IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

A Suvery on DWT-DCT Based RST Attacks Invariant Watermarking Approach

Rashmika N Baria[1*], Mahesh M Goyani[2]

[1,2]Dept. of Computer Engineering & Information Technology, Government Engineering Collage, Modasa, India

Corresponding author: rashmikabaria85@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i3.574583 | Available online at: www.ijcseonline.org

Accepted: 09/Mar/2019, Published: 31/Mar/2019

Abstract— Digital Image Security is still recent topic of research in computer science engineering. Images are being shared from one device to another device. Security of digital data becomes important for many reasons such as confidentiality, authentication and integrity. Digital watermarking has emerged as an advanced technology to enhance the security of digital images. The insertion of watermark in images can authenticate it and guarantee its integrity. The watermark must be generally hidden does not affect the quality of the original image. In this paper, we discuss on different spatial and frequency domain watermarking methods and Various attacks like Translation, Rotation and Scaling will be addresses to make the approach RST invariant are also discuss.

Keywords— Discrete Wavelet Transform, Discrete Cosine Transform, Singular Value Decomposition, RST Attack

I. INTRODUCTION

In this digital world, there is rapidly growing and sharing of multimedia files. Billions of digital files are transferred via the internet per day. There are many ad- vantages privileged to users. But there are numerous disadvantages also like a security problem, copyright of data, data transformation. The main source of these problems is Internet. So security of the authentic information and some other issues has become a big question with multimedia source and content [1].

Digital data can be easily copied and transferred to an- other user without loss of data and quality of data. Solving these types of problems are challenges for the re- searchers. Data hiding technique is the solution of these problems [2]. Some multimedia data is introduces into the owner's data extracted process is used. This idea was initially used in bank currency notes. The watermark is embedded in the currency notes to hide the originality of the original data. Digital watermarking is a technique in which the original data is hidden with the watermark to preserve the originality of the original data. There are many requirements of watermarking techniques i.e. copyright protection, robustness, invisibility, data pay- load etc [1],[4]. In this paper we provide a survey of the latest techniques that are employed to watermark images. As shown in figure 1. Watermark data can be added in the binary format to the digital data and we can extract later to show an authentication about the data [1].

Digital watermarking is the process in which the image file is modified in such a way that either text or another image (watermark) is embedded without much change to the original image. The watermark can be hidden in the digital data either visibly or invisibly [1]. Digital watermarking technique can be classified by many different ways, according to the domain, the type of document, human perception, the application. Based on the embedding information concept, watermarking algorithms can be classified as either Spatial or transform domain.

The word watermark was first used at the end of the eighteenth century. In 1779, the first bank note forgery was attempted by John Mathison. The word watermark may have been acquired from the German term warking, which means watermark in English. The term digital watermarking appeared first in 1993, when Tirkel introduced two watermarking methods to conceal the watermark information within the images [3].

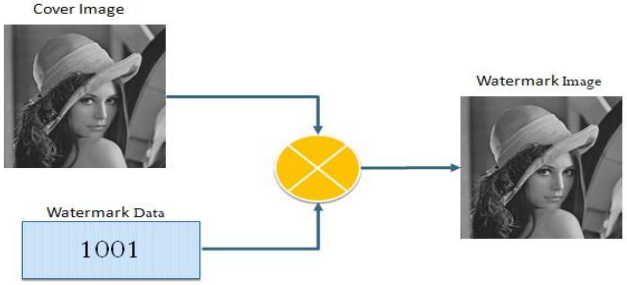

Figure 1. *Flow of Watermarking*

Watermarks have traditionally been used as a form of authentication for legal documents and paper currency. A watermark is embedded within the fibres of paper when it is first constructed and it is essentially invisible unless held up to a light or viewed at a particular angle. More importantly, a watermark is very difficult to remove without destroying the paper itself and it is not transfer if the paper is photocopied. The goal of digital watermarking is similar [4]. Watermark information usually inserted in a binary format to pixel value of the host image. Digital watermarking is a technique of embedding pieces of information into digital data such as text, audio, video and images that can be detected or extracted later to show authentication about the data.

A. Process of Image Watermarking

The process of image watermarking is divided into two parts [5]:

Watermark Embedding

The process of image watermarking is done at the source end. In this process watermark is embedding in the host image by using any watermarking algorithm or process [5]. The whole process is shown in figure 2.

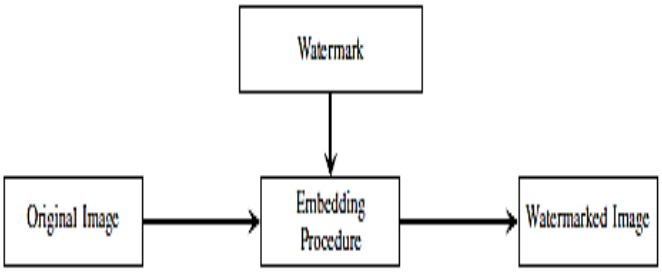

Figure 2. *Embedding Process*

Watermark Extraction

This is the process of extracting watermark from the watermark image by reverse the embedding algorithm [5]. The whole process is shown in figure 3.

