attack and the performance evaluation of the algorithm based on imperceptibility and robustness were measured using PSNR and NC respectively. However, inability to integrate the characteristics of human visual system into the algorithm caused an adverse effect on the quality of the host image after embedding.

Rahman, (2013), developed watermarking algorithm using DWT, DCT and SVD transformation, where the host image was reshuffled using zigzag series and the DWT was applied on reshuffled image, in order to split the image into four sub-bands (LL, HL, LH and HH). DCT and SVD were applied on all the high sub-bands. The watermark was enclosed by the modification of singular value of both the host image and watermark and added together. The watermarked image was created by the application of inverse DCT and DWT. The performance of the technique was evaluated based on PSNR and NCC to measure the level of imperceptibility and robustness. It was established in this work that the mid sub-bands and high sub-bands ensured high visual quality and more robustness against different kinds of attacks. However, the algorithm was susceptible to Gaussian, salt and pepper, speckle and Poisson noise and in addition; its performance was degraded when tested on colour images.

Santhi & Arulmozhivarman, (2013), developed a novel and dynamic technique for perceptible and undetectable watermarking in frequency domain based on Hadamard transform and sigmoid function. The algorithm adaptively calculated the scaling factor centered on the content of underlying cover image. In the embedding procedure, RGB cover image was converted into YUV colour space and the Hadamard transform was used to transform the luminance channel Y and the watermark image was as well transformed based on the Hadamard transform. The secret image was embedded by modulating the transformed coefficients of shelter image with that of the watermark. The robustness of the technique was measured using median filtering, JPEG compression, noise, low pass filtering, and high pass filtering, cropping, and geometric attacks. However, the technique was found not to be robust against cropping and Gaussian noise and also as the JPEG compression ratio increased, the robustness tended to decrease likewise the perceptual quality of the watermarked images.

Sharma & Swami (2013), implemented a digital image watermarking based on 3-level DWT. Alpha blending technique was used to embed a multi-bit watermark into low frequency sub-band of the host image. The technique was tested on the original image (Lena) and watermark (bird) of same size 256 x 256. The performance of the technique was evaluated using PSNR and MSE. These measures were found to be better than those obtained using first and second levels of decomposition of DWT. However, the technique was easily distorted by geometric attacks, since the watermark was inserted in low frequency of the second level of decomposition.

Ahmad *et al.* (2014), implemented image watermarking algorithm in transform domain using DWT. In this approach, both the cover and watermark images were splitted using 3-level 2-D DWT and so LL sub band of decomposed watermark image was embedded into the LL sub band of decomposed host image based on alpha blending technique. Eventually, watermarked image was obtained by performing inverse 3-levels 2-D DWT. The performance of the algorithm was evaluated using PSNR and was examined on gray scale images of fruits as cover image and pepper image as watermark image. Although, the algorithm demonstrateds a high performance in occasion of no attacks, but after subjecting it to various attacks, such as JPEG compression, adding noise and filtering attacks, the watermarked image quality was below 30 dB which is below the minimum required level.

Gattani & Warnekar, (2014), studied a new invisible digital watermarking scheme for colour images based on the merger of wavelet transform with SVD and Advanced encryption scheme (AES). In this approach, the watermark was embedded into the channels of the host image using a scaling factor lamda. This lamda was multiplied with singular matrix of watermark and added to the singular matrix of the host image. The AES was then used to encrypt the watermarked image in order to further enhance its security. The approach was tested on colour images (Lena) of size 512 X 512 as original image and watermark (Baboon) of size 256 X 256. The reliability of this approach was evaluated by PSNR and NCC. It was found that the application of SWT2 technique through SVD reduces distortion and the AES ensures the security of the image. Although, the embedding and extraction time of the watermark was very high.

Kaur & Jindal, (2014), proposed a new SVD-DWT video watermarking embedding technique. In this technique, third level DWT and SVD were applied on chosen frames and the watermark was embedded into randomly selected frames with the aid of private key to authenticate the video. The technique was tested with different variations using colour host video clips. Ten random features were selected and watermark (Penguin) of size 512 X 512 was embedded into the frames. The combined inverse DWT was performed to reconstruct the watermarked video. The robustness and quality of watermarked video were tested using different performance evaluation metrics such as SSIM, PSNR, MSE and BER. It was shown that the algorithm gave a high robustness and good quality watermarked video. Nevertheless, in this study public key was consider for embedding and extraction processes, because it has be established that secrete keys are more secure than dynamic keys. This exposes the algorithm to security treat.

