

Ridgelet Transform based Robust Image Watermarking Technique

*Thesis submitted in partial fulfillment
of the requirements for the award of degree*

of

Master of Engineering

in

Computer Science and Engineering

Submitted By

Jashanjot

(Roll No. : 801632013)

Under the supervision of

Dr. Singara Singh Kasana

Associate Professor



THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

Computer Science and Engineering Department

Thapar Institute of Engineering and Technology, Patiala-147004

June 2018

CERTIFICATE

I hereby certify that the work presented in the thesis entitled, "*Ridgelet Transform based Robust Image Watermarking Technique*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Computer Science and Engineering* submitted in Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Singara Singh Kasana* and refers other researcher's work which are duly listed in the reference section. The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature: *Jashanjot*

Jashanjot

It is certified that the given statement made by my student is correct to the best as per my knowledge and belief.

S. Kasana
22/8/18

Dr. Singara Singh Kasana

Associate Professor,

CSED, TIET, Patiala

ACKNOWLEDGEMENT

First of all, I would like to thank the Almighty, who has always guided me to work on the right path of the life. This work would not have been possible without the encouragement and able guidance of my supervisor **Dr. Singara Singh Kasana**. I thank my supervisor for his time, patience, discussions and valuable comments. His enthusiasm and optimism made this experience both rewarding and enjoyable.

I would like to express my gratitude to **Dr. Maninder Singh**, Head of Computer Science and Engineering Department and **Dr. Ashutosh Mishra**, P.G. coordinator for their constant motivation and encouragement.

I am also thankful to the entire faculty and staff members of Computer Science Department for their direct-indirect help, cooperation, love and affection.

Last but not the least, I would like to thank my parents for their wonderful love and encouragement, without their blessings none of this would have been possible. I would also like to thank my close friends for their constant support.

Jashanjot

ABSTRACT

Image watermarking is a mechanism to embed secret data within the image contents to protect the copyright and prove authentication. Watermarking is basically requirement for improving the robustness and invisibility opposing the various attacks in embedding watermark procedure. Among the two main types of domains used for watermarking, the more robust domain is transform domain as compared to spatial domain. Wavelets are widely used in existed algorithms for transform based watermarking but the wavelets are able to just describe the three image directions namely; horizontal, vertical and diagonal when dealing with the images. Wavelets fail to handle the linear singularities because of their isotropic support and hyperplane singularities of the image more effectively or the point wise singularities. These problems are effectively overcome by Multi-scale geometric analysis. In order to capture the geometric regularity of an image and to find an optimal directional representation; Curvelet, Contourlet, Ridgelet Transforms have been proposed. In this work, hybrid watermarking system is proposed which uses Ridgelet Transform, Robust Principle Components, Singular Values Decomposition in the watermarking process. First input image is transformed into *HSI* color space and *I* channel is operated by Robust Principle Components to get the low rank matrix. Further, Singular Values Decomposition is applied on this matrix to decompose the contents in order to embed the watermark in it. Using Arnold Transform, watermark is scrambled to make it secure. Ridgelet transform is directional sensitive, and provides

edge information in the image. Unlike other frequency transform domain, Ridgelet Transform has spatial frequency locality and is robust towards a broad range of attacks. Proposed technique is more robust and imperceptible than the existing algorithms. The quantitative and visual results show the effectiveness of the proposed technique as it is highly tolerant against various geometric and image-processing attacks.

Contents

Acknowledgement	ii
Abstract	iii
List of Figures	ix
List of Tables	xiii
List of Abbreviations	xiv
1 Introduction	1
1.1 History of Hiding Data	1
1.1.1 General Framework of Watermarking	2
1.1.2 Different types of Digital Watermarking	4
1.2 Fundamental Transforms used for Watermarking	5
1.2.1 Discrete Cosine Transform	5
1.2.2 Discrete Wavelet Transform	5
1.2.3 Singular Value Decomposition	5
1.2.4 Curvelet Transform	6
1.2.5 Discrete Fourier Transform	7
1.2.6 Continuous Ridgelet Transform	8
1.2.7 Contourlet Transform	8
1.3 Attacks on Watermarking System	9

1.3.1	Affine Attack	9
1.3.2	Contrast Enhancement Attack	10
1.3.3	Additive Gaussian Noise Attack	10
1.3.4	Histogram Equalization Attack	10
1.3.5	Multiplicative Speckle Noise Attack	10
1.3.6	Rotation Attack	11
1.3.7	Salt and Pepper Noise Attack	11
1.3.8	Sharpening Attack for Contrast Variations	11
1.3.9	X-Shear Attack	11
1.3.10	Y-Shearing Attack	11
1.4	Characterstics of Watermarking	11
2	Literature Survey	13
2.1	<i>DWT-SVD</i> based Watermarking Techniques	13
2.2	<i>SVD</i> based Watermarking Schemes	14
2.3	Miscellaneous Watermarking Techniques	15
3	Problem Statement	18
3.1	Research Gaps	18
3.2	Problem Definition	19
3.3	Objectives	19
4	Proposed Technique	21
4.1	Introduction	21
4.1.1	Ridgelet Transform	21
4.1.2	Robust Principal Component Analysis	22

4.1.3	Arnold Transform	23
4.2	Proposed Technique	24
4.2.1	Algorithm for Embedding Watermark	25
4.2.2	Algorithm for Extraction Process	27
5	Experimental Results and Analysis	29
5.1	Experimental Results	29
5.2	Quality Parameters	31
5.3	Effect of Attacks	32
5.3.1	Affine Attack	32
5.3.2	Contrast Enhancement Attack	33
5.3.3	Additive Gaussian Noise Attack	34
5.3.4	Histogram Equalization Attack	35
5.3.5	Multiplicative Speckle Noise Attack	36
5.3.6	Rotation Attack	38
5.3.7	Salt and Pepper Noise Attack	39
5.3.8	Sharpening Attack for Contrast Variations	40
5.3.9	X-Shear Attack	41
5.3.10	Y-Shearing Attack	42
5.4	Analysis of the Results	43
6	Conclusion and Future Work	50
6.1	Conclusion	50
6.2	Future Work	51
	<i>Bibliography</i>	52

Appendix 58

List of Figures

1.1	General Watermark Embedding Framework	3
1.2	General Watermark Extraction Framework	3
4.1	Distribution of Image Coordinates	23
4.2	Flow chart for the Embedding Process	26
4.3	Flow chart for Extraction Process	27
5.1	Different images used in Experiment	30
5.2	Results produced at different stages using Lena image	31
5.3	(a) Watermarked image produced after Affine Attack (b) Extracted Watermark when CT is used for decomposition on Affine attack	33
5.4	(a) Watermarked image after Affine Attack (b) Extracted Watermark when RT is used on Affine attack	33
5.5	(a) Watermarked image after Contrast Enhancement (b) Ex- tracted Watermark after applying Contrast Enhancement at- tack on CT	34

5.6	(a) Watermarked image after Contrast Enhancement (b) Extracted Watermark after applying Contrast Enhancement attack on RT	34
5.7	(a) Watermarked image after Gaussian Noise (b) Extracted Watermark after apply CT on Gaussian attack	35
5.8	(a) Watermarked image after Gaussian Noise (b) Extracted Watermark after applying additive Gaussian Noise Attack when RT is used for decomposition	35
5.9	(a) Watermarked image after Histogram Attack (b) Extracted Watermark after applying Histogram Attack when Curvelet Transform is used for decomposition	36
5.10	(a) Watermarked image after Histogram Attack (b) Extracted Watermark after applying Histogram Attack when Ridgelet Transform is used for decomposition	36
5.11	(a) Watermarked image after Multiplicative Speckle Noise (b) Extracted Watermark after applying Multiplicative Speckle Noise Attack when Curvelet Transform is used for decomposition	37
5.12	(a) Watermarked image after Multiplicative Speckle Noise (b) Extracted Watermark after applying Multiplicative Speckle Noise Attack when Ridgelet Transform is used for decomposition	37

5.13	(a) Watermarked image after Rotation (b) Extracted Watermark after applying Rotation Attack when Curvelet Transform is used for decomposition	38
5.14	(a) Watermarked image after Rotation (b) Extracted Watermark after applying Rotation Attack when Ridgelet Transform is used for decomposition	38
5.15	(a) Watermarked image after Salt and Pepper (b) Extracted Watermark after applying Salt and Pepper Noise Attack when Curvelet Transform is used for decomposition	39
5.16	(a) Watermarked image after Salt and Pepper (b) Extracted Watermark after applying Salt and Pepper Noise Attack when Ridgelet Transform is used for decomposition	39
5.17	(a) Watermarked image after Sharpening (b) Extracted Watermark after applying Sharpening Attack when Curvelet Transform is used for decomposition	40
5.18	(a) Watermarked image after Sharpening (b) Extracted Watermark after applying Sharpening Attack when Ridgelet Transform is used for decomposition	40
5.19	(a) Watermarked image after X-Shear (b) Extracted Watermark after applying X-Shear Attack when Curvelet Transform is used for decomposition	41
5.20	(a) Watermarked image after X-Shear (b) Extracted Watermark after applying X-Shear Attack when Ridgelet Transform is used for decomposition	41

5.21	(a) Watermarked image after Y-Shear (b) Extracted Watermark after applying Y-Shear Attack when Curvelet Transform is used for decomposition	42
5.22	(a) Watermarked image after Y-Shear (b) Extracted Watermark after applying Y-Shear Attack when Ridgelet Transform is used for decomposition	42
5.23	Values of <i>PSNR</i> for Extracted Watermark after Attacks on Lena image	44
5.24	Values of <i>NC</i> for Extracted Watermark after Attacks on Lena image	45
5.25	Values of <i>PSNR</i> for Extracted Watermark after Attacks on Peppers image	46
5.26	<i>NC</i> values for Extracted Watermark after Attacks on Peppers image	46
5.27	Values of <i>PSNR</i> for Extracted Watermark after Attacks on Barbara image	47
5.28	<i>NC</i> values for Extracted Watermark after Attacks on Barbara image	48
5.29	Value of <i>PSNR</i> for Extracted Watermark after Attacks on Baboon image	49
5.30	<i>NC</i> values for Extracted Watermark after Attacks on Baboon image	49

List of Tables

5.1	Values of <i>PSNR</i> and <i>NC</i> for different attacks for Lena image	43
5.2	<i>PSNR</i> and <i>NC</i> values at different attacks for Peppers image	45
5.3	Values of <i>PSNR</i> and <i>NC</i> for Barbara image for different attacks	47
5.4	The values of <i>PSNR</i> and <i>NC</i> for Baboon image for different attacks	48

List of Abbreviations

<i>AT</i>	Arnold Transform
<i>CT</i>	Curvelet Transform
<i>DCT</i>	Discrete Cosine Transform
<i>DFT</i>	Discrete Fourier Transform
<i>DIBR</i>	Depth Image Based Rendering
<i>DOST</i>	Discrete Orthogonal Stockwell Transform
<i>DWT</i>	Discrete Wavelet Transform
<i>HSI</i>	Hue Saturation Intensity
<i>IRT</i>	Inverse Ridgelet Transform
<i>NC</i>	Normalized Correlation
<i>NMF</i>	Non-negative Matrix Factorization
<i>PC</i>	Principal Component
<i>PCA</i>	Principal Component Analysis
<i>PSNR</i>	Peak Signal to Noise Ratio
<i>RGB</i>	Red Green Blue
<i>RPCA</i>	Robust Principal Component Analysis
<i>RT</i>	Ridgelet Transform
<i>SLT</i>	Slant Transform
<i>SVD</i>	Singular Value Decomposition

Chapter 1

Introduction

1.1 History of Hiding Data

From the beginning of development, to the extremely interacted citizens that we living in currently, communication has always been a fundamental major piece of our reality. Approaches of communication now a days comprise communication of radio, telephone, network and mobile. Every one of these strategies and methods of correspondence have had a critical impact of our lives, yet during past years, network communication, specifically over Internet has appeared as the greatest commanding communication with an overwhelming effect in our lives. By the development in the technology, unlawful procedures in digital means have become easy. Therefore, protection of digital contents has turn out to be a significant matter. Different types of approaches are used for this protection [1].

Cryptography, Steganography and Watermarking are basic techniques which are mainly used for data security. Crypto means secret writing whereas stego means cover writing. Cryptography is process of sending message in

distinct form so that only receiver can read the message by removing disguise. Disguised message is cipher text where sending message is plain text. The way of conversion of plain text to cipher text is called encryption and vice versa is called decryption. The method of transmitting a data through a carrier along with hiding, it is called steganography. In addition to the sender and recipient, no one knows the existence of the message, so it protects data from unauthorized or unwanted visions.

Watermarking is the process defined as hiding digital information into carrier signal. It is not necessary that hidden information contains a relation to the carrier signal. It can probably be used for authenticity or integrity of carrier signal or for showing its owners identity. Majorly, it's used is in tracing of copyright infringements and for banknote authentication. It is a type of marker covertly embedded in a signal which is noise tolerant. For example, an image, video or audio data. It can also be used as an application in identifying the one who owns the copyright of given signal.

1.1.1 General Framework of Watermarking

Watermarking is a process which involves embedding of watermark into a multimedia object in a particular way so that to make an assertion about the object. The object can either be an image, audio or video. An indication of digital watermark can be a seen from the seal that is placed on an image for identification of copyright. Although, the watermark can even contain some more information like identity of the particular purchaser.