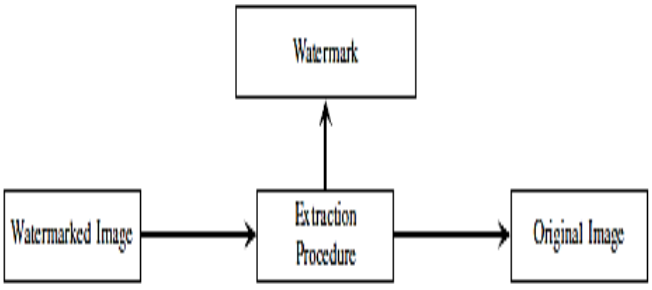

Figure 3. *Extracting Process*

Aspect of Data Hiding

Watermarking need some desirable properties based on the application of the watermarking system. These properties include robustness, transparency, capacity, blind detection and security. Some of the properties are presented here: [1],[4]

Imperceptibility: Imperceptibility refers to the amount of invisibility of watermark image and can be measured by standard metrics such as SSIM or PSNR. It measures the quality of host image should not be degraded when watermark is inserted in host image. That means watermark data cannot be heard by human eyes or human ear. It can be only accessible by authorized person [1]. Imperceptibility refers to as the perceptual similarity between the original image and the watermarked image. It means that the end user should not be able to perceive any visual or audio effect [3].

Capacity: An appropriate measure of data is inserted into an image in a watermarking framework. This inserted measure of data in a watermarked image is referred to as data payload. It implies the quantity of bits encoded with the image [3]. Capacity refers to the amount of information that can be hidden into the cover image. That means how it describes how many information bit hide into the cover image. The number of bits encoded in watermarking and image information should make an adequate amount of combination for figured application [4].

Security: Security refers to an eavesdropper's inability to detect hidden information that means it water- mark said to be secure if without having full knowledge of extraction and detection algorithm hacker cannot detect watermark data [1]. The aim of the watermark is to directly eliminate the inserted information that is watermark should resist against attacks [3].

Robustness: Robustness refers to an amount of modification of watermark image before an adversary can destroy hidden information that means without having full knowledge of extraction and detection algorithm any unauthorized person cannot detect hidden information, so it should be robust. It should be impossible to eliminate the watermark [3].

B. Classification

Digital watermarking techniques are classified into various types. This classification based on several criteria. All the classification describe in following table.

In the image watermarking domain based technique is generally used. They are spatial domain and transfer domain. But transfer domain techniques are more used compared to spatial domain because transfer domain is more robust than spatial domain to the attack [1] [3].

Table 1: Types of Watermarking Basis of Different Criteria

Sr.no	Criteria	Classification
1	Watermark Type	1. Noise: PseudoNoise, Gaussian Random and Chaotic Sequence 2. Image: Any Logo, Stamp Image, etc.
2	Robustness	1. Fragile: Easily Manipulated 2. Semi-Fragile: Resist From Some Type of Attacks 3. Robust: Not Affected From Attacks
3	Domain	1.Spatial:LSB,PatchworkAlgorithm 2.Frequency:DWT,DCT,DFT,SVD
4	Perceptivity	1. Visible Watermarking: Channel Logo 2. Invisible Watermarking
5	Host Data	1. Image watermarking 2. Text watermarking 3. Audio Watermarking 4. Video Watermarking
6	Data Extraction	1. Blind 2. Semi-Blind 3. Non-Blind

C. Objectives

The objective of research work is to increase robustness, accuracy and security. Digital watermarking is techniques for embedding various types of information in digital content. In general information protecting copyrights and proving the validity of data is embedded as a watermark. Why we need to embed such information in digital content using digital watermarking technology? The internet is one of the reasons. Watermarked content can prove its origin, thereby protecting copyrights. The transform watermark algorithms are more robust than spatial domain. Different watermark geometric attacks such as rotation, translation and scale attack are not recovered data easily.

D. Applications

It can be applied to different applications including digital signatures, finger printing, broadcast and copy control, document and image security, copy protection, medical application and so on.

Copyright protection: This application is of great interest to other vendors of digital information, such as news and photo agencies. For example, now days, a news channel, Aaj-tak is showing the animal's clips which are already shown on discovery channel logo on the video clips. As per the law, the Aaj-tak should pay the copy- right fee to the discovery channel [1]. Copyright protection appears to be one of the first applications for which digital watermarking were targeted. The Meta data in this case contains information about the copyright owner [4].

Copy control: Watermarking can be used as a strong tool to prevent illegal copying. For example, if an audio CD has a watermark embedded into it, then any of the system H/W like DVD or S/W cannot make a copy of it and even if it copies, the watermark data will not get copied to new duplicate audio CD. Now, the duplicate CD can be easily found because it does not have water- mark data. Watermarks can be used for copy prevention and control [4].

Finger printing: If monitoring and owner identification application place the same content, it may create a problem, if the owner finds on illegal copy, he can find out who is selling his contents by finding the watermark [1]. Additional data embedded by watermark in this application is used to trace the originator or recipients of a particular copy of multimedia file. For example, watermarks carrying different serial or ID numbers are embedded in different copies of multimedia information before distributing them to a large number of recipients [4]. Fingerprinting should be resistant to the collusion attack, that is, it is impossible to embed more than one ID number in the host multimedia file; otherwise a group of users with the same image containing different finger- prints would be able to collude and validate the finger- print or create a copy without any fingerprints [7].

Document and image security: A watermark system is said to be secure, if the hacker cannot remove the water- mark without having full knowledge of embedding algorithm, detector and composition of watermark. A watermark should only be accessible by authorized parties [1].

Medical application: Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster [1].

The above represent a few example applications where digital watermarks could potentially be of use. In addition, there are many other applications for right management and protection like tracking use of content, binding content to specific players, automatic billing for viewing content, and broadcast monitoring, among others [4].