Kester *et al.,* (2014), proposed a hybrid cryptographic and digital watermarking technique for securing digital images based on a generated symmetric key from the image features. In this technique, the encryption scheme made use of both digital image pixel displacement and visual cryptographic encryption schemes, in order to secured the digital images engaged in sequential embedding scheme and method used for authentication process of the image at the pixel level. The technique was examined on captured surveillance camera image. The operation of the algorithm was evaluated using NCC based on robustness and fidelity. It was reported in the work that the technique has a high robustness and good fidelity. However, the scheme has low capacity due to loss of pixel during encryption process.

Sharma & Jain, (2014), carried out a robust fusion watermarking scheme using SVD and DWT, where the watermark was embedded in the singular values of the red component of the

cover image DWT coefficients. These coefficients were combined with the green and blue components to yield the watermarked image. The technique was examined on a colour Lena image of size 512 X 512 and cameraman of size 256 X 256 as watermark. The quality of the approach was evaluated using PSNR. In the work the quality and robustness of the watermarked image was high. However, it is susceptible to the human visual system.

Singh *et al.*, (2014), proposed a new robust digital image watermarking scheme in transform domain for image authentication based on DWT, DCT and SVD. In this approach, DCT was employed over DWT to improve robustness and imperceptibility. In the insertion process, first level 2-D DWT was employed to decompose the cover image and then DCT and SVD were applied on HH sub-band of the decomposed first level 2-D DWT cover image. Arnold transformation was used to scramble the watermark and subsequently decomposed by applying 1-level 2-D DWT and SVD was applied on the HH sub band of the decomposed 1-level 2-D DWT watermark image. The orthogonal matrix was used to embed SVD of watermark into SVD of host image and inverse DCT and inverse DWT were performed respectively to obtain the watermarked image. Nevertheless, the technique is complicated and when the watermark data is embedded in high frequency components of the image, high frequency content of an image behaves like added noise and hence, noise removal algorithms such as filtering and sharpening destroys it. JPEG compression algorithms also try to reduce the image size by removing the small details which correspond to high frequency content of the image.

Venkatram, *et al.* (2014) developed RSA-DWT based medical image watermarking scheme. The watermark was encrypted with a public key generated from the RSA algorithm and the host image was decomposed up to second level of decomposition. Two scaling factors were used to insert the encrypted watermark into the host image and the private key for decryption is transmitted along with the embedded image. The watermarked image is created by applying inverse DWT. The technique was tested on a set of medical images using magnetic resonance imaging, computed tomography (MRI, CT and ultra-sound scans) as host image of standard resolution 256 x 256 and patient image of resolution 64 x 64 as watermark. PSNR and NCC were used as performance metrics. The results showed a good non-perceptible, high robustness and superior protection to normal DWT based watermarking scheme. However, the system was still vulnerable to noise when subjected to various types of geometric attacks.

Rahman & Rabbi. (2015), developed image watermarking algorithm based on hybrid of DWT and SVD with decomposition error. A host colour image is separated into three respective colour channels (RGB) and 4-level 2-D DWT was employed to decompose R band of the host image and SVD was applied to the watermark matrices and embedded into the HL sub-band of the decomposed R channel of the host image and eventually inverse 4-level 2-D DWT was performed to obtain the watermarked image. The performance of the algorithm was evaluated using RGB image of size 512 x 512 as a host image and secret matrices of size 64 x 64 as a watermark image. However, the scheme exhibited weak robustness against attacks such as rotation and Gaussian high pass filtering with PSNR values of below 30dB (which is benchmarked as a non-robust value).

Paliwal & Jain, (2015) implemented digital watermarking technique for embedding colour image using DWT with the aim of maintaining the quality of the image for which a signal is

inserted. The inverse DWT was applied on the watermark to create the watermarked image. The performance of the technique was evaluated using PSNR and MSE. However, the results showed that the technique was vulnerable to low pass filtering.