A watermarking technique generally contains three parts:

- i Watermark: It is a secret data which is to be embedded in the digital medium. It can be text, image, audio *etc.*
- ii Embedding Algorithm: It is a process embedding the watermark in a cover medium, to produce the watermarked medium. A general embedding process is shown in Figure 1.1.

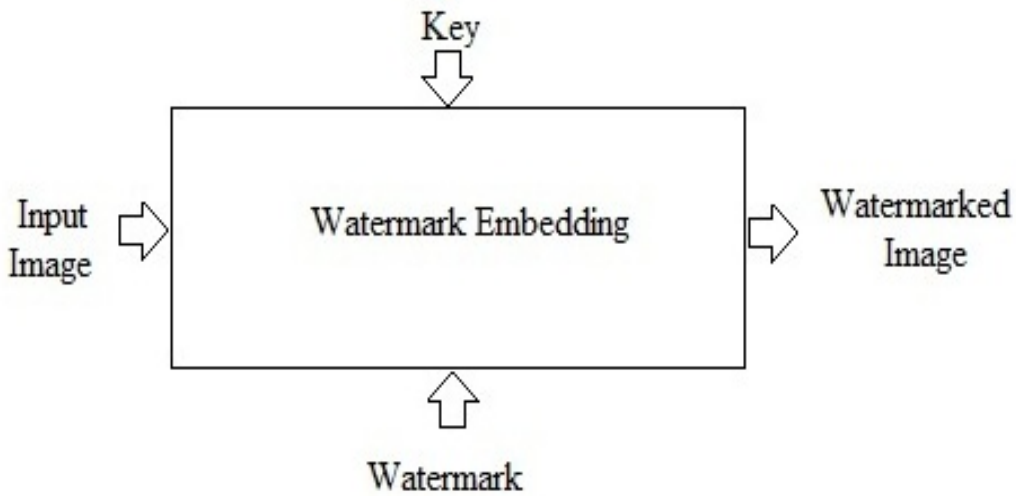


Figure 1.1: General Watermark Embedding Framework

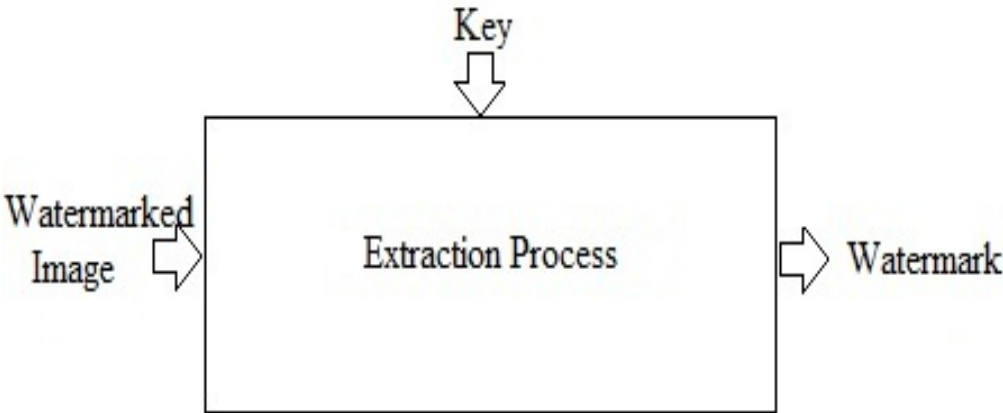


Figure 1.2: General Watermark Extraction Framework

iii Extraction Algorithm: It is a process which is applied to watermarked medium to extract the watermark from it, as shown in Figure 1.2.

1.1.2 Different types of Digital Watermarking

According to application point, it is divided into two types:

- i The one is source based in which there can be used of watermark for authentication and determination of tampered data or image which is received.
- ii The second is destination based where identification of particular buyer is done by giving a unique watermark to each distributed copy. This can also be used in tracing of buyer, whenever there is chance of illegal reselling.

Various other types are:

- i Spacial Domain Approach: The record is straight inserted by amending the values of pixel of original image. Spatial domain approaches [2] are less difficult and not vigorous contrary to several assaults as no conversion is used in them.
- ii Frequency Domain Approach : In frequency domain approaches which set in the data by modulating the coefficients of an appropriately selected transform [3].

1.2 Fundamental Transforms used for Watermarking

There are various types of transforms which are used to detect watermark.

These are listed below:

1.2.1 Discrete Cosine Transform

Discrete Cosine Transform (*DCT*) is utilized for transforming the image linear to frequency domain. Image energy is focused in merely rare low frequency constituents of *DCT* which depends on the association into the information.

1.2.2 Discrete Wavelet Transform

Discrete Wavelet Transform (*DWT*) is based on wavelets concept which is localized in frequency and in time domain. *DWT* usage filters with diverse limit frequencies to examine an image on dissimilar resolutions. It is distributed over large number of low pass filters, to consider the low frequencies. It is also known as scaling function. The image is distributed over numeral high pass filters. It is known as wavelet functions used to examine the high frequencies.

1.2.3 Singular Value Decomposition

Factorization tool commonly used in order to extract algebraic features from various matrices is Singular Value Decomposition (*SVD*) [4]. There are many applications of *SVD* like image compression, Clustering a Mixture of Spherical Gaussians, Spectral Decomposition, *etc* . *SVD* of an image *A* is

assumed as subsequent in equation (1.1):

$$A = U \sum V^T = \sum_{i=1}^r u_i \sum v_i^T = u_1 \sum v_1^T + u_2 \sum v_2^T + \dots + u_r \sum v_r^T \quad (1.1)$$

$$U \times U^T = I, V \times V^T = I \quad (1.2)$$

$$I = USV^T \quad (1.3)$$

where U is a matrix of size $m \times m$ of left singular vectors.

S is the matrix which is diagonal with size $m \times n$. It contains values in decreasing order.

V is the matrix of size $n \times n$ having right singular vectors.

T is conjugate transpose of V .

1.2.4 Curvelet Transform

A multiscaling directional transform which permits an early optimal non-adaptive sparse representation of objects with edges is known as Curvelet Transform (CT). For instance CT has a sparse representation and deals with upgraded compression potentials, it similarly has improved denoise performances [5]. The CT have excessive directional anisotropy as well as sensitivity. Here occur two distinct CT procedures; Wrapping Transform (WT) and Unequispaced Fast Fourier Transform ($USFFT$). $USFFT$ usages a reduced four-sided grid slanted alongside the leading way of every curvelet. There is one this type of grid per scale and angle. WT usages as an al-

ternative a demolished rectangular grid associated through the image axes. Curvelet coefficient $c(j, l, k)$ can be represented as:

$$c(j, l, k) = \langle f, \varphi_{j,l,k} \rangle \quad (1.4)$$

where $j = 0, 1, 2, \dots$ is a measure constraint, $l = 0, 1, 2, \dots$ is coordination factor and $k = (k_1, k_2), k_1, k_2 \in U_j$ is a conversion factor. The waveform $\varphi_j(x)$ is demarcated by Fourier $\varphi_\Lambda = U_j(w)$.

1.2.5 Discrete Fourier Transform

Discrete Fourier Transform (*DFT*) is a famous mathematical process which converts the image from spatial domain into frequency domain. Let $f(x, y)$ characterizes an image of size $M \times N$, $x = 0, 1, 2, \dots, M-1$ and $y = 0, 1, 2, \dots, N-1$. The onward and converse *DFT* are specified in Eqs. (1.5) and (1.6):

$$F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi(ux/M+vy/N)} = R(u, v) + jI(u, v) \quad (1.5)$$

$$f(x, y) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F(u, v) e^{j2\pi(ux/M+vy/N)} \quad (1.6)$$

where $F(u, v)$ is *DFT* factor, $v = 0, 1, 2, \dots, N-1$ and $u = 0, 1, 2, \dots, M-1$. The two further factors $I(u, v)$ and $R(u, v)$ represents imaginary and real parts of Fourier.

Degree and stage comprise the minimum and the maximum extent of facts, correspondingly, regarding the image and deliver possible applicants for embedding watermark evidence.

1.2.6 Continuous Ridgelet Transform

The 2-D uninterrupted ridgelet change in R^2 could be stated for instance below [6]. It is preferred that a plane univariate task $\psi : R \rightarrow R$ with adequate deterioration in addition sustaining acceptability criteria.

$$\int |\hat{\psi}(\xi)|^2 / |\xi|^2 d\xi < \infty \quad (1.7)$$

Where, ψ has a disappearance mean $\int \psi(t) dt = 0$. It is supposed that is standardized so as to $\int |\psi(\xi)|^2 \xi^{-2} d\xi = 1$. On behalf of every $a > 0$, every $b \in R$ and every $\theta \in [0, 2\pi)$, the bivariate ridge. Its formulation is steady as single has a Parseval relation

$$\int |f(x)|^2 dx = \int_0^{2\pi} \int_{-\infty}^{\infty} \int_0^{\infty} |R_f(a, b, \theta)|^2 \frac{da}{a^3} db \frac{d\theta}{4\pi} \quad (1.8)$$

Therefore, far alike the Fourier or wavelet transforms, the individuality states information which individual may characterize an indiscriminate function as a uninterrupted superposition of ridgelets.

1.2.7 Contourlet Transform

The additional transform founded system is the Contourlet Transform, presented in [7]. It divides an assumed image in high in addition to low frequency sub bands via means of Laplacian Pyramid Decomposition (*LPD*) filter. Subsequently, guiding facts can be acquired by put on Directional Filter Banks (*DFB*) to band pass images. *DFB* is considered for signify the directional of high frequency mechanisms of an image. According to [8], wa-

termarking in the contourlet domain demonstrates improved strength contrary to a range of attacks and determines satisfactory hiddenness in contrast to wavelet domain watermarking. It is due to Contourlet which has greater ability in mining the directionality contours and edges of the image.

1.3 Attacks on Watermarking System

An attack is a process which misleads the detector of watermark. A watermarked entity is expected to be exposed to definite controlling procedures a fore it reaches the receiver. Common signal processing tasks for instance digital to analog conversion and vice versa, quantization, recompression, requantization, non linear and linear filtering, high and low pass filtering, Gaussian and non-Gaussian noise are communal operations. We categorize the attacks into four unlike kinds, such as cryptographic attacks, elimination and interference, protocol and geometric attacks. Also estimation based attack where approximations of each the watermark can be attained by stochastic approaches. Different types of attacks are performed which are listed below:

1.3.1 Affine Attack

Affine transformation is a linear mapping method which preserves points, planes and straight lines. After an affine transformation, the sets of parallel lines remain parallel. It is typically used to correct for geometric distortions or deformations that occur with non-ideal camera angles.

1.3.2 Contrast Enhancement Attack

In order to increase or decrease contrast, Contrast manipulations changes the range of values in an image.

1.3.3 Additive Gaussian Noise Attack

It contain a noise having *PDF* equal to normal distribution which is also known as Gaussian distribution. Gaussian random variable probability density function is:

$$p_G(z) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(z-\mu)^2}{2\sigma^2}} \quad (1.9)$$

1.3.4 Histogram Equalization Attack

For adjusting image intensities to enhance contrast, Histogram technique is used which results in distortion of content in original image if used as an attack on image.

1.3.5 Multiplicative Speckle Noise Attack

Speckle is a granular 'noise' that inherently exists in and degrades the active radar quality, medical ultrasound. The vast majority of surfaces, synthetic or natural, are extremely rough on the scale of the wavelength. Images obtained from these surfaces by coherent imaging systems such as laser, and ultrasound suffer from a common phenomenon called speckle.

1.3.6 Rotation Attack

Rotation attack involves rotation of the image by an angle in which both x and y direction shifts to same angle. By performing rotation attack at an angle, we can extract the watermark from cover image.

1.3.7 Salt and Pepper Noise Attack

This type of noise can be produce by sudden disturbances and sharpness in image signal. This noise is seen on images which are also called impulse noise.

1.3.8 Sharpening Attack for Contrast Variations

Sharpness is basically the contrast of various colors. In this attack, a quick transition from black to white looks sharp. Where different colors meet, images increase the contrast.

1.3.9 X-Shear Attack

Shear transformations produce a shape distortion in which X-shear produces a shearing along x that is proportional to y .

1.3.10 Y-Shearing Attack

Y-shear produces a shearing along y that is proportional to x . In this attack, image is flipped horizontally.

1.4 Characterstics of Watermarking

The watermarking characteristics are discussed below:

- i Unnoticeable: The invisible watermarks should be difficult to be noticed by the viewers. It should be imperceptible. In case, when signal is truly imperceptible, then lossy compression algorithm based on perceptual should eradicate such signal.
- ii Robustness: A watermark ought to be robust to those transformations which include *D/A* and *A/D* conversions, loss compression and common signal distortions. The survival of geometric distortions such as cropping, translation and scaling *etc* is important for images and video. Many says that if the placing of watermark is done in regions of image, robustness can be attained which are significant perceptually. But if the watermark is plated in perceptually insignificant regions of an image, it should be imperceptible.

Chapter 2

Literature Survey

In this chapter, the transform based watermarking techniques have been reviewed in detail.