The organization of the paper as follows, Section I contains the introduction of digital watermarking, aspect of digital watermarking, objective, classification and applications of digital watermarking methods, Section II contains the related work of digital watermarking methods for embedding and extracting watermark and the Section III conclusion of the survey.

II. RELATED WORK

Watermarking is the method to hide the secret in- formation into the digital media using some strong and appropriate algorithm [8]. Algorithm plays an important role in watermarking as, if the used watermarking technique is efficient and strong then the watermark being embedded using that technique cannot be easily detected. The attacker can only destroy or detect the secret information if he know the algorithm otherwise it is critical to know the watermark. There are various algorithms which are used to hide the information. Those algorithms come into two domains, Spatial and Frequency domain. Fig 4. Shown different spatial and frequency domain based watermarking method. Digital watermarking involves embedding watermark data into original in- formation. In other words, a watermark is a pattern of bits inserted into multimedia data such as digital image, audio or video file that helps to identify the file's copy- right information (author, rights, etc.).

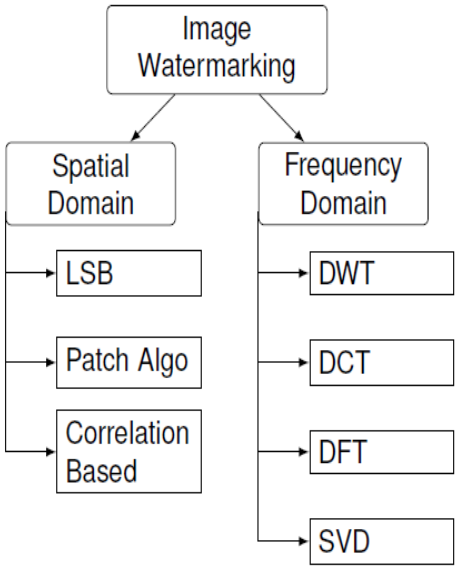

Figure 4. *Techniques of Watermarking*

Spatial Domain Techniques

In the spatial domain, the watermark information is embedded directly into the pixel value of the host or cover image, and to preserve the image quality, the watermark is usually embedded into the least significant bits of the image. These methods are fast and simple and provide law information hiding capacity [9].

However, spatial domain approaches cannot survive against noise compression attacks. Further- more, once the method is uncovered, embedded water- mark can be easily modified by a third party [9]. Spatial domain method includes least significant bit, patchwork algorithm, Additive watermarking and co-relation based technique. The strength of the spatial domain watermarking is

- ✓ Simplicity
- ✓ Very law computational complexity.
- ✓ Less time consuming

Some of its main algorithms are as discussed below:

A. Least Significant Bit (LSB)

The LSB is the simplest spatial domain water- marking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image. Example of least significant bit watermarking:

Image:
10010101 00111011 11001101 01010101. . . .
Watermark:
1 0 1 0. . . ..
Watermarked Image:
10010101 00111010 11001101 01010100. . . ..

According to P. Singh and R. S. Chadha [1] this method is easy to implement and does not generate serious distortion to the image; how- ever, it is not very robust against attacks. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The watermark may be spread throughout the image or may be in the select location of the image.

Baisa L. Gunjal and R.R. Manthalkar [2] proposed that LSB based watermarking in spatial do- main is the straight forward method, but once algorithm is discovered, watermark will be no more secured. An improvement on LSB substitution is to use pseudo random generator to determine pixels to be used for embedding, based on given key. Manasha Saqib and Sameena Naaz [3] proposed that the most straight for- ward method to implement is LSB technique. In this process watermark bit is added to each pixel of the LSB. During extraction or detection method, the last bit of every pixel is read to unveil the watermark information.

Seyed Mojtaba et al [9] proposed that one of the simplest spatial domain techniques is the least significant bit (LSB) method. As shown in the Fig.3, the input image is firstly binaries by the LSB method. The right- most bits of each pixel are replaced by input watermark bits. Finally, the modified binary pixel values are converted back to decimal pixel values.

The main advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not degrade.

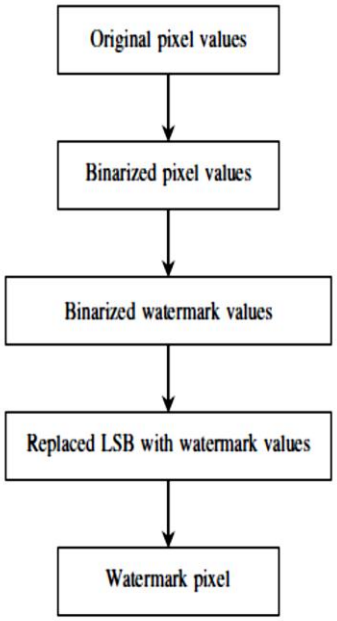

Figure 5. *Least Significant Bit*

The main drawback of LSB technique is its poor robustness to common signal processing operations because by using this technique watermark can easily be destroyed by any signal processing attacks. It is not vulnerable to attacks and noise but it is very much imperceptible.

B. Patchwork Algorithm

P. Singh and R. S. Chadha [1] proposed that Patchwork is a data hiding technique developed by Bender et al and published on IBM systems Journal, 1996. It is based on a pseudo random, statistical model. Patchwork imperceptibly inserts a watermark with a particular statistic using a Gaussian distribution. Manasha Saqib and Sameena Naaz [3] proposed that Patchwork technique is one of the statistical technique that was develop by Bender et al Based on a statistic discovered utilizing a Gaussian distribution, patches of watermark are inserted in this technique. The working of this technique is as follows: Two patches are arbitrary chosen say patch A and patch B. The image information of patch A is brightened and image information of patch B is darkened. In this method redundant pattern encoding is used to insert information into an image.