Vaidya & Mouli. (2015), developed an adaptive robust watermarking algorithm for digital images based on DWT. The technique was adaptive in the sense that Bhattacharyya distance and Kurtosis were used in the embedding factor and scaling factor calculation. In the insertion period, the watermark was embedded into the LL sub-band of the transformed second level 2-D DWT host image. The algorithm was tested on eleven different gray scale images (airplane, Barbara, girl1, girl2, house1, house2, Lena, mandrill, original frame, peppers and tree) of size 256 x 256 and cameraman image of size 64 x 64 were used as cover images and watermark image respectively. The performance evaluation of the algorithm was based on robustness and imperceptibility using PSNR and NCC by applying different kinds of signal manipulations and geometric attacks to the watermarked image during communication such as noise attacks, cropping, rotation, scaling and translation. The approach was found to be robust to these attacks but at the cost of the imperceptibility of the watermarked image.

Azeem *et al.,* (2016) developed an effective robust video watermarking technique based on DCT. The video frame was decomposed into three video channels Y, U and V. The V channel was chosen for the embedding of the watermark and the 2D DCT was applied to all blocks of each frame in the V luminance. The watermarked video frame was created by combining the modified Y, U and V components and inverse 2D DCT was performed on the watermarked video to obtain the watermark. The presentation of the algorithm was evaluated using PSNR and MSE. The results showed that the algorithm was susceptible to geometric attacks such as cropping, warping, rotation, and line and column removal.

Chanda & Choudhury (2016) implemented an image watermarking algorithm for copyright protection based on third level DWT. The watermark was inserted into the low frequency sub-band of the cover image by the use of alpha blending method. The watermarked image was obtained by performing inverse DWT. The technique was tested on host images (Lena, Sailboat, Rabindrama and Netaji) and cameraman as watermark. PSNR and RMSE were employed to evaluate the performance of the proposed technique, in terms of perceptual transparency and robustness. The results showed a high level of imperceptibility but that it was susceptible to geometric attacks since the watermark was inserted in the low frequency of the host image which made it less robust.

Malonia & Agarwal. (2016), developed a digital image watermarking algorithm in frequency domain using DWT and arithmetic progression (AP) techniques. AP was used to insert the binary watermark bits into the cover image. In the embedding period, 1-level 2-D DWT was applied to decompose RGB host image and then the secret bits were embedded into the HH, HL and LH sub-bands of the decomposed host image. The performance of the technique was examined on different host images (Lena, Baboon, Barbara) of size 512 x 512 and a quick response (QR) code image of size 48 x 48 as watermark image. It was found that by performing different signal processing manipulations and geometric attacks on watermarked images, PSNR and SSIM values (above 50dB and 0.2 respectively) were obtained. However, in this technique imperceptibility was traded-off for robustness during performance evaluation.

Salama & Mokhtar, (2016) developed an improved technique (IMD-WC-T) that combined DWT and DCT. The host image was disintegrated into four multi-resolution sub-bands that are non-overlapping up to second level of decomposition. The watermark signal was inserted into the second level sub-band of the cover image and DCT was then applied on the second level sub-band. Watermarking was then carried out in the sub-band. The technique was tested on a host image (Lena) of size 512 x 512 and a binary image of size 20 x 50 as watermark. The watermarked image was achieved by the application of inverse DCT and DWT respectively. The performance of the technique was measured based on PSNR, NC, MSE and watermark document ratio (WDR). It was established that the technique offered improved performance against separate DCT and DWT respectively in terms of fidelity and robustness. However, the technique was found to be vulnerable to rotation and scaling.

Bajracharya & Koju (2017) developed a DWT and SVD based digital watermarking using alpha blending and Arnold transformation in the colour images. The cover image was converted from RGB colour space to YCbCr colour space. DWT was applied on the chosen Y channel of the cover image, which was used to subdivide the image into low frequency and high frequency sub-bands up to the fourth level of decomposition. The high frequency sub-band was selected for embedding the watermark, that is, HH4. R channel was extracted from RGB of the watermark. Arnold transformation was used to scramble the R colour channel to improve the safety of the watermark image. DWT was applied on the scramble R channel of the watermark image, which was used to subdivide the image into low frequency and high frequency sub-bands up to the third level of decomposition. The high frequency sub-band of the watermark was selected, that is, HH3. The SVD was applied to the coefficients of DWT of both the cover image and watermark in order to modify them for embedding. Alpha blending scheme was used to embed the watermark in the cover image. The inverse DWT was performed on the modified SVD to generate the watermarked image. While in the reconstruction process the inverse DWT and anti-Arnold transformation were performed on the watermarked image to obtain the original watermark. The technique was tested on images (pepper and Lena) as cover image and Nepal Telecom logo as watermark information. The performance of the technique was measured using PSNR and NCC with a view to evaluating imperceptibility and robustness. It was found that the algorithm had accepted imperceptibility and robustness levels. Nevertheless, the capacity of the technique was very low, which implied that the cover image got distorted with increasing data.