2.1 *DWT-SVD* based Watermarking Techniques

Bhatnagar *et al.* [9] offered a watermarking scheme based on *DWT* and *SVD* where watermark is substituted as grey scale logo rather than noise type Gaussian. The insertion of watermark into image by modifying the image singular values with the help of watermark singular values.

Lu *et al.* [10] proposed a novel image watermark utilizing Non-negative Matrix Factorization (*NMF*) in *DWT*. Using *DWT*, cover image is transformed into subband coefficients then a pseudo irregular Gaussian watermark is inserted in the encoding process of host image using *NMF*.

Mishra *et al.* [11] proposed an improved watermark framework based on joining *SVD* and *DWT*. Using Multiple Scaling Factors (*MSF*), singular values of *LL3* subband elements of the cover image are modified. Using Firefly Algorithm, *MSF* is upgraded having a target which is gathering of robustness

and imperceptibility.

Jane *et al.* [12] introduced a non blind watermarking scheme based on *SVD* and *DWT*. Cover image is decomposed into sub groups (High Low (*HL*), High High (*HH*), Low Low (*LL*) and Low High (*LH*)), put *SVD* to *LL* band and adjust diagonal singular values with the watermark itself by scaling factor. In the end, *LL* band coefficients are constructed again with modified *SVD* values and apply inverse of *DWT* to acquire watermarked image.

Kumar *et al.* [13] presented a color image decoding and encoding procedure based on Discrete Orthogonal Stockwell Transform (*DOST*). *SVD* and *DWT* is utilized as a part of *DOST* with certain predefined parameters that enhanced the security of the scrambled images. The encoded images can't be unscrambled appropriately without the data of correct means and specific direction of strategy of wavelet sub bands.

Robust, blind and imperceptible watermarking framework to keep the copyright of *3D DIBR* images was proposed by Haj *et al.* [14]. The framework is based on hybrid *SVD* and *DWT* changes. Watermark bits at the sender side is hidden using chaos based process of embedding and removed blindly at the recipient side from left, right, center view.

2.2 SVD based Watermarking Schemes

Ming-Quan *et al.* [15] presented double procedures for *SVD* based scheme of watermarking. When watermark is embedded in *U* or *V* component of *SVD*, these procedures increase the robustness and visibility.

Mathew *et al.* [16] displayed the *SVD* based image watermarking frame-

work, to increase robustness of image. In the prescribed framework, U and D components are used for implanting watermark. Differentiating from other, SVD uses non fixed orthogonal bases.

Run *et al.* [17] presented a system that could resolve the vulnerabilities condition and false positive issue. Security is increased by using wavelet function. Focus of this scheme is robustness on various attacks.

Jia *et al.* [18] proposed a watermarking framework based on SVD for securing duplicate rights. This strategy has the accompanying focal points: i) color image is inserting as watermark ii) color image watermark is inserted into cover image by adjusting the connection among second and third components in each block of U matrix after SVD iii) overcome the problem of false positive detection.

2.3 Miscellaneous Watermarking Techniques

Jose *et al.* [19] proposed an extraordinary cross breed watermarking scheme using $DCT-DWT-SVD$. Before applying DCT , image is recorded. Using DWT , recorded image is decomposed into subbands. To embed watermark, SVD is applied to middle subband. This strategy can be utilized for copyright assurance.

Rahman *et al.* [20] displayed watermarking method using DWT , SVD and DCT that includes robustness with various watermarking frameworks Using zigzag sequence, the initial image is arranged and apply DWT on it. Every single high band LH , HH , HL are chosen and DCT and SVD applied on it. By modification of singular values, watermark is embeded in it and inverse

process of embedding process is extraction process.

Rani *et al.* [21] proposed two frameworks made on zero watermarking for copyright protection using *DWT* and *SVD*. Encryption of watermark with cover image is done by master and ownership share. Using classification of extracted features, share of master is generated. By using, master share and watermark, ownership share is generated. They reveal watermark, when both shares put together.

Rabizadeh *et al.* [22] proposed a strong and ideal multiplicative watermark indicator in contourlet domain using Bessel *K* Form. The optimum watermark finder as stated by the Likelihood ratio test has been suggested.

SVD and Hybrid *DCT*-Walsh transform was proposed by Natsu *et al.* [23]. Using *SVD* on column hybrid, transformed host image and watermark. Secondly, *SVD* on sorted column, transform the host image and watermark coefficients. Low frequency transform coefficients are used in both cases.

Tarif *et al.* [24] executed scheme of hiding to make sure security of biometric data in biometric system. Using threshold technique, iris vector and secret fingerprint are sparsely approximated and embedded in host *SLT-SVD* domain of image.

Mankar *et al.* [25] utilized curvelet transform to embed the secret data into a cover image. Versatile square based inserting in non-homogeneous districts of curvelet coefficients achieves enhanced subtlety. Visual quality of the image is evaluated utilizing *PSNR*, *SSIM* and *UQI*. Another commitment of their work incorporates another cover determination procedure grounded on image intricacy and spatial data.

Gafoor *et al.* [26] proposed a hybrid watermarking technique is proposed based on combination of Fast Curvelet Transform, Robust Principal Component Analysis (*RPCA*) and *SVD*. The Arnold Transform (*AT*) on gray-scale watermark image is used to improve the security and robustness. The processed watermark is added to the significant curvelet coefficients of the original image. The robustness of the proposed technique is tested against different geometric and image processing attacks.

Chapter 3

Problem Statement

3.1 Research Gaps

There are many research gaps which are determined as follows:

- i Effect of watermark scrambling on a provided watermark picture has been neglected by many of the existing researchers.
- ii The use of *RT* with *AT* and *RPCA* was not explored enough.
- iii Improvement in the Robustness and imperceptibility required.
- iv Some *SVD* based schemes are fully *SVD* based where some are hybridized with some transforms. For the enhancement of performance and security of images, hybridization is needed. Mostly *SVD* based algorithms are less resilient with attacks like Rotation, Sharpening, Affine, Shearing *etc.*

3.2 Problem Definition

The existing *DWT* based watermarking schemes which has lack of high capacity in embedded information and robustness from attacks. Because of the benefit of *DWT* ended other frequency transforms; it is the most frequently used frequency transform domain in digital watermarking. This transform is even widely used, yet the robustness of *DWT* based algorithms is attained by cooperating the size, the nature and the type of the watermark signal. Hence, the study of new transform based digital watermarking schemes to embed a watermark image into another image need to be explored. Additionally, A new scheme based upon *RT* and *CT* with additional (*RPCA*), *SVD* and (*AT*) has been planned. This technique associates the benefits of these transforms. This technique can support in satisfying the robustness and imperceptibility features of watermarking algorithm by enhancing the watermarked image quality and being robust against various attacks. Various kinds of multiple attacks will be measured to estimate the efficiency of the proposed method.

3.3 Objectives

We design a digital watermarking scheme which is situated on the transform domain where *RT* and *CT* has been used. The objective of choosing this domain is that, unlike other frequency transform domain, this domain is not a full frame domain, has spatial frequency locality and is robust towards an attacks of large range. The main objective of this thesis is to utilize and

enhance these features of the transform domain for digital watermarking.

The objective is to propose an efficient watermarking technique that can:

- i Enhance the security of the watermark.
- ii Increase robustness to various kinds of image processing attacks.

Chapter 4

Proposed Technique

4.1 Introduction

In this section, Ridgelet Transform, *RPCA* and *AT* used in the proposed technique has been discussed in details. Embedding and extraction algorithms of the proposed technique have been discussed in the last Subsection of the Chapter.

4.1.1 Ridgelet Transform

Wavelets are being utilized professionally to characterize the point data, *i.e.* a zero dimensional independence is accomplished from it, and for instance detaching in intelligibility close to the edge, anyway for complex data around the equality alongside the edge isn't achieved. Thusly, the thought *RT* is progress in [27] to characterize the independences along the line. It changes the point uniqueness into line uniqueness by the Radon change and further exhibiting point peculiarity by put on *DWT* on the majority of the Radon projections. Ridgelet change is directional touchy, insofar as edge

data in the image.

4.1.2 Robust Principal Component Analysis

Assuming the information framework D is made out of the low rank background L and sparse foreground S , the best approach to fragment S and L from D is to tackle the accompanying *RPCA* issue which is characterized as

$$\min_{L,S} \text{Rank}(L) + \lambda \|S\|_0 \text{ s.t. } D = L + S \quad (4.1)$$

where $\text{Rank}(L)$ signifies the rank of L and $\|S\|_0$ signifies to the non-zero components in S . The adjust parameter λ is used to measure the commitments of L (low-rank property) and S (sparse property) in limiting the target work. The measurements of the info network are utilized to compute λ which is characterized as

$$\lambda = 1/\sqrt{\max(m, n)} \quad (4.2)$$

The adjust parameter λ has an essential influence in fragmenting S and L as we found in tests. A major λ is advantage to the inadequate property of S . Commotion is extraordinarily smothered in the portioning comes about at the cost of losing halfway protest cover. Then again, a little λ is advantage to the low-rank property of L . Protest veil can be totally safeguarded with much commotion.

4.1.3 Arnold Transform

AT is an technique of image scrambling that is used to encrypt and decrypt image data.

Arnold Scrambling Algorithm

Arnold scrambling algorithm has simplicity and periodicity as its features. Figure 4.3 shows the change of point (x, y) in the unit square altered to another point (X', Y') is:

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{1} \quad (4.3)$$

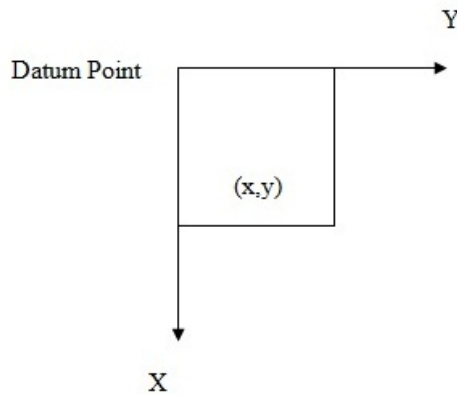


Figure 4.1: Distribution of Image Coordinates

This change is known as 2-D Arnold scrambling. To be point by point to the computerized image, we required to adjust the 2-dimensional Arnold scrambling of mod 1 to mod N .

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (4.4)$$

It is mod N which is Arnold scrambling. For (x, y) belongs to $(1, 2, 3, \dots, N-1)$. N represents order of digital image. The change of mod 2 is framework A. (x, y) T in the privilege is the info, (X', Y') in the left is the yield, as the reaction, iterative strategy that can sort out as the subsequent:

$$P_{xy}^{n+1} = AP_{xy} \text{ mod } N \quad (4.5)$$

$$P_{xy}^n = x, y^T \quad (4.6)$$

Where n characterize the period of cycles, $n = 0, 1, 2, \dots$. Image data (for instance the dim value) with the reserve of the discrete cross section for transplantation, they delivered another image after the greater part of the purposes of the first picture have been explored [28], [29].

4.2 Proposed Technique

The main objective of this work is to increase the robustness of the watermarking technique with the help of *RT*, *RPCA*, *AT* and *SVD* algorithms. Firstly, the host image is converted into *HSI* color space. After that, Intensity channel is processed through *RPCA* which is a statistical method frequently used with multivariate data. To decrease the dimensionality of a data set consisting of large amount of variables with many being correlated while still contains many variations as in the data set Principal Component Analysis (*PCA*) is used. This is attained by transforming the data into new variables, which are called Principal Components (*PC*) that are uncorrelated

and order in such a way that starting few components contain many variation of the original data set. *PCs* give a sparser representation of the data after reducing to these new variables. Instead of normal *PCA*, *RPCA* is used because it is able to choose principal components more reliably than normal *PCA* and is also faster in speed. Then, with the help of using *RT*, *PCA* coefficients are further decomposed into bands and sub bands. After that, watermark image is read and resized and encrypted through *AT* to increase data security. Then watermark is merged into host image with the application of *SVD* technique. Finally, the performance of proposed technique is analyzed and evaluated to find out the results of analysis. Performance parameters are taken to validate the research work.

4.2.1 Algorithm for Embedding Watermark

The algorithm for embedding process has been briefed below and is displayed in Figure 4.2

Step 1: Convert *RGB* image to Hue Saturation Intensity (*HSI*) color space.

Step 2: Apply Robust *PCA* to intensity channel of *HSI* space to get the low rank *L* matrix.

Step 3: Perform 2-*D RT* on Low rank *L* matrix at level 1 of cover image.

Step 4: Next extract the low frequency components at level one and apply *SVD* on it.

Step 5: Read the watermark and resize it the desired size with respect to the size of low frequency components obtained for host image.