C. Correlation Based Watermarking

P. Singh and R. S. Chadha [1] proposed that a pseudo random pattern says W(x, y) is added to cover image I(x, y).

$$I_w(x,y) = I(x,y) + K * W(x,y) \quad (1)$$

Where k represent the gain factor, I_w represent watermark image at position x, y and I represent cover image. Here, if increase the gain factor then although it increases.In correlation based technique, a pseudorandom noise pattern says $W(x,y)$ is added to cover image$I(x,y)$.

Limitations of spatial domain watermarking:

The spatial domain watermarking is simple as com- pared to the transform domain watermarking. The robustness is the main limitation of the spatial domain watermarking. It can survive simple operations like crop- ping and addition of noise. Another limitation of spatial domain technique is that they do not allow for the subsequent processing in order to increase the robustness of watermark.

Frequency Domain Techniques:

In frequency domain technique, watermark can be inserted into frequency coefficients of image giving more information hiding capacity and more robust- ness against watermark attacks. Watermarking in frequency domain is more robust than watermarking in spatial domain because information can be spread out to entire image. DCT, DWT and DFT are frequency domain method. As shown in figure 4 image is decomposed in sub-layer.

A. Discrete Wavelet Transform

Discrete wavelet transform (DWT) of the image produces multi resolution representation of an image. The multi resolution representation provides a simple frame- work for interpreting the image information. The DWT analyses the signal at multiple resolution. DWT divides the image into high frequency quadrants and low frequency quadrants. The low frequency quadrant is again split into two more parts of high and low frequencies and this process is repeated until the signal has been entirely decomposed.

The single DWT transformed two dimensional image into four parts: one part is the low frequency of the original image, the top right contains horizontal details of the image, the one bottom left contains vertical details of the original image, the bottom right contains high frequency of the original image. The low frequency coefficients are more robust to embed watermark because it contains more information of the original image. The reconstruct of the original image from the decomposed image is performed by IDWT.

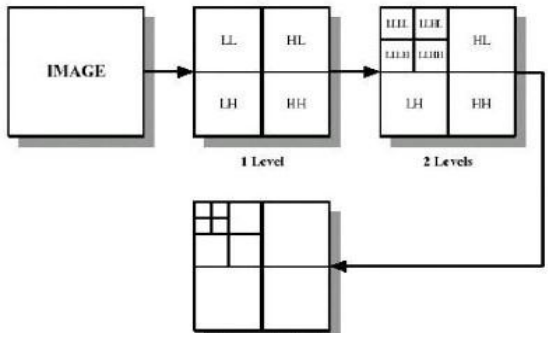

Figure 6. *Workflow of 2 level DWT [10]*

The digital wavelet transform are scalable in nature. DWT more frequently used in digital image watermarking because of its excellent spatial localization and multi resolution techniques. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermark is embedded efficiently.

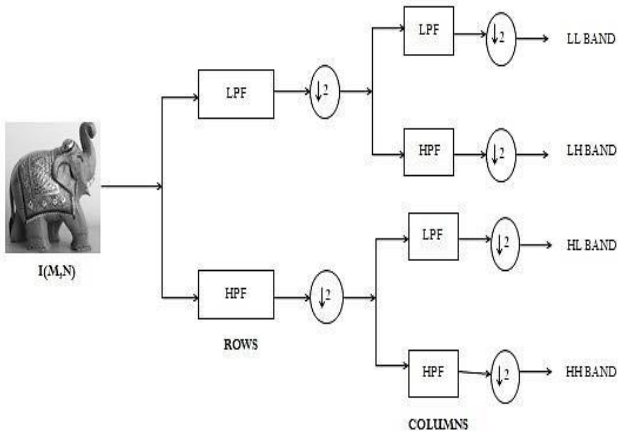

Figure 7. *Schematic Diagram of 2D Wavelet Transform*

The DWT is applied on the host image to decompose the image into four non overlapping multi resolution co-efficient sets.

P. Singh and R. S. Chadha [1] proposed that the wavelet transform decomposes the image into three spatial directions, i.e, and horizontal, vertical and diagonal. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decom- position and is smaller for other bands (HH, LH, and HL). According to Baisa L. Gunjal and R.R. Manthalkar [2], image itself is considered as two dimensional signal. When image is passed through series of low pass and high pass filters, DWT decomposes the images into sub bands of different DWT levels. DWT offers multi resolution representation of a signal. Manasha Saqib and Sameena Naaz [3] proposed that DWT is a multipurpose numerical transform having different applications in various areas. Firstly, in DWT the cover image is converted into frequency domain and after that the coefficients of frequency are modified de- pending upon the transformed coefficients of the watermark and afterwards a robust watermarked image is archived. Then the inverse DWT is applied to obtain the reconstructed image. Hai Tao and Li Chongmin et al [4] proposed that multi resolution image representations using DWT have received wide range of attention in the recent years. It is an efficient mathematical tool that decomposes an image into hierarchical sub-bands. Each sub-band is logarithmically separates an image into a lower resolution and labels the resulting sub-images. LL, which is the coarse overall shape, covers the low frequency components that contain most of the energy in the image and LH, HL and HH which represent higher frequency detailed information have the finer scale wavelet coefficients according to the filters used to generate sub-image. Normally, embedding the watermark into image's high frequency parts will strength robustness, but reduce imperceptibility. Otherwise, image's low frequency is embedded by watermark, it will results increasing imperceptibility, but reduce robustness. NileshRathi and Ganga Holi [6] said that DWT is a multi-resolution decomposition of a signal. It is a new signal analysis theory and is a "time-frequency" method. It captures both frequency and location information. A signal is split into two parts, usually high frequencies and low frequencies. The edge components of the signal are largely contained to the high frequency part. The low frequency part is split again into two parts of high and low frequencies. This process is continued an arbitrary number of times.