Loukhaoukha *et al.,* (2017) showed how redundant wavelet transform (RDWT) and SVD resisted two ambiguity attacks. They performed one level RDWT to decompose the original image into four sub-bands and SVD was applied to all the sub-bands. The singular values for each sub-band were modified in order to enclose the watermark. The reverse RDWT was done on the modified singular values to obtain the watermarked image. The algorithm was tested on an original image (Lena and Pepper) of size 256 x 256; owners and attackers watermarks of cameraman were of the same size. The performance of the algorithm was evaluated on two different attacks referred to as ambiguity attack using PSNR and NC. However, it was established that the algorithm was not suitable to be used for ownership identification and authentication due to the fact that the algorithm failed when subjected to two ambiguity attacks.

Ouazzane *et al.,* (2017) explored the extended used of DOST in image watermarking by suggesting a fragile and blind medical image watermarking scheme that embedded the secret image based on dual symmetric high frequency sub-bands of the two dimensional DOST illustration of the original image. The technique was examined on 14 DICOM images of separate modalities. The secret images that were explored in this technique were bit series and the performance of the scheme was evaluated in order to measure the transparency of the misrepresentations presented to the original image by the insertion of the watermark using PSNR and RMSE. It was evaluated that the DOST watermarking obtained a good tradeoff between fidelity and payload when compared with DWT watermarking in blind insertion technique. However, it was not shown how the approach would behave when tamper localization capacity is added in order to ascertain modified areas and achieve enhanced integrity of the image.
The merits and demerits of the efficacies of various transform domain techniques employed in the development of the aforementioned algorithms measured in the review literatures are found in (Araghi *et al.,* 2016, Yan & Zhu, 2011 and Stockwell, 2007).

## FUTURE RESEARCH DIRECTIONS

In view of the aforementioned imperfections associated with the reviewed works, and the need to overcome the inefficiencies of the traditional watermarking techniques such as inability to obtain an optimal trade-off between imperceptibility, robustness and capacity and to withstand mostly geometric attacks. It is evident from the reviewed works that the major challenges in digital image copyright protection have been the effects of both geometric attacks and signal processing manipulations on watermarked images. Researchers have concentrated on the development of robust techniques to mitigate these effects. Most works have focus on enhancing the robustness and imperceptibility of the watermarking technique by using frequency domain techniques such as, DCT, DWT and SVD. And more recently DST and DOST has been introduced for image transformation. DCT, DWT and SVD have been identified to possess limited properties. Such properties are less robust to geometric attacks, blur near edges of images, false positive outcome and insufficient reveal of all the details within an image. These make them to be vulnerable to some attacks. To this end, hence, combining the transforms recompense for the downsides of each other, resulting in effective watermarking. Therefore, development of an enhanced robust digital image watermarking technique has been proposed. The proposed technique will employ the combination of DOST, DWT and SVD with a view to strengthening the watermarking technique.

## CONCLUSION

Watermarking techniques offered monumental applications in area of broadcast monitoring, copyright protection, source tracking, medical application, image and content authentication and fingerprint. However, for a watermarking to be useful its must satisfy imperceptibility and robustness requirement simultaneously. Achieving these properties is a major challenge in the field of watermarking technique. Therefore, an enhanced digital image watermarking in DOST domain using DWT and SVD with a view to mitigating signal processing

manipulation and geometric attacks in order to simultaneously satisfy both robustness and imperceptibility requirements need to been developed.

**REFERENCES**

Ahmad, A., Sinha, G., & Kashyap, N. (2014). 3-level DWT Image watermarking against frequency and geometrical attacks. *International Journal of Computer Network and Information Security, 6*(12), 58.

Al-Mansoori, S., & Kunhu, A. (2012). Robust watermarking technique based on DCT to protect the ownership of DubaiSat-1 images against attacks. *International Journal of Computer Science and Network Security (IJCSNS), 12*(6), 1.