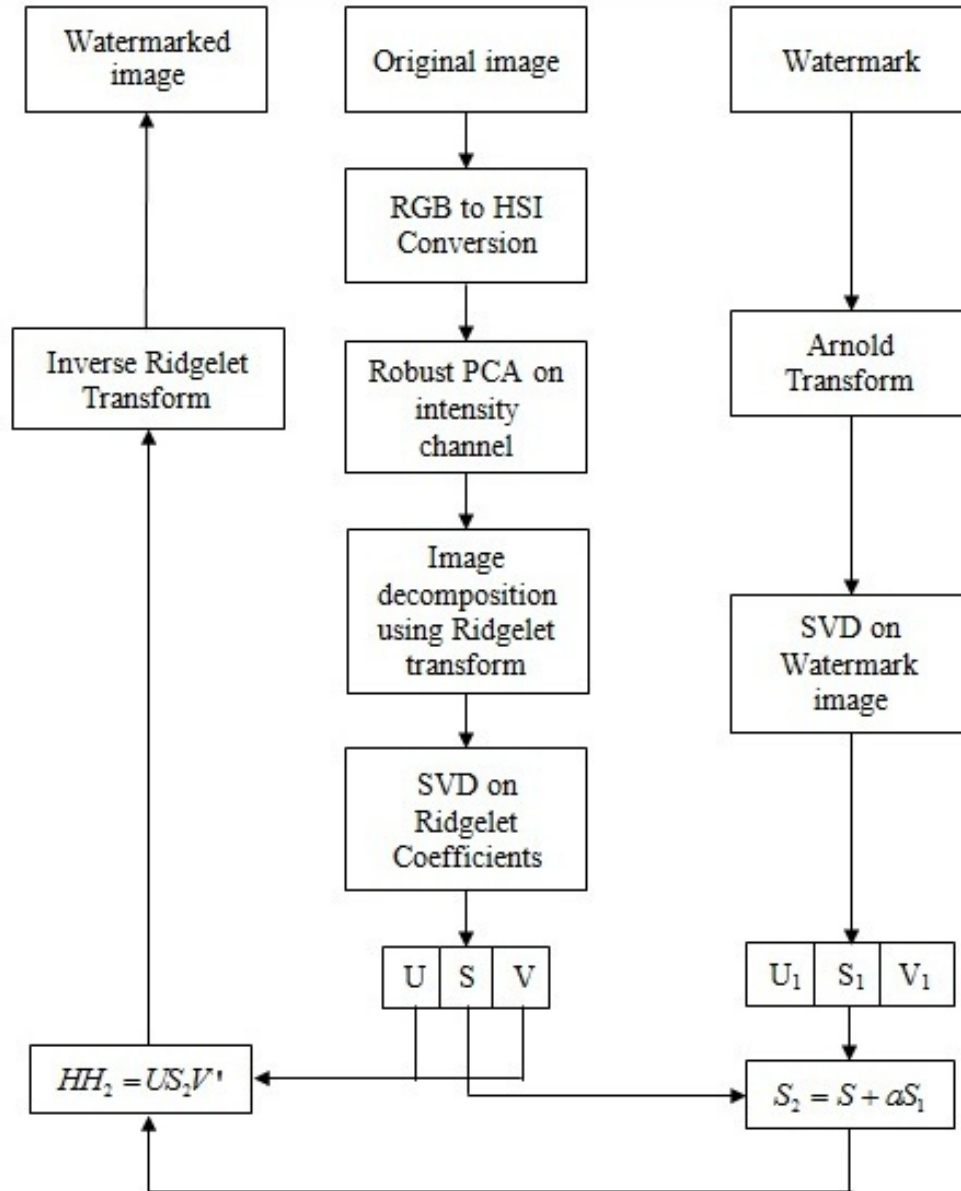


Figure 4.2: Flow chart for the Embedding Process

Step 6: Apply AT to watermark image in order to scramble the pixel values.

Step 7: Obtain SVD of scrambled watermark image.

Step 8: Merge the diagonal matrix S of watermark SVD with S component of SVD host image.

Step 9: Perform 2-D Inverse Ridgelet transform (IRT) to get the watermarked

intensity component.

Step 10: Convert *HSI* components of watermarked image to *RGB* color space.

4.2.2 Algorithm for Extraction Process

Extraction process is carried out in reverse way in which watermarked image has been made as shown in Figure 4.3. These steps are as follow:

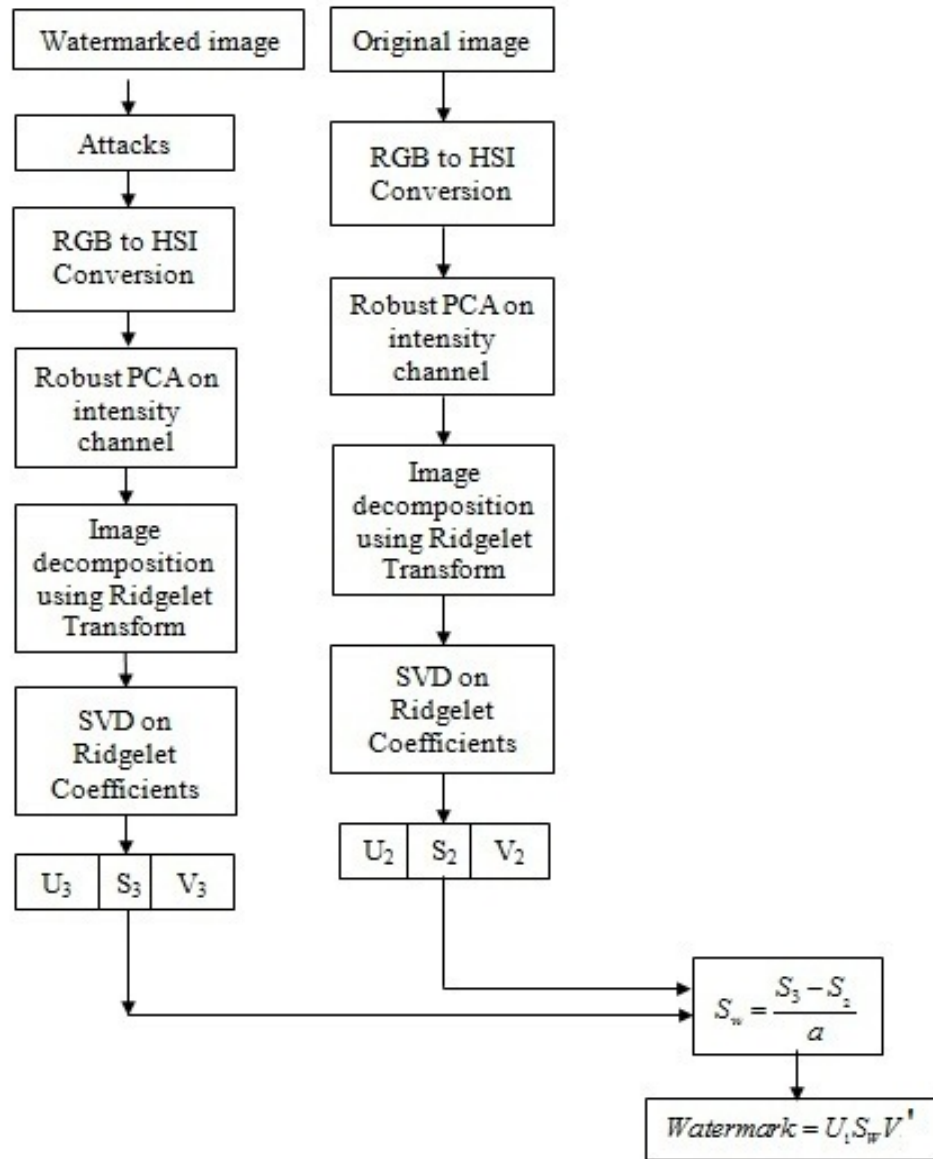


Figure 4.3: Flow chart for Extraction Process

Step 1: Take watermarked image which is obtained by applying attack on it and the original host image. Perform the following steps individually.

i Convert cover image to *HSI* color space.

ii Apply Robust *PCA* to intensity channel of *HSI* space to get the low rank *L* matrix.

iii Perform 2-D *RT* on Low rank *L* matrix at level 1 of cover image.

iv Next extract the low frequency components at level one and apply *SVD* on it.

Step 2: Taking *S* components of *SVD* implemented outputs for both images get the new *S* component by subtraction of these two values.

Step 3: Perform matrices multiplication for *U* component of watermarked image, new *S* component received in previous step and *V* component of watermarked image which results in extracted watermark.

Step 4: Evaluate *PSNR* and *NC* values of recovered watermark.

Chapter 5

Experimental Results and Analysis

5.1 Experimental Results

Proposed technique is implemented using MATLAB 2016. In this experiment, we have considered four colored images named as Lena, Peppers, Barbara and Baboon and are shown in Figure 5.1. Watermark considered in this experiment is of size 128×128 .

The results produced at different stages by the presented algorithm shown in visual images in the section below. Here, Lena image has been selected for displaying the results in detail, whereas performance evaluation by quality metrics *PSNR* and *NC* for peppers, Barbara and Baboon images has been represented in the graphical and tabular form. Figure 5.2(a) shows the result when *HSI* is applied on cover image and apply *RPCA* to intensity channel of *HSI* to get low matrix *L*. When Curvelet Transform is used on watermarked image Figure 5.2(b) takeout as output. Watermarked image produced in *RGB* color space using Curvelet shows in Figure 5.2(c). Result after Ridgelet is used shown in Figure 5.2(d).



(a) Lena Image



(b) Peppers Image



(c) Barbara Image



(d) Baboon Image



(e) Watermark Image

Figure 5.1: Different images used in Experiment



(a) Rank matrix L produced after Robust PCA implementation on Lena Image



(b) Watermarked image produced in Intensity channel using Curvelet Transform



(c) Watermarked image produced in RGB color space using Curvelet Transform



(d) Watermarked image produced in RGB color space using Ridgelet Transform

Figure 5.2: Results produced at different stages using Lena image

5.2 Quality Parameters

Quality parameters considered in this work are Peak Signal to Noise Ratio ($PSNR$) and Normalized Correlation (NC). $PSNR$ is the ratio between the maximum possible power of a signal and the power of corrupting noise. It is represented as:

$$PSNR = 10 \log_{10} \frac{(2^d - 1)^2 WH}{\sum_{i=1}^W \sum_{j=1}^H (p[i, j] - p'[i, j])^2} \quad (5.1)$$

where d is the bit depth of pixel, W the image width, H the image height, and $p[i, j]$, $p'[i, j]$ is the i th-row j th-column pixel in the original and watermarked image respectively.

Another method to check the degradation in original and extracted watermark is the NC coefficient which measures the robustness of the algorithm from the attacks. It is defined as the ratio between the net sum of the multiply of the corresponding pixel values of original and extracted watermark. It is calculated as:

$$NC = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 (y_i - \bar{y})^2}} \quad (5.2)$$

5.3 Effect of Attacks

The extraction process is applied to extract the watermark after various attacks applied on the extracted image. For both Curvelet and Ridgelet based watermarking methods, the effect of different attacks has been provided.

5.3.1 Affine Attack

Watermark image after Affine Attack shows in Figure 5.3 (a) and Figure 5.3 (b) shows Extracted Watermark after applying Affine attack when Curvelet transform is used for decomposition. As seen the extracted watermark from curvelet is not visible and has low $PSNR$ and NC *i.e.* 9.9 and 0.46 respectively whereas Figures 5.4(a) and(b) show the result when RT is used. Here the extracted watermark image is shown visible with NC 0.93, which shows ridgelet shows better result on Affine attack.

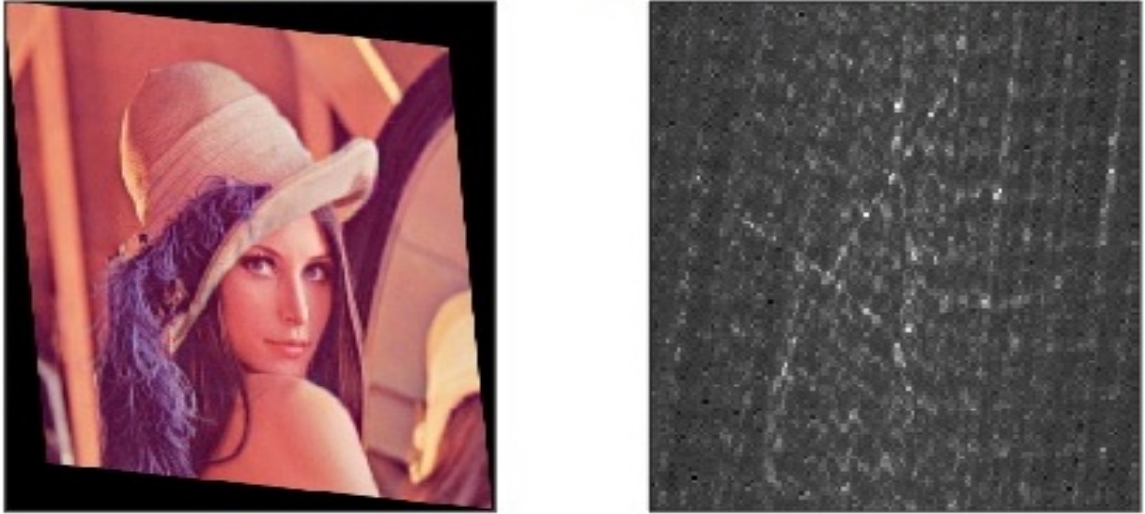


Figure 5.3: (a) Watermarked image produced after Affine Attack (b) Extracted Watermark when *CT* is used for decomposition on Affine attack