B. Discrete Cosine Transform

In DCT, for embedding the watermark information, we divide the image into different frequency bands. In Figure 8 FL denotes the lowest frequency component of the block, while FH denotes the higher frequency component and FM denotes the middle frequency component which is chosen as the embedding region. The Discrete cosine transform achieves good robustness against various signal processing attacks because of the selection of perceptually significant frequency domain coefficients.

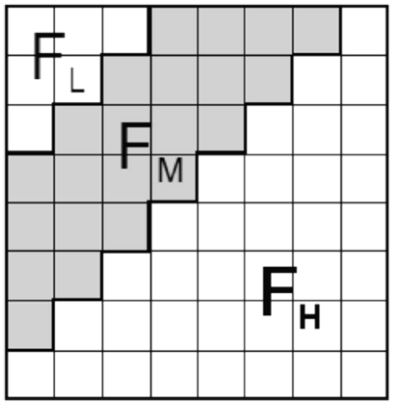

Figure 8. *DCT Transform*

Based on Md Saiful Islam and UiPil Chong [11], the popular block-based DCT transform segments an image non-overlapping block and applies DCT to each block. This result in giving three frequency sub-bands: low frequency sub band, mid-frequency sub band and high frequency sub-band. DCT-based watermarking is based on two main facts. The first one is that most of the signal energy lies at low-frequencies sub band which contains the most important parts of the image and second one is that high frequency components of the image are usually removed through compression and noise attacks. Nilesh Rathi and Ganga Holi [6] according to them, DCT express a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. For DCT with block size (M*N), the

connection between the spatial domain image pixels $x(i,j)$and the transform coefficient $y(u,v)$is as follows:

$$Y(u,v) = \frac{2c(u)c(v)}{\sqrt{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} x(i,j) \cos\left[\frac{(2i+1)}{2M}\right] \cos\left[\frac{(2j+1)}{2N} v\pi\right] (2)$$

Where u = 0, 1, .. M-1, v = 0, 1,, ..N-1 , and

$$c(k)\begin{cases}\frac{1}{\sqrt{2}}, & if\ k=0;\\ 1, & Otherwise\end{cases}$$

The conversion of time domain signal into the frequency domain signal is done by DCT. Manasha Saqib and Sameena Naaz [3] proposed the 2-dimensional DCT of a matrix gives the transform coefficients in form of other matrix. The lowest frequency coefficients is represented by the left top most corner of the matrix while the highest frequency coefficients is represented by the right bottom most corner of the matrix. In DCT, an image is divided into pseudo frequency bands, and the watermark is embedded into the middle frequency sub bands.

P. Singh and R. S. Chadha [1] proposed that DCT like a Fourier transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away. Bhupendra Ram [7], DCT is related to DFT in a sense that it transforms a time domain signal into its frequency components. The DCT however only uses the real parts of the DFT coefficients. In terms of property, the DCT has a strong energy compaction property and most of the signal information tends to be concentrated in a few low frequency components of the DCT. Based on Seyed Mojtaba Mousavi et al [9], DCT based method is a block-based technique. By using his transform, the image will be divided into three frequency bands: Low (FL), Middle(FM), high (FH) frequency regions. These algorithms are robust compared to digital image processing operations for example low pass filtering, brightness and contrast adjustment and few more. . Based on Radhika v. Totla and K.S.Bapat [10], DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. In order to invisibly embed the watermark that can survive loss data compressions, a reasonable tradeoff is to embed the watermark into the middle-frequency range of the image. The middle frequency bands are chosen such that they have minimized that they avoid the most visual important parts of the image (low frequency) without over-exposing themselves to removal through compression and noise attacks. DCT domain watermarking can survive against the attacks such as Noising, compression, sharpening, and filtering. Tulika Bhuyan et al. proposed that DWT can be effectively used to identify areas in the image where the watermark can be embedded maintaining the visual transparency of the host. This is one major advantage of DWT over DCT. The image is divided into four sub-bands LL, HL, LH and HH using two types of filter; scaling and wavelet filter. LL sub-band is the low frequency sub-band representing the approximate image, HL is the high frequency sub-band containing the horizontal details of the image, LH is the high frequency sub-band containing the vertical details of the image and HH is the high frequency sub-band of the image [12]. These results in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks.

C. Discrete Fourier Transform

Discrete Fourier Transform (DFT) offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT decomposes an image in sine and cosine form. The DFT based watermark embedding techniques are divided in two types: one is the direct embedding and the other one is the template based embedding. According to the direct embedding technique the watermark is embedded by modifying DFT magnitude and phase coefficients. The template based embedding technique introduces the concept of templates. A template is structure which is embedded in the DFT domain to estimate the transformation factor. Once the image undergoes a transformation this template is searched to resynchronize the image, and then the detector is used to extract the embedded spread spectrum watermark. The DFT is a well-known mathematical operation that transforms the image from the spatial domain to frequency domain. Let $f(x,y)$ represents an image of size M*N, x=0, 1, 2,,...,M-1 and y=0, 1, 2,..,N-1. The forward and reverse DFT are given in equations:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{x=0}^{M-1} f(x,y) e^{-j2\pi} \left(\frac{ux}{M} + \frac{vy}{N}\right) (3)$$

$$F(x,y) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{x=0}^{M-1} f(u,v) e^{j2\pi} \left(\frac{ux}{M} + \frac{vy}{N}\right) (4)$$