Anitha, V., & Velusamy, R. L. (2012). Authentication of digital documents using secret key biometric watermarking. *InternationalJournal of Communication Network Security, 1*(4), 5-11.

Araghi, T. K., Manaf, A. B. A., Zamani, M., & Araghi, S. K. (2016). A survey on digital image watermarking techniques in spatial and transform domains. *Int. J. Adv. Image Process. Techn.–IJIPT, 3*(1), 6-10.

Arnold, M. K., Schmucker, M., & Wolthusen, S. D. (2003). *Techniques and applications of digital watermarking and content protection*: Artech House.

Averkiou, M. Digital Watermarking. *PDF). Source: https://www. cl. cam. ac. uk/teaching/0910, 8*, 1.

Azeem, N., Ahmad, I., Jan, S. R., Tahir, M., Ullah, F., & Khan, F. (2016). A New Robust Video Watermarking Technique Using H. 264/AAC Codec Luma Components Based On DCT. *International Journal of Advance Research and Innovative Ideas in Education, Online ISSN-2395-4396*.

Bajracharya, S., & Koju, R. (2017). An Improved DWT-SVD Based Robust Digital Image Watermarking for Color Image. *IJEM-International Journal of Engineering and Manufacturing (IJEM), 7*(1), 49.

Chahal, J. S., & Khurana, S. (2013). A Review on Digital Image Watermarking. *International Journal of Emerging Technology and Advanced Engineering, 3*(12), p482-484.

Challita, K., & Farhat, H. (2011). Combining steganography and cryptography: new directions. *International Journal of New Computer Architectures and their Applications (IJNCAA), 1*(1), 199-208.

Chanda, P. B., & Choudhury, J. P (2016). Secure Data Transmission using DWT Based Image Watermarking Scheme. *International Journal of Engineering Trends and Technology, 35*(10), p453-459.

Chandramouli, R., Memon, N., & Rabbani, M. (2002). Digital watermarking. *Encyclopedia of Imaging Science and Technology*, 1-21.

Cherian, J., & Mereena, A. T. (2016). A Survey on DWT and LWT based Digital Image Watermarking. *International Journal of Research in Computer Application and Information Technology, 4*(3), p27-32.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory, 22*(6), 644-654.

Gattani, P. V., & Warnekar, C. (2014). Security and Watermarking of Color Images. *International journal on Recent and Innovation Trends in Computing and Communication, 2*(6), 1471-1475.

Harish, N., Kumar, B., & Kusagur, A. (2013). Hybrid robust watermarking technique based on DWT, DCT and SVD. *International Journal of Advanced Electrical and Electronics Engineering, 2*(5), 137-143.

Kashyap, N., & Sinha, G. (2012). Image watermarking using 3-level discrete wavelet transform (DWT). *International Journal of Modern Education and Computer Science, 4*(3), 50.

Kaur, P., & Jindal, S. (2014). A New approach of SVD-DWT Video Watermarking Embedding Algorithm. *International Journal of Recent Advances in Engineering and Technology, 2*(5), p36-40.

Kavitha, K., & Shan, B. P. (2016). An Introduction to the Digital Watermarking. *International Journal of Advanced Engineering Research and Science, 3*(6), p 157-160.

Kejgir, S. G., & Kokare, M. (2012). Lifting wavelet transform with singular value decomposition for robust digital image watermarking. *International Journal of Computer Applications, 39*(18), 10-18.

Kester, Q.-A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., & Quaynor, N. N. (2014). A Hybrid Cryptographic and Digital Watermarking Technique for Securing Digital Images based on a Generated Symmetric Key. *International Journal of Computer Applications, 94*(19), p19-27.

Lai, C.-C., Chan, C.-F., Ouyang, C.-S., & Chiang, H.-F. (2013). *A robust feature-based image watermarking scheme.* Paper presented at the Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2013 14th ACIS International Conference on.

Lai, C.-C., & Tsai, C.-C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on instrumentation and measurement, 59*(11), 3060-3063.

Loukhaoukha, K., Refaey, A., & Zebbiche, K. (2017). Ambiguity attacks on robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *Journal of Electrical Systems and Information Technology*, p1-10.

Malonia, M., & Agarwal, S. K. (2016). *Digital Image Watermarking using Discrete Wavelet Transform and Arithmetic Progression technique.* Paper presented at the Electrical, Electronics and Computer Science (SCEECS), 2016 IEEE Students' Conference on.