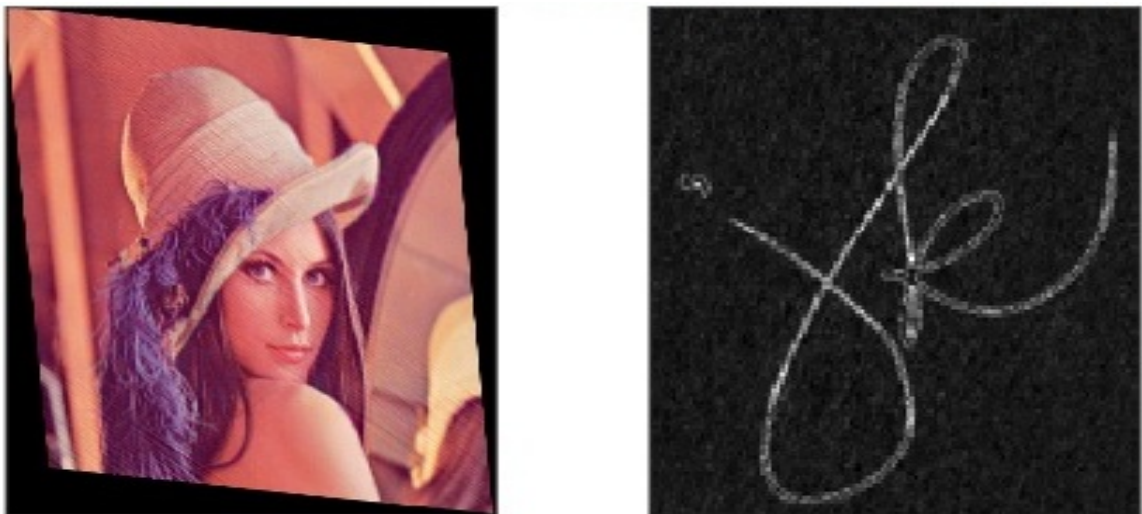


Figure 5.4: (a) Watermarked image after Affine Attack (b) Extracted Watermark when *RT* is used on Affine attack

5.3.2 Contrast Enhancement Attack

When *CT* is used on Watermarked image as shown in Figure 5.5, it results *PSNR* 18.20 and *NC* 0.71 whereas *RT* (shows in Figure 5.6) gives us better values of both *PSNR* and *NC* as 38.06 and 1. So it is clear from the values that *RT* gives us more robustness.

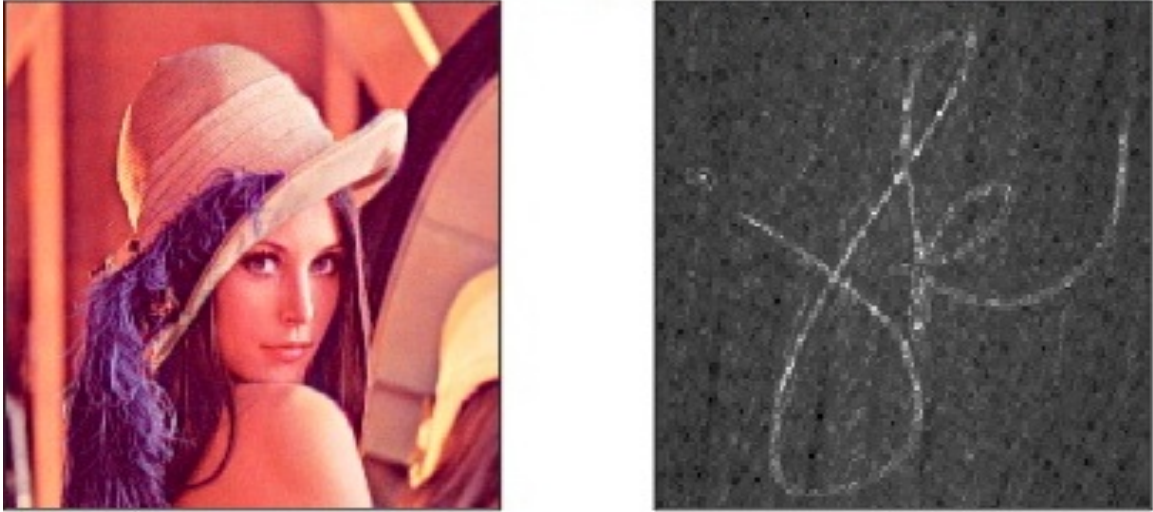


Figure 5.5: (a) Watermarked image after Contrast Enhancement (b) Extracted Watermark after applying Contrast Enhancement attack on *CT*



Figure 5.6: (a) Watermarked image after Contrast Enhancement (b) Extracted Watermark after applying Contrast Enhancement attack on *RT*

5.3.3 Additive Gaussian Noise Attack

Against Gaussian noise attack, the robustness using *CT* is shown in Figure 5.7 and using *RT* shown in Figure 5.8. This is clear from the readability of the extracted watermark (Figure 5.8 (b)) and the high value of the *NC* (0.98) that robustness of *RT* against Gaussian noise is acceptable.



Figure 5.7: (a) Watermarked image after Gaussian Noise (b) Extracted Watermark after apply *CT* on Gaussian attack



Figure 5.8: (a) Watermarked image after Gaussian Noise (b) Extracted Watermark after applying additive Gaussian Noise Attack when *RT* is used for decomposition

5.3.4 Histogram Equalization Attack

Figures 5.9 and 5.10 show the results after applying Histogram attack using both *CT* and *RT* respectively. *PSNR* and *NC* using *CT* is 55.67 and 0.51 resp. whereas using *RT* the value of *PSNR* is 10.65 and *NC* is 0.99. Notice the failure value of *PSNR* in *RT*, so in this case both *CT* and *RT* gives better

result CT in $PSNR$ and RT in NC .



Figure 5.9: (a) Watermarked image after Histogram Attack (b) Extracted Watermark after applying Histogram Attack when Curvelet Transform is used for decomposition



Figure 5.10: (a) Watermarked image after Histogram Attack (b) Extracted Watermark after applying Histogram Attack when Ridgelet Transform is used for decomposition

5.3.5 Multiplicative Speckle Noise Attack

CT degrades the quality when we extract watermark from it as shown in Figure 5.11. RT gives more clear (shown in Figure 5.12) and accurate NC

value *i.e.* 0.97. So *RT* is extremely robust against this attack.

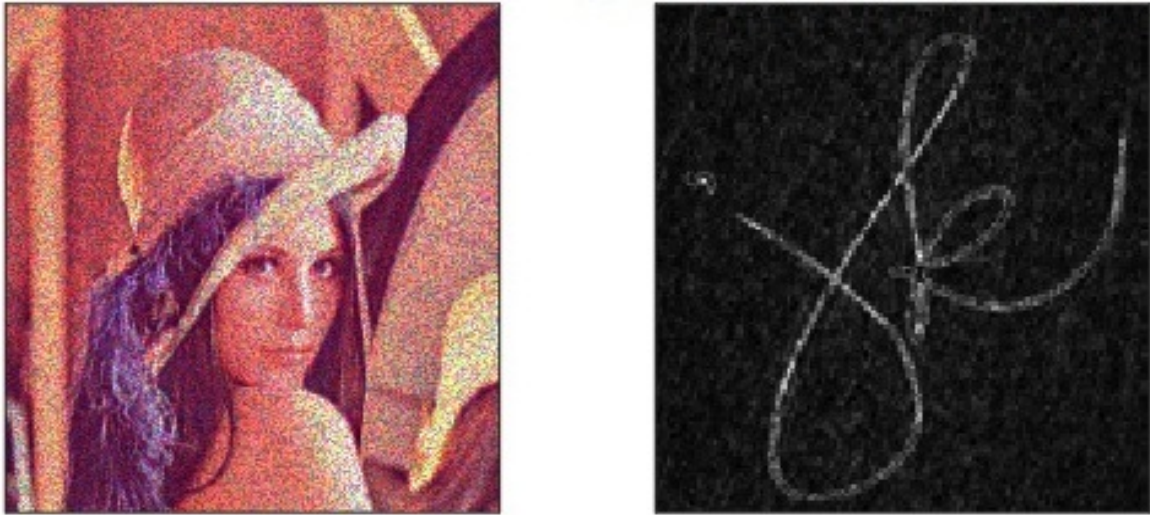


Figure 5.11: (a) Watermarked image after Multiplicative Speckle Noise (b) Extracted Watermark after applying Multiplicative Speckle Noise Attack when Curvelet Transform is used for decomposition

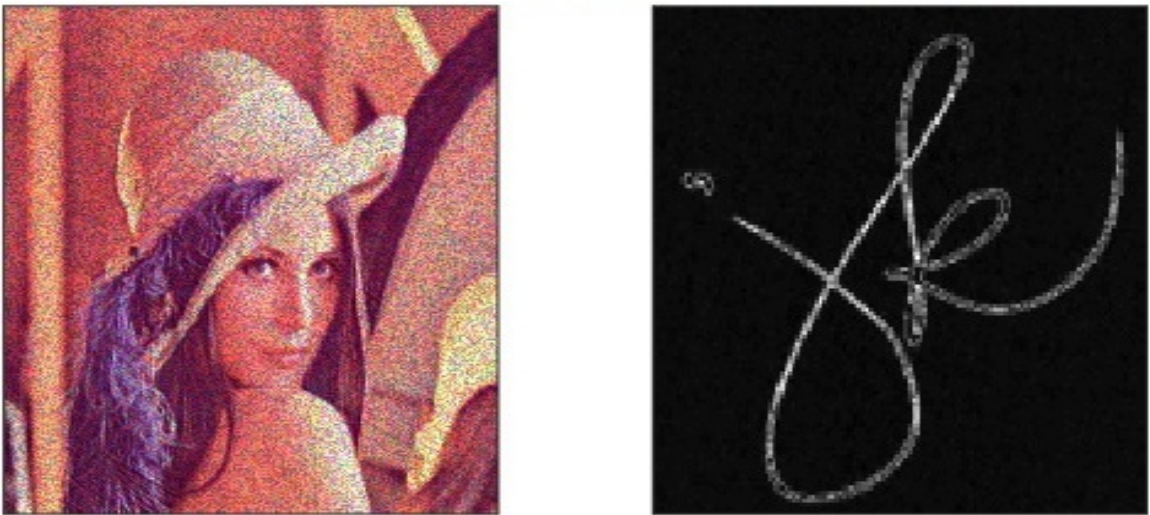


Figure 5.12: (a) Watermarked image after Multiplicative Speckle Noise (b) Extracted Watermark after applying Multiplicative Speckle Noise Attack when Ridgelet Transform is used for decomposition

5.3.6 Rotation Attack

The results for rotation attack using *RT* by 30 degrees shows in Figure 5.14. Figure 5.14 (a) shows the rotated watermarked image, (b) extracted watermark. As *NC* is 0.85 using *RT* and 0.55 using *CT*, proposed *RT* algorithm is extremely robust against rotation attacks than *CT*.

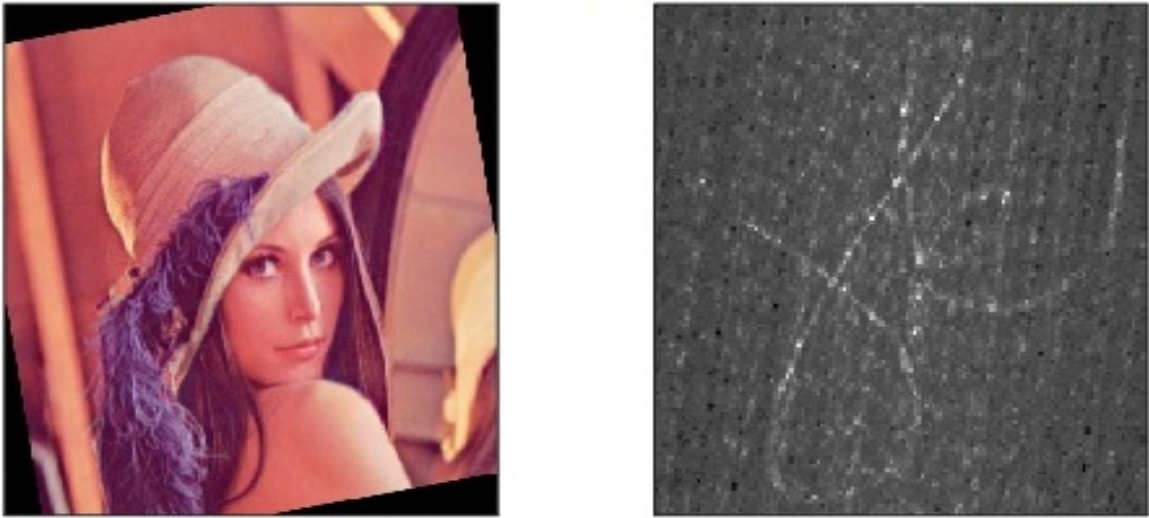


Figure 5.13: (a) Watermarked image after Rotation (b) Extracted Watermark after applying Rotation Attack when Curvelet Transform is used for decomposition



Figure 5.14: (a) Watermarked image after Rotation (b) Extracted Watermark after applying Rotation Attack when Ridgelet Transform is used for decomposition

5.3.7 Salt and Pepper Noise Attack

Disturbance in images can be produced using this attack. Here, Ridgelet shows better result with NC 0.99 and image clarity can be seen in Figure 5.16.

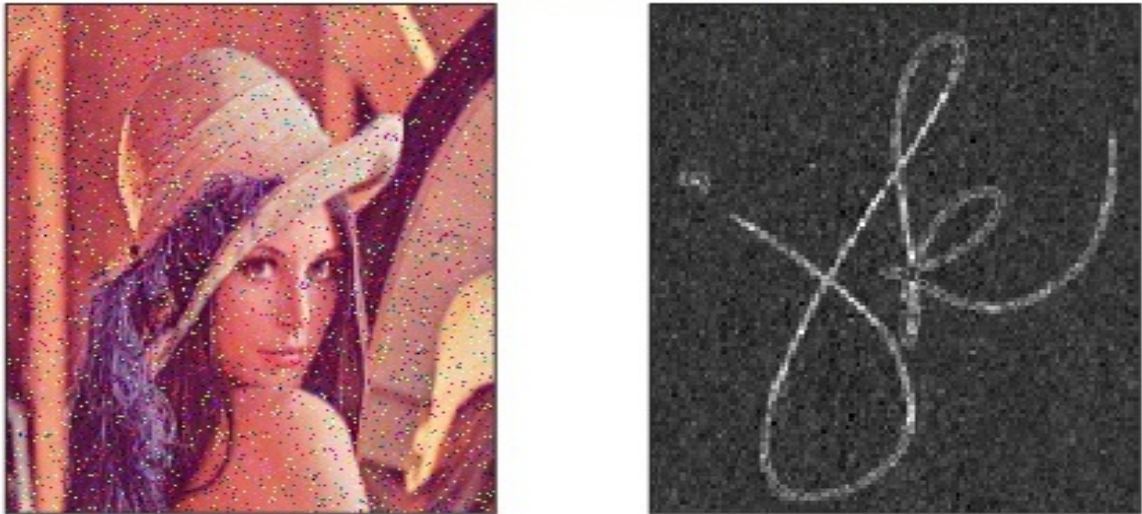


Figure 5.15: (a) Watermarked image after Salt and Pepper (b) Extracted Watermark after applying Salt and Pepper Noise Attack when Curvelet Transform is used for decomposition



Figure 5.16: (a) Watermarked image after Salt and Pepper (b) Extracted Watermark after applying Salt and Pepper Noise Attack when Ridgelet Transform is used for decomposition

5.3.8 Sharpening Attack for Contrast Variations

Using *RT* the extracted watermark is more sharpen (as shown in Figure 5.18) than *CT* with *NC* 0.98. This shows that *RT* is more reliable in this attack.



Figure 5.17: (a) Watermarked image after Sharpening (b) Extracted Watermark after applying Sharpening Attack when Curvelet Transform is used for decomposition



Figure 5.18: (a) Watermarked image after Sharpening (b) Extracted Watermark after applying Sharpening Attack when Ridgelet Transform is used for decomposition

5.3.9 X-Shear Attack

X-Shear Attack gives $PSNR$ 14.35 and NC 0.45 when CT is used, also the extracted watermark does not give visible result. When RT is applied, $PSNR$ is 37.20 and NC is 0.97 which gives us visible extracted watermark. So Figure 5.20 shows RT is more robust.

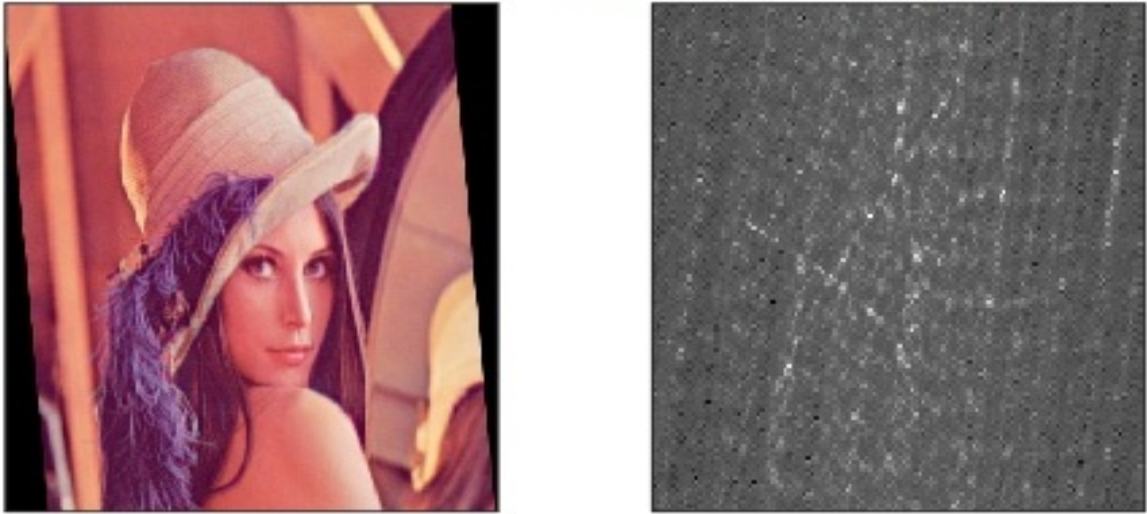


Figure 5.19: (a) Watermarked image after X-Shear (b) Extracted Watermark after applying X-Shear Attack when Curvelet Transform is used for decomposition



Figure 5.20: (a) Watermarked image after X-Shear (b) Extracted Watermark after applying X-Shear Attack when Ridgelet Transform is used for decomposition

5.3.10 Y-Shearing Attack

Y-Shear Attack gives $PSNR$ 16.44 and NC 0.51 when CT is used, in this the extracted watermark does not give visible result. When RT is applied, $PSNR$ gives 37.09 and 0.95 NC which gives us visible extracted watermark. So Figure 5.22 shows RT is more robust.

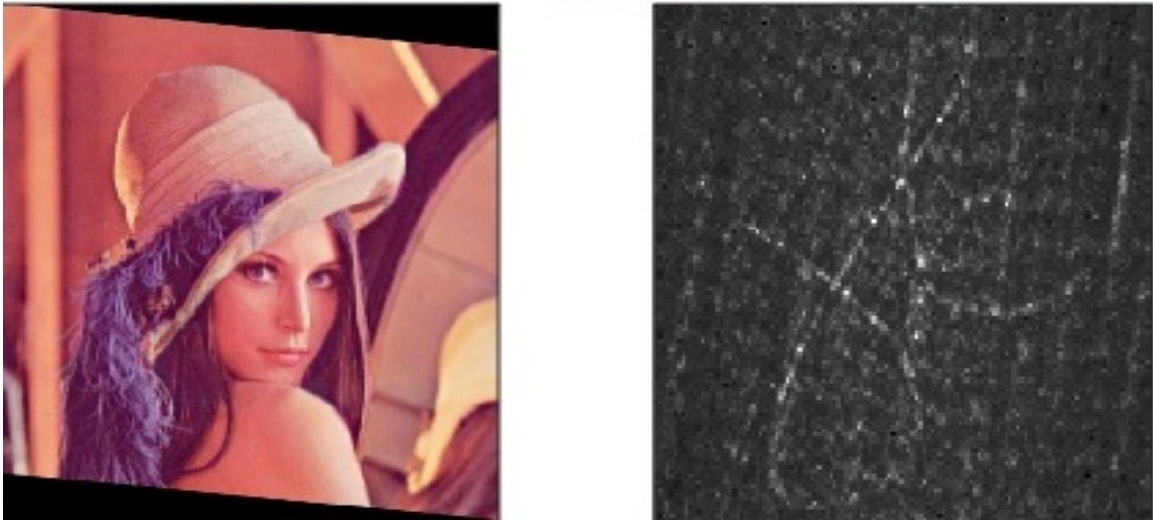


Figure 5.21: (a) Watermarked image after Y-Shear (b) Extracted Watermark after applying Y-Shear Attack when Curvelet Transform is used for decomposition



Figure 5.22: (a) Watermarked image after Y-Shear (b) Extracted Watermark after applying Y-Shear Attack when Ridgelet Transform is used for decomposition

5.4 Analysis of the Results

The results for quality assessment on different images have been given below:

In Table 5.1 we compare the results of *PSNR* and *NC* between existing Curvelet approach and proposed Ridgelet Transform. Here in proposed approach, the value of *NC* lies between 0.8-1.0 which shows the image quality is good and is much cleared in *RT* as shown in Figure 5.23 and 5.24.

Table 5.1: Values of *PSNR* and *NC* for different attacks for Lena image

Lena Image	Curvelet Transform[26]		Ridgelet Transform	
Attack Name	<i>PSNR</i>	<i>NC</i>	<i>PSNR</i>	<i>NC</i>
Affine Attack	9.9	0.46	36.92	0.93
Contrast Enhancement Attack	18.20	0.71	38.06	1.00
Additive Gaussian Attack	30.28	0.90	38.34	0.98
Histogram Attack	55.67	0.51	10.65	0.99
Multiplicative Speckle Noise Attack	24.91	0.84	38.50	0.97
Rotation Attack	13.97	0.55	36.60	0.85
Salt and Pepper noise Attack	41.01	0.85	37.57	0.99
Sharpening Attack	44.63	0.94	38.64	0.98
X-Shearing Attack	14.35	0.45	37.20	0.97
Y-Shearing Attack	16.44	0.51	37.09	0.95

In Table 5.2 comparison of results of *NC* and *PSNR* using Curvelet and Ridgelet Transform in Peppers image . Here the value of *NC* lies between 0.7-1.0 which shows that the quality of image is better and is cleared in *RT* as shown in Figure 5.25 and 5.26. Also the *PSNR* value is good using *RT* as compared to Curvelet except in Salt and Pepper noise attack and Sharpening attack.

In Table 5.3 results are shown of *NC* and *PSNR* when Curvelet and

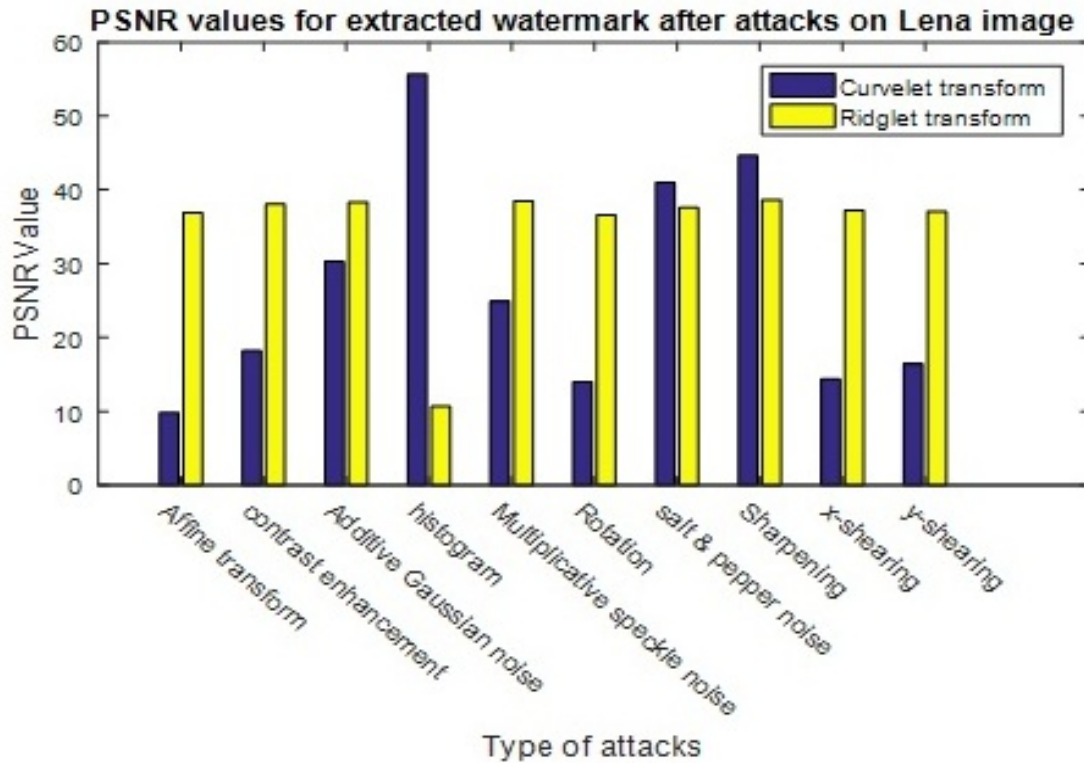


Figure 5.23: Values of *PSNR* for Extracted Watermark after Attacks on Lena image

Ridgelet Transform in Barbara image is used. Here the value of *NC* lies between 0.7-1.0 that means the image quality is better and is visible in *RT* as shown in Figure 5.27 and 5.28 and *PSNR* value is better when *RT* is used as compared to Curvelet except in Salt and Pepper noise attack and Sharpening attack.

Table 5.4 shows the result of *PSNR* and *NC* on Curvelet and Ridgelet Transform. It shows that Ridgelet is better mostly in all cases to Curvelet as shown in Figures 5.29 and 5.30.

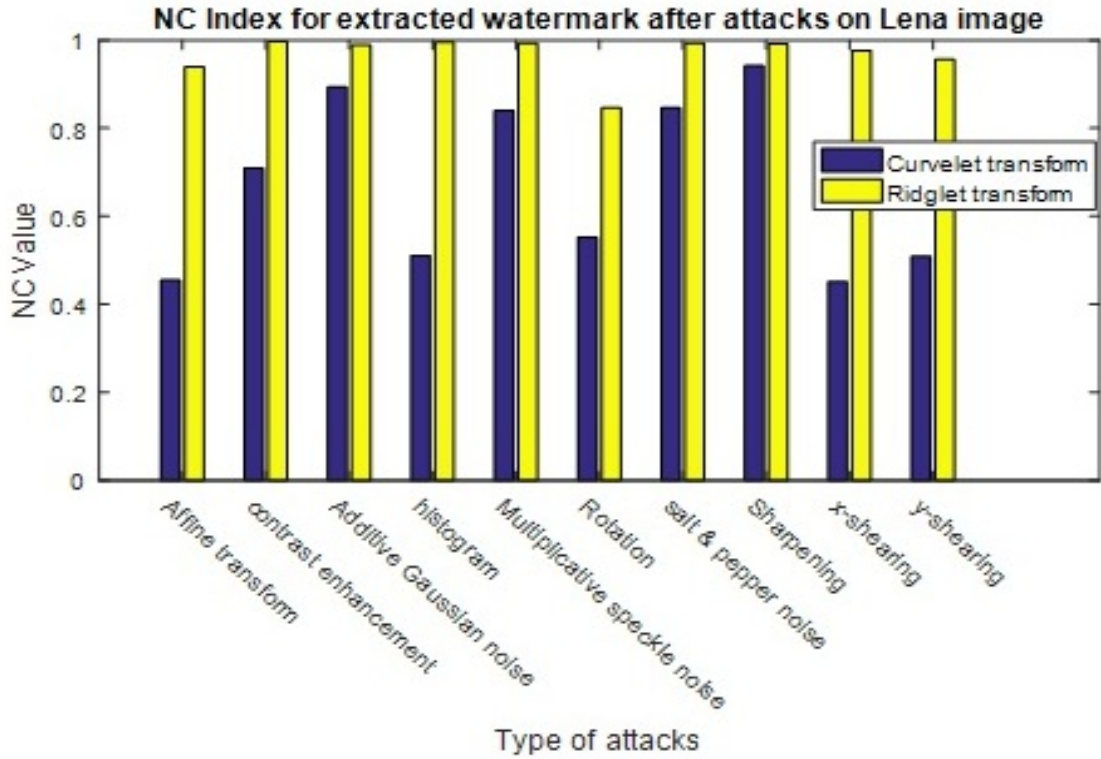


Figure 5.24: Values of *NC* for Extracted Watermark after Attacks on Lena image

Table 5.2: *PSNR* and *NC* values at different attacks for Peppers image

Peppers Image Attack Name	Curvelet Transform[26]		Ridgelet Transform	
	<i>PSNR</i>	<i>NC</i>	<i>PSNR</i>	<i>NC</i>
Affine Attack	12.18	0.43	36.94	0.90
Contrast Enhancement Attack	19.33	0.69	37.90	0.97
Additive Gaussian Attack	28.39	0.87	38.30	0.96
Histogram Attack	8.80	0.59	10.95	0.99
Multiplicative Speckle Noise Attack	27.18	0.88	38.39	0.97
Rotation Attack	16.48	0.51	36.56	0.75
Salt and Pepper noise Attack	40.34	0.83	37.50	0.95
Sharpening Attack	40.18	0.77	38.90	0.98
X-Shearing Attack	18.88	0.43	37.10	0.96
Y-Shearing Attack	17.56	0.47	37.03	0.93

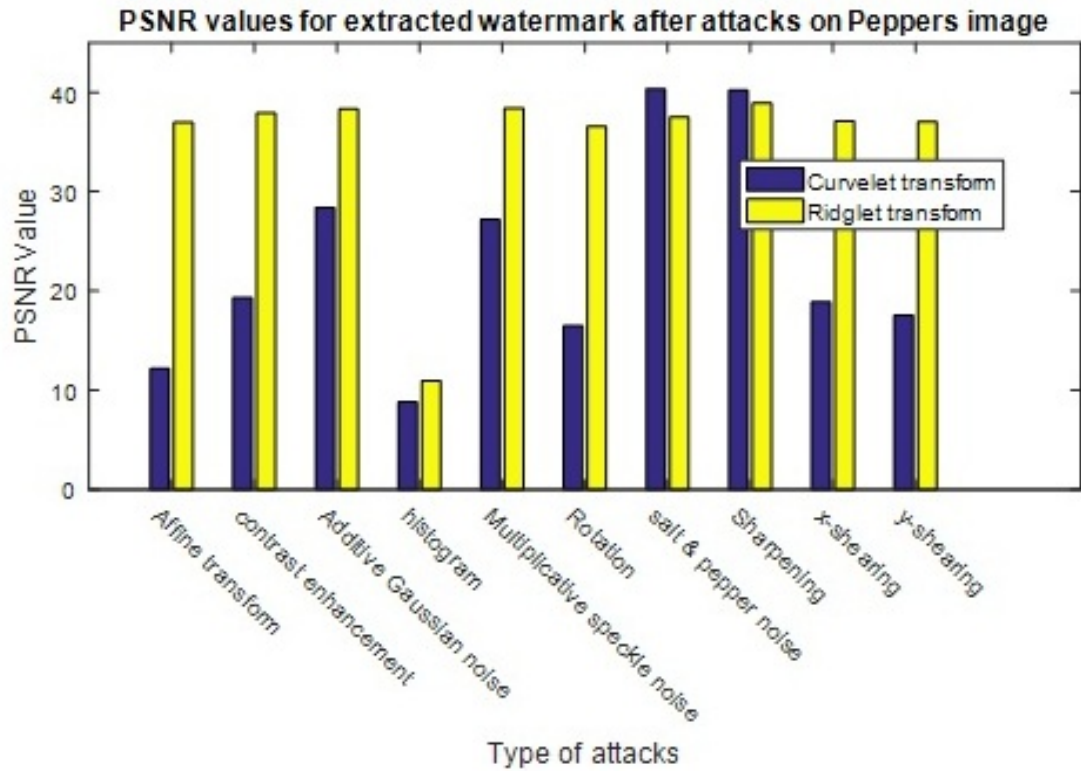


Figure 5.25: Values of *PSNR* for Extracted Watermark after Attacks on Peppers image

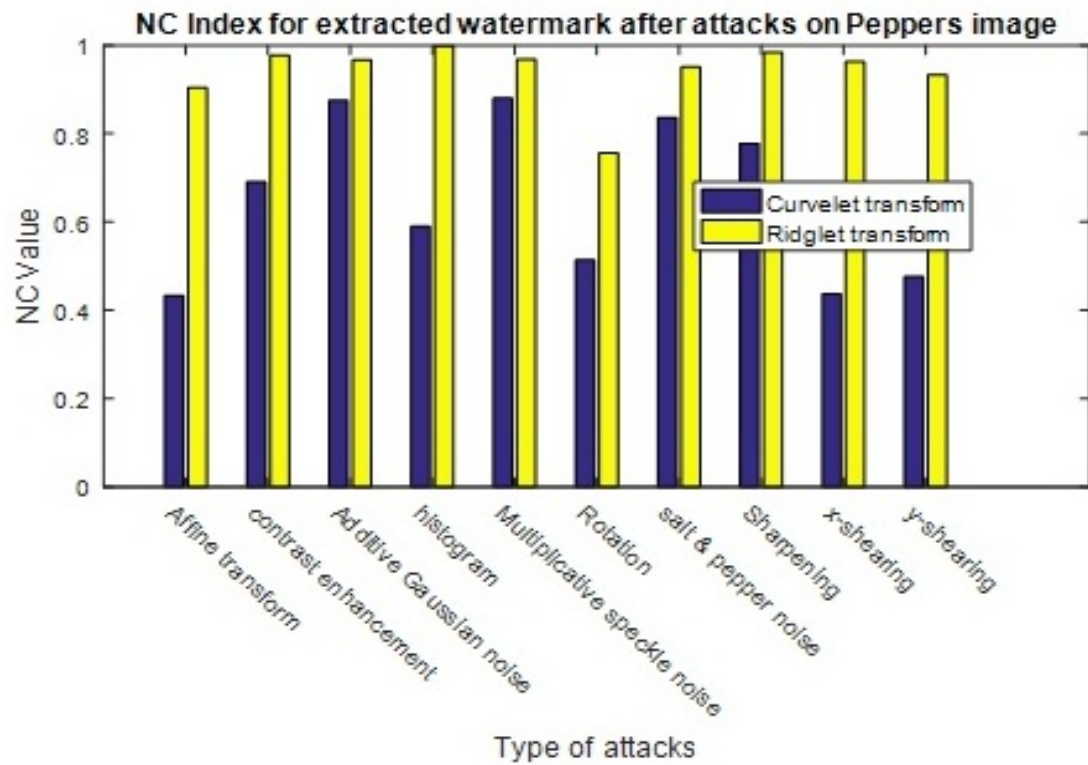


Figure 5.26: *NC* values for Extracted Watermark after Attacks on Peppers image

Table 5.3: Values of *PSNR* and *NC* for Barbara image for different attacks

Barbara Image	Curvelet Transform[26]		Ridgelet Transform	
Attack Name	<i>PSNR</i>	<i>NC</i>	<i>PSNR</i>	<i>NC</i>
Affine Attack	13.15	0.38	37.02	0.93
Contrast Enhancement Attack	16.33	0.75	38.80	0.98
Additive Gaussian Attack	31.47	0.90	38.52	0.99
Histogram Attack	6.65	0.64	8.59	0.97
Multiplicative Speckle Noise Attack	27.96	0.86	38.48	1.00
Rotation Attack	19.99	0.55	36.57	0.79
Salt and Pepper Noise Attack	40.94	0.82	38.03	0.99
Sharpening Attack	46.23	0.94	39.72	0.98
X-Shearing Attack	19.08	0.51	37.39	0.96
Y-Shearing Attack	19.55	0.44	37.30	0.94

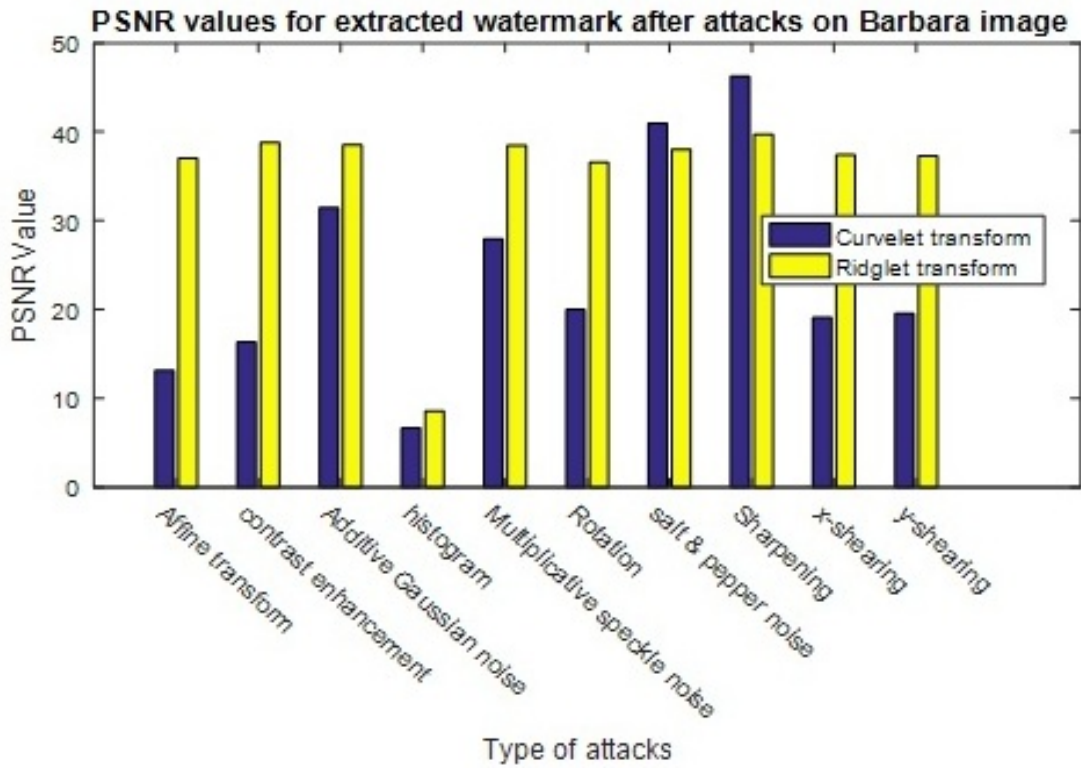


Figure 5.27: Values of *PSNR* for Extracted Watermark after Attacks on Barbara image