Where $F(u,v)$ is the DFT coefficient, u =0, 1, 2,..,M-1 and v=0, 1, 2,..,N-1. The polar representation of the Fourier transform can also shown by:

$$F(u,v) = |F(u,v)| e^{j} \emptyset(u,v) (5)$$

Where $|F(u,v)|$ is magnitude spectrum and $\emptyset(u,v)$ is phase spectrum. The magnitude and phase contain the least and the most amount of information, respectively, about the image and provide potential candidates for embedding watermark information. Bhupendra Ram [7] proposed DFT is an operation that transforms a continuous function into its frequency components. The equivalent transform for discrete function requires the DFT Fourier transform allow analysis and processing of the signal in its frequency domain by means of analyzing and modifying these coefficients. Fourier transform is not able to offer frequency data in any partial time quantum.

D. Singular Value Decomposition

Based on Amarjot Kaur and Jagdeep Singh [14], by perception of picture processing, a picture might be considered as the matrix with nonnegative scalar entries. SVD is really an emphatic mathematical evaluation tool applied to analyze matrices. Columns of U and V would be the left singular vectors and right singular vectors respectively of image. These watermarking methods are mainly used for obtaining either SVD of original picture or each block of host picture, furthermore it alters singular values to the watermark. Using SVD it is possible to locate the best estimate of the original information points using less dimensions. Thus, SVD is viewed as a technique for reduction of data. During this transformation, one matrix is often decomposed in 3 matrices which have an equivalent size due to the real matrix. It is helpful to determine a distinction with Gaussian elimination and its equation.

Hai Tao el al [4] proposed that Singular Value Decomposition is a numerical method that is based upon linear algebra and is used by complex matrix or factorization of a real matrix having many useful applications in statistics and signal processing. It is considered to be a technique for changing co-related variables into a set of co-related variables that better uncover the different relationships among the original information. Nilesh Rathi and Ganga Holi [6] proposed this type of algorithms has proven to be robust in watermarking system. Although SVD works for any N*M matrix, and without loss of the generality, The singular value decomposition of A is represented by:

$$A = U \sum V^T (14)$$

Where U and V are the unitary matrix, and Σ is a diagonal matrix and the superscript T denotes as matrix transposition. SVD is based on a theorem from linear algebra which says that a rectangular matrix A can be broken down into the product of three matrices - an orthogonal matrix U, a diagonal matrix S, and the transpose of an orthogonal matrix V. The theorem is usually presented something like this:

$$A = U * S * V^T (15)$$

Based on Manasha Saqib and Sameena Naaz [3] is a numerical method that is based upon linear algebra and is used by complex matrix or factorization of a real matrix having many useful applications in statistics and signal processing. SVD is considered to be one of valuable numerical analysis tools that is used to analyze matrices. Seyed Mojtaba Mousavi [9] et al proposed that using SVD it is possible to locate the best estimate of the original information points using less dimensions. Thus, SVD is viewed as a technique for reduction of data. SVD is rectangular matrix can be decomposed into three matrices U, S and the conjugate transpose V. U and V are orthogonal square matrices and S is a rectangular diagonal matrix with its values arranged in descending order. Tulika Bhuyan et al. proposed SVD based watermarking based on image decomposition. The U matrix and V matrix are orthogonal matrices. Columns of U and V are called the left and right singular vectors respectively. They represent the horizontal and vertical details of an image. The S matrix is a diagonal matrix of singular values. S matrix gives the gray scale values of the image layers formed by U and V. SVD is widely used for various image processing applications due to the stability of singular values. These singular values remain intact even after the matrix is rotated, translated or transposed. According to Zhang Nana, SVD is one of the important orthogonal transformations in linear algebra. It has important applications in signal and image processing, image compression, digital watermarking, optimization and so on.

Table 2: Comparison Table

Ref.	S/F	S/H	Methods	Parameter	Attacks
[6]	F	H	DWT, DCT, SVD	PSNR, MSE,NC	MF, RO-TATION,
[16]	S,F	H	LSB, DWT	PSNR, MSE	-
[17]	S,F	H	LSB, DCT	PSNR, MSE	-
[18]	F	H	DWT,DCT and Saliency detection	PSNR, SSIM, MSE	GN, JC
[19]	F	H	DWT, DCT	PSNR, SSIM	GN, JC, MF,
[20]	F	S	DWT	PSNR, NC	S AND P, GN, JPWG,
[21]	F	H	SVD, QIM	PSNR, NC	GN, JC, MF,
[22]	F	H	DFT, DCT, AT	PSNR, SSIM, MSE, NC	GN, S AND P, GF, HF,

[23]	F	H	DFT-SVD, DCT-SVD	PSNR	GN, JPEG

III. WATERMARKING ATTACKS

There are various possible malicious intentional or unintentional attacks that may be affect the watermarked image. A brief introduction to various types of watermarking attacks is as under.

Removal attacks: Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal [1].

Cryptographic attacks: Cryptographic attacks are quite equivalent to the attacks applied in cryptography. There are the seriously forced attacks which intend to discover secret information using the exhaustive searches. Ever since numerous watermarking system utilize a secret key, it is greatly significant to use keys with a safe length. In addition, another attack is the so-called oracle attacks in this category, which is able to apply to produce a non-watermarked image while a device of a watermark detector is attainable [4].