Navas, K., Ajay, M. C., Lekshmi, M., Archana, T. S., & Sasikumar, M. (2008). *Dwt-dct-svd based watermarking.* Paper presented at the Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on.

Nin, J., & Ricciardi, S. (2013). *Digital watermarking techniques and security issues in the information and communication society.* Paper presented at the Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on.

Ouazzane, H., Mahersia, H., & Hamrouni, K. (2017). *How to extend the use of the discrete orthogonal stockwell transform to image watermarking.* Paper presented at the Proceedings of the Symposium on Applied Computing.

Paliwal, M., & Jain, Y. K. (2015). Digital Watermarking Algorithm for Embedding Color Image using Two Level DWT. *International Journal of Computer Applications, 116*(13).

Rahman, M. (2013). A DWT, DCT and SVD based watermarking technique to protect the image piracy. *arXiv preprint arXiv:1307.3294*.

Rahman, M. A., & Rabbi, M. F. (2015a). DWT-SVD based New Watermarking Idea in RGB Color Space. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 8*(6), 193-198.

Rahman, M. A., & Rabbi, M. F. (2015b). Non-Blind DWT-SVD based Watermarking Technique for RGB Image. *Global Journal of Research In Engineering, 15*(4), p1-5.

Salama, A. S., & Mokhtar, M. A. (2016). *Combined technique for improving digital image watermarking.* Paper presented at the Computer and Communications (ICCC), 2016 2nd IEEE International Conference on.

Santhi, V., & Arulmozhivarman, P. (2013). Hadamard transform based adaptive visible/invisible watermarking scheme for digital images. *Journal of Information Security and Applications, 18*(4), 167-179.

Sathik, M. M., & Sujatha, S. (2012). A Novel DWT Based Invisible Watermarking Technique for Digital Images. *Int. Arab J. e-Technol., 2*(3), 167-173.

Sharma, P., & Jain, T. (2014). *Robust digital watermarking for coloured images using SVD and DWT technique.* Paper presented at the Advance Computing Conference (IACC), 2014 IEEE International.

Sharma, P., & Swami, S. (2013). *Digital image watermarking using 3 level discrete wavelet transform.* Paper presented at the Conference on Advances in Communication and Control Systems.

Shieh, C.-S., Huang, H.-C., Wang, F.-H., & Pan, J.-S. (2004). Genetic watermarking based on transform-domain techniques. *Pattern recognition, 37*(3), 555-565.

Singh, A. K., Dave, M., & Mohan, A. (2012). *A novel technique for digital image watermarking in frequency domain.* Paper presented at the Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on.

Singh, B., Sharma, K. D., & Jatav, L. S. (2014). *New robust watermarking approach for image authentication.* Paper presented at the Consumer Electronics (GCCE), 2014 IEEE 3rd Global Conference on.

Singh, P., & Chadha, R. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT), 2*(9), 165-175.

Tanaka, K., Nakamura, Y., & Matsui, K. (1990). *Embedding secret information into a dithered multi-level image.* Paper presented at the Military Communications Conference, 1990. MILCOM'90, Conference Record, A New Era. 1990 IEEE.

Tao, P., & Eskicioglu, A. M. (2004). *A robust multiple watermarking scheme in the discrete wavelet transform domain.* Paper presented at the Proc. SPIE.

Vaidya, S. P., & Mouli, P. C. (2015). Adaptive digital watermarking for copyright protection of digital images in wavelet domain. *Procedia Computer Science, 58*, 233-240.

Venkatram, N., Reddy, L., Kishore, P., & Shavya, C. (2014a). RSA-DWT BASED MEDICAL IMAGE WATERMARKING FOR TELEMEDICINE APPLICATIONS. *Journal of Theoretical & Applied Information Technology, 65*(3).

Venkatram, N., Reddy, L., Kishore, P., & Shavya, C. (2014b). RSA-DWT BASED MEDICAL IMAGE WATERMARKING FOR TELEMEDICINE APPLICATIONS. *Journal of Theoretical & Applied Information Technology, 65*(3), p801-812. Zheng, D., Liu, Y., Zhao, J., & Saddik, A. E. (2007). A survey of RST invariant image watermarking algorithms. *ACM Computing Surveys (CSUR), 39*(2), 5.