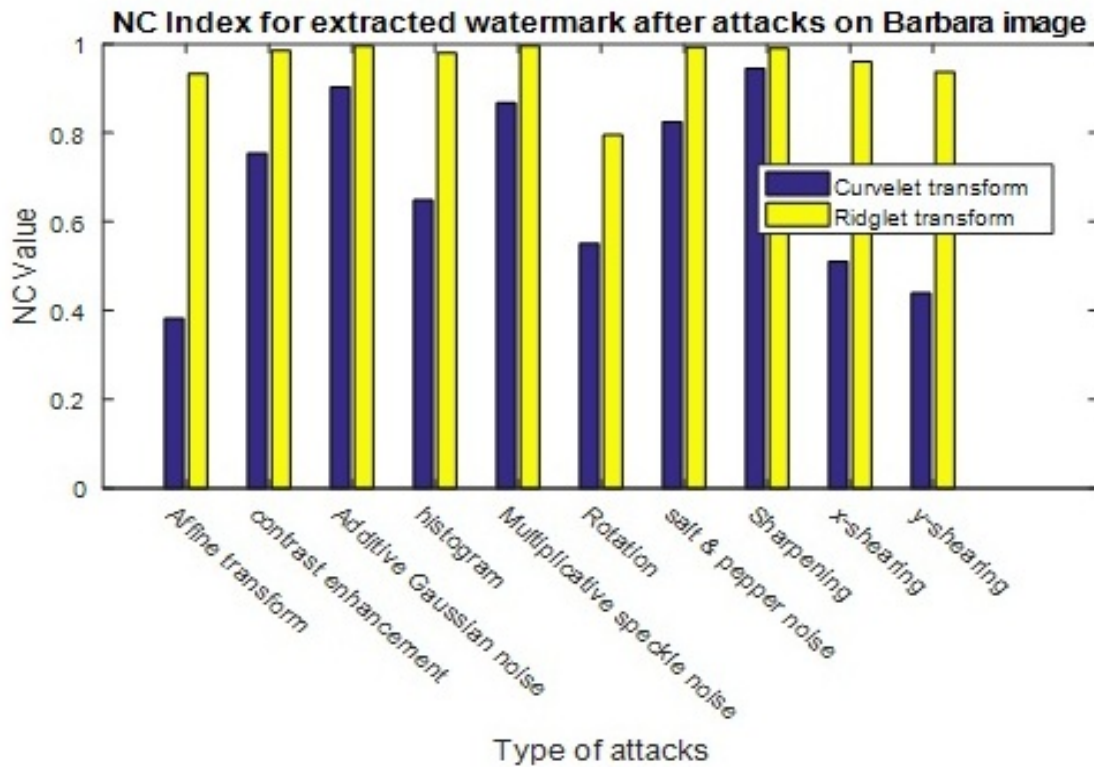


Figure 5.28: NC values for Extracted Watermark after Attacks on Barbara image

Table 5.4: The values of *PSNR* and *NC* for Baboon image for different attacks

Baboon Image Attack Name	Curvelet Transform[26]		Ridgelet Transform	
	<i>PSNR</i>	<i>NC</i>	<i>PSNR</i>	<i>NC</i>
Affine Attack	11.71	0.50	36.82	0.90
Contrast Enhancement Attack	19.17	0.70	39.43	0.92
Additive Gaussian Attack	32.33	0.92	38.05	0.99
Histogram Attack	11.35	0.69	4.23	0.91
Multiplicative Speckle Noise Attack	26.05	0.79	38.15	1.00
Rotation Attack	16.01	0.61	37.12	0.88
Salt and Pepper Noise Attack	43.07	0.88	37.86	0.98
Sharpening Attack	46.08	0.94	40.73	0.96
X-Shearing Attack	17.89	0.50	37.60	0.89
Y-Shearing Attack	17.81	0.51	37.22	0.91

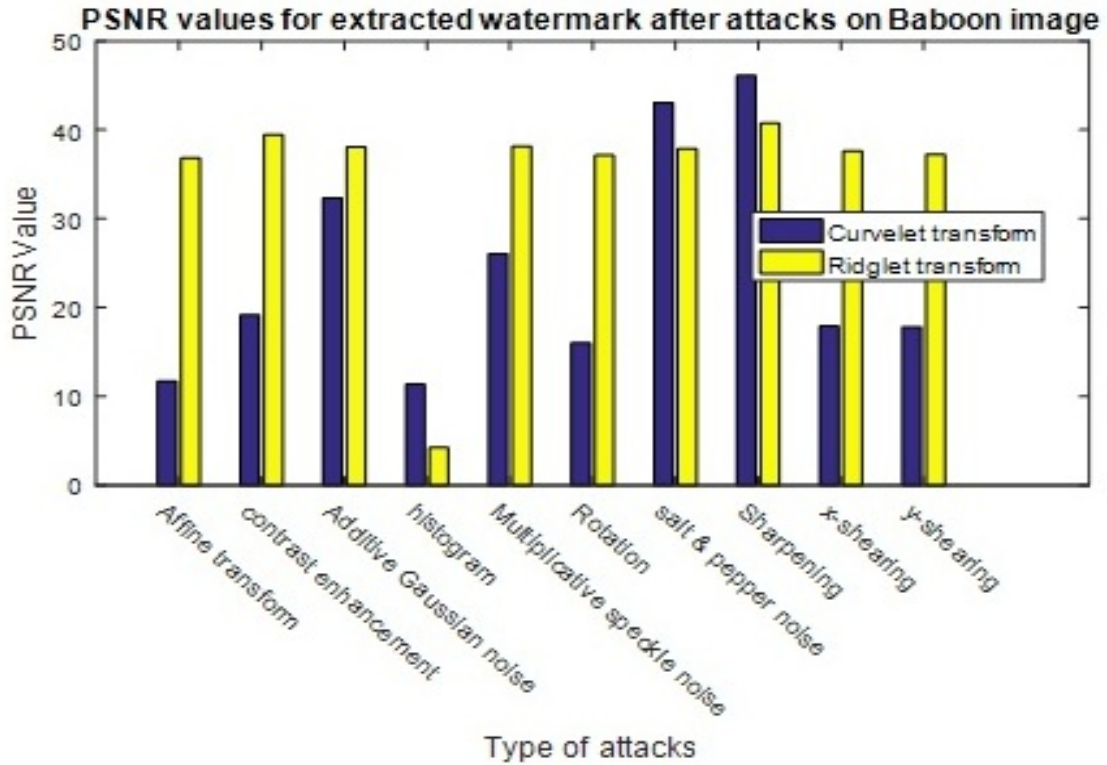


Figure 5.29: Value of *PSNR* for Extracted Watermark after Attacks on Baboon image

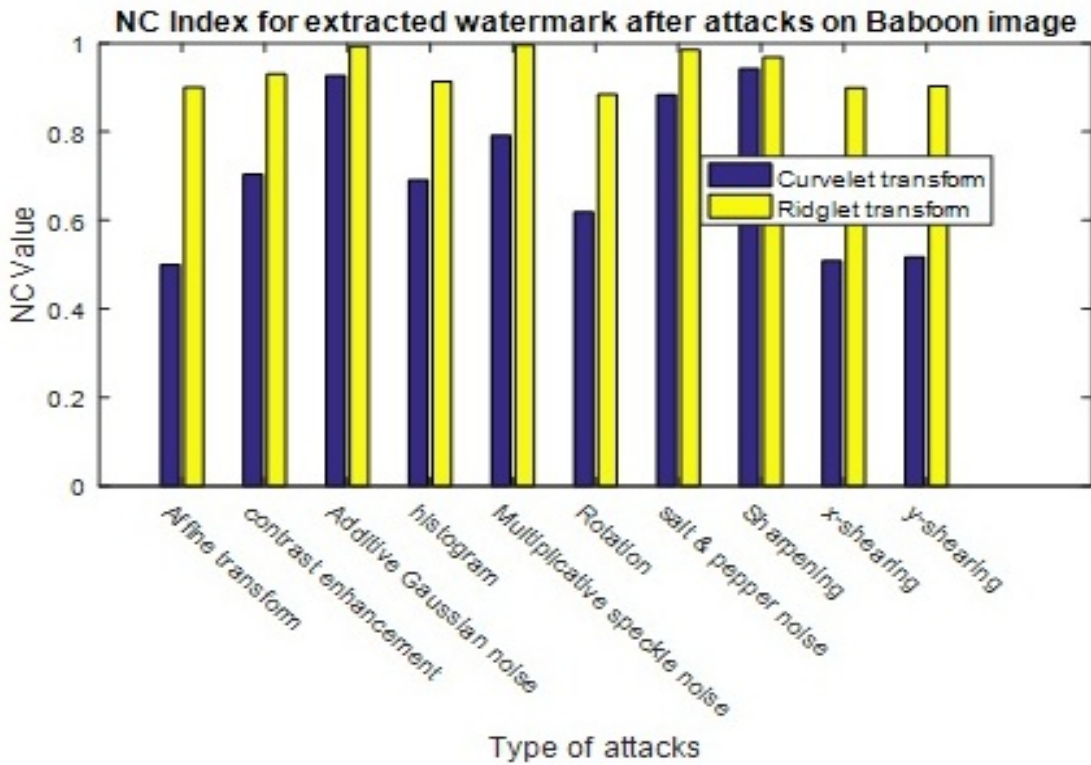


Figure 5.30: *NC* values for Extracted Watermark after Attacks on Baboon image

Chapter 6

Conclusion and Future Work

6.1 Conclusion

Focus of this work is to design watermarking technique more robust to attacks and to preserve more information when watermark is extracted after the attacks. Embedding and extracting procedure involve many steps *i.e.* *RT*, *RPCA*, Arnold transform and *SVD*. At first, cover image is read and then converted it into *HSI* color space. Then Intensity channel is processed through Robust *PCA* which is a statistical method that is frequently used with multivariate data. *PCA* is a method to decline the dimensionality of a dataset that consists of plenty of variables with many being correlated while still preserves as many variations that exist in the data set. This polished the data by transforming it into new variables called *PC* that are ordered in a way that initial few components contains many variations of the original data set. After reducing to these new variables, the *PCs* give a sparser representation of the data. *RPCA* is used instead of normal *PCA* because it is able to choose principal components more reliably than normal *PCA* and is

faster in speed. Then *PCA* coefficients are further decomposed into bands and sub bands using *RT*. After that watermark image is read and resized and encrypted through Arnold transform to increase data security. Then *SVD* technique is applied to merge the watermark into cover image. Finally comparison has been done between proposed approach with existing approach. *PSNR* value between cover image and extracted image generated by proposed technique after different attacks is upto 39 db and *NC* between cover image and extracted images given by proposed technique is 0.85-1. The proposed *RT* approach found more robust then existing *CT* approach for geometric attacks *i.e.* X-Shear, Y-Shear, Affine transform, Rotation and Image processing attacks *i.e.* Contrast Enhancement, Speckle Noise addition, Salt and Pepper noise and sharpening attacks. Existing *CT* approach founds more robust only in Histogram attacks.

6.2 Future Work

In this work, only geometric and noise addition attacks has been implemented to check the robustness and imperceptibility of *RT* based watermarking systems. Other attacks *i.e.* scaling, flipping, filtering attacks can be implemented. Also other transform techniques can be explored *i.e.* Shearlet, Brushlet, Contourlet and Bandelet etc to increase the robustness and imperceptibility. This can be applied on different images of different dimensions. To increase the value of *PSNR* and *NC* in Histogram attack, another transform can be applied. This technique can be extended to audio and video compression.

Bibliography

- [1] L. H. Chen and J. J. Lin, “Mean quantization based image watermarking,” *Image and Vision Computing*, vol. 21, no. 8, pp. 717–727, 2003.
- [2] A. Bors and I. Pitas, “Image watermarking using *DCT* domain constraints,” in *Image Processing, Proceedings, International Conference on*, vol. 3. IEEE, 1996, pp. 231–234.
- [3] R. B. Wolfgang and E. J. Delp, “A watermark for digital images,” in *Image Processing, Proceedings, International Conference on*, vol. 3. IEEE, 1996, pp. 219–222.
- [4] C. C. Chang, P. Tsai, and C. C. Lin, “SVD based digital image watermarking scheme,” *Pattern Recognition Letters*, vol. 26, no. 10, pp. 1577–1586, 2005.
- [5] J. Joy, S. Peter, and N. John, “Denoising using soft thresholding,” *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no. 3, pp. 1027–1032, 2013.
- [6] E. J. Candès, “Harmonic analysis of neural networks,” *Applied and Computational Harmonic Analysis*, vol. 6, no. 2, pp. 197–218, 1999.

- [7] M. N. Do and M. Vetterli, "Contourlets: a directional multiresolution image representation," in *Image Processing. 2002. Proceedings. 2002 International Conference on*, vol. 1. IEEE, 2002, pp. I–I.
- [8] F. Rahimi and H. Rabbani, "A dual adaptive watermarking scheme in contourlet domain for *DICOM* images," *Biomedical engineering online*, vol. 10, no. 1, p. 53, 2011.
- [9] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on *DWT-SVD*," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 1002–1013, 2009.
- [10] W. Lu, W. Sun, and H. Lu, "Robust watermarking based on *DWT* and nonnegative matrix factorization," *Computers & Electrical Engineering*, vol. 35, no. 1, pp. 183–188, 2009.
- [11] A. Mishra, C. Agarwal, A. Sharma, and P. Bedi, "Optimized gray-scale image watermarking using *DWT-SVD* and firefly algorithm," *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858–7867, 2014.
- [12] O. Jane, E. Elbaşı, and H. İlk, "Hybrid non-blind watermarking based on *DWT* and *SVD*," *Journal of applied research and technology*, vol. 12, no. 4, pp. 750–761, 2014.
- [13] M. Kumar and S. Agrawal, "Color image encoding in *DOST* domain using *DWT* and *SVD*," *Optics