Interference attacks: Interference attacks are those which add additional noise to the watermarked object. Lossy compression, quantization, collusion de-noising, demodulation, averaging and noise storm are some examples of this category of attacks [1].

Geometric attacks: All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack [1].

IV. CONCLUSION

The paper studies different approaches, algorithms and attacks and gaining robustness against RST attacks. Watermarking is the process of embedding predefined data into images in a way that the degradation of quality is minimized and remain in an imperceptible level. Many digital watermarking algorithms have been proposed in spatial and transform domains. The techniques in the spatial domain still have relative low-bit capacity and are not resistant enough to loss image compression. On the other hand, frequency domain-based techniques can embed more bits for watermark and are more robust to attack. In our system, different transform watermark algorithms based on robustness have been evaluated.

ACKNOWLEDGMENT

I would like to thank my guide, Prof. (Dr.) Mahesh M. Goyani, Assistant Professor of Department of Computer Engineering & Information Technology Government Engineering College, Modasa for providing continual encouragement through a relaxed approach and support and proper guidance for holding us to a higher standard.

REFERENCES

[1] P. Singh and R. S. Chadha, "A survey of digital wa- termarking techniques, applications and attacks," International Journal of Engineering and Innova- tive Technology, vol. 2, no. 9, pp. 165–175, 2013.

[2] B. L. Gunjal and R. Manthalkar, "An overview of transform domain robust digital image water- marking algorithm," Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 1, pp. 37–42, 2010-11.

[3] M. Saqib and S. Naaz, "Spatial and frequency do- main digital image watermarking techniques for copyright protection," International Journal of En- gineering Science and Technology, pp. 691–698, 2017.

[4] H. Tao, L. Chongmin, J. M. Zain, and A. N. Ab- dalla, "Robust image watermarking theories and techniques: A review," Journal of Research and Technology, vol. 12, pp. 122–135, 2014.

[5] L. K. Saini and V. Shrivastava, "A survey of digi- tal watermarking techniques and its applications," International Journal of Computer Science Trends and Technology, vol. 2, pp. 70–73, 2014.

[6] N. Rathi and G. Holi, "Securing medical im- ages by watermarking using dwt-dct-svd," Inter- national Journal of Computer Trends and Technol- ogy, vol. X, pp. 1–8, 2014.

[7] B. Ram, "Digital image watermarking technique using discrete wavelet transform and discrete co- sine transform," International Journal of Advance- ments Research and Technology, vol. 2, no. 4, pp. 19–27, 2013.

[8] E. Sonia, E. N. K. Garg, and E. G. Singh, "A sur- vey on digital image watermarking," International Journal of Advanced Research in Computer Engi- neering and Technology, vol. 3, pp. 2054–2057, 2014.

[9] S. M. Mousavi, A. Naghsh, and S. A. R. Abu- Bakar, "Watermarking techniques used in medi- cal images: a survey," Journal of Digital Imaging, vol. 27, no. 6, pp. 714–729, 2014.

[10] R. v. Totla and K.S.Bapat, "Comparison analysis of watermarking in digital image using dct and dwt," International Journal of Scientific and Research Publications, vol. 3, pp. 1–4, 2013.

[11] M. S. Islam and U. P. Chong, "A digital image wa- termarking algorithm based on dwt dct and svd," International Journal of Computer and Commu- nication Engineering, vol. 3, no. 5, pp. 356–360, 2014.

[12] T. Bhuyan, V. kumar Srivastva, and F. Thakkar, "Shuffled svd based robust and secure digital image watermarking," International Conference on Electrical, Electronics, and Optimization Tech- niques, pp. 1229–1233, 2016.

[13] J. sahu and D. shukla, "Digital image watermark- ing method 4 level dwt-dct on the basis of psnr," International Journal of Engineering Development and Research, vol. 3, pp. 1008–1012, 2015.

[14] A. Kaur and J. Singh, "Digital image watermark- ing techniques: A review," International Journal of Advanced Research in Computer Science, vol. 8, no. 8, pp. 714–718, 2017.

[15] N.Senthikumaran and S.Abinaya, "Comparison analysis of digital image watermarking using dwt and lsb technique,"

International Conference on Communication and Signal Processing, pp. 448– 451, 2016.
[16] Anushka and A. Saxena, "Digital image water- marking using least significant bit and discrete co- sine transformation," International Conferenceon Intelligent Computing ,Instrumentation and Control Technologies, pp. 1582–1585, 2017.
[17] O. Hosam and N. B. Halima, "A hybrid roi- embedding based watermarking technique using dwt and dct transform," Journal of Theoretical and Applied Information Technology, vol. 81, no. 3, pp. 514–528, 2015.
[18] M.Jamali, S.Samavi, N.Karimi, S. Soroushmehr, K. Ward, and K. Najarian, "Robust watermarking in non-roi of medical images based on dct- dwt," IEEE Transactions on Image Processing, pp. 1200–1203, 2017.
[19] R. Keshavarzian, "A new roi and block based watermarking scheme using dwt," Iranian Confer- ance on Electrical Engineering, pp. 1323–1328, 2012.
[20] P. Singh, B. Raman, and M. Misra, "Region of interest based robust watermarking scheme exploit- ing the homogeneity analysis," International Con- ference on Intelligent Computing and Control Systems, pp. 797–803, 2017.
[21] M. Hamidi1, M. E. Haziti, and H. C. and Mo- hammed El Hassouni, "Hybrid blind robust im- age watermarking technique based on dft-dct and arnold transform," Springer, vol. 77, no. 20, pp. 27181–27214, 2018.
[22] D. Sudiana and D. Apriyadi, "Dft-svd and dct-svd domain digital image watermarking: Implementa- tion and performance analysis," Optics and Remote Sensing Research Group, 2015.
[23] H. Cai, H. Liu, M. Steinebach, and X. Wang, "A roi-based self-embedding method with high recov- ery capability," IEEE Transactions on Image Pro- cessing, pp. 1722–1726, 2015.
[24] H. L. Khor, S.-C. Liew, and J. M. Zain, "Region of interest-based tamper detection and lossless re- covery watermarking scheme (roi-dr) on ultra- sound medical images," Journal of Digital Imag- ing, vol. 30, no. 3, pp. 328–349, 2017.
[25] R. Choudhary and G. Parmar, "A robust im- age watermarking technique using 2-level discrete wavelet transform (dwt)," IEEE International Con- ference on Communication, Control and Intelligent Systems, pp. 120–124, 2016.
[26] A. Chen and X. Wang, "An image watermarking scheme based on dwt and dft," International Journal of Computer Technology and Applications, 2017.
[27] S. D. Degadwala and D. S. Gaur, "4-share vcs based image watermarking for dual rst attacks," International Journal of Computer Technology and Applications, pp. 902–912, 2018.
[28] E. Najafi, "A robust embedding and blind ex- traction of image watermarking based on discrete wavelet transform," Mathematical Sciences, vol. 11, no. 4, pp. 307–318, 2017.
[29] Y. Wang1, J. Liu1, Y. Yang1, D. Ma1, and R. Liu1, "3d model watermarking algorithm robust to geometric attacks," The Institution of Engineering and Technology, vol. 11, no. 10, pp. 822–832, 2017.
[30] D. V. Singh, "Digital watermarking: A tutorial," Multidisciplinary Journals in science and technol ogy, pp. 10 – 19, 2011.
[31] A. D'Silva and N. Shenvi, "Data security using svd based digital watermarking techniques," Interna tional Conference on Trends in Electronics and In- formatics, pp. 382–386, 2017.
[32] N. Sahu and A. Chugh, "A survey on digital im- age watermarking techniques based on frequency domain," International Journal of Current Trends in Engineering and Technology, vol. 3, pp. 56–59, 2017.
[33] A. Sheshasaayee and S. D, "Analysis of techniques involving data hiding and watermarking," International Conference on Innovative Mechanisms for Industry Applications, pp. 593–596, 2017.
[34] H. Li, S. Wang, W. Song, and Q. Wen, "A novel watermarking algorithm based on svd and zernike moments," Springer Berlin Heidelberg, pp. 448– 453, 2005.
[35] P. Parashar and R. K. Singh, "A survey: Digital im- age watermarking techniques," International Jour- nal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 6, pp. 111–124, 2014.
[36] M. S. Islam and U. P. Chong, "A digital image wa- termarking algorithm based on dwt dct and svd," International Journal of Computer and Commu- nication Engineering, vol. 3, no. 5, pp. 356–360, 2014.
[37] L. K. Saini and V. Shrivastava, "A new hybrid dwt- dct algorithm for digital image watermarking," International Journal of Advance Engineer ing and Research Development, vol. 1, pp. 1–8, 2014.
[38] M. Singh, A. Singhal, and A. Chaudhary, "Digital image watermarking techniques: A survey," International Journal of Computer Science and Telecommunications, vol. 4, pp. 51–55, 2013.
[39] R. Kaur and H. Singh, "Image watermarking in dct, dwt and their hybridization using svd: A survey," International Journal of Innovations in Engineer- ing and Technology, vol. 4, pp. 376–379, 2014.
[40] N. Mittal and A. S. Bisen, "Digital watermaking using svd and dwt, fft, dct based method : A sur- vey," International Journal of Innovations in Engi- neering and Technology, vol. 3, pp. 40–45, 2017.
[41] A. Singh1 and D. A. Sharma, "Digital image water- marking techniques: A survey," International con- ference on science, technologies and management, pp. 620–625, 2017.
[42] R. Patel and Prof.A.B.Nandurbarkar, "Implemen- tation of dct dwt svd based watermarking algo- rithms for copyright protection," International Re- search Journal of Engineering and Technology, vol. 2, pp. 340–344, 2015.
[43] S. Kaur, "A digital image watermarking technique based on dwt," International Journal of Computer and IT, pp. 1–6, 2015.
[44] M. H. Arya, S. S. Bundela, V. Kushwah, and P. Jain, "A survey on digital watermarking tech- niques," International Journal of Engineering Technology Science and Research, vol. 3, pp. 1–6, 2016.
[45] H. Lala, "Digital image watermarking using discrete wavelet transform," International Research Journal of Engineering and Technology, vol. 4, pp. 1682–1685, 2017.

Authors Profile

Ms. Rashmika N Baria pursued Bachelor of Engineeringfrom Babaria Institute of Engineering , Vadodara, India in 2016 and currently pursuing Master of Engineering Computer Engineering from Department of Computer Engineering & Information Technology, Government Engineering College (GEC), Modasa, India (2018).

Prof.(Dr.) Mahesh M. .Goyani received the Bachelor of Engineering degree from VNSGU, Surat, India in 2005 and Master Of Engineering Computer Engineering from SPU, V.V.N, India in 2009 and P.H.D from Charusat, Changa in 2017. He is now with Government Engineering Collage, Modasa as the assistant professor. His main research work focuses on Machine learning, Pattern recognition, Image processing. He has 13 years of teaching experience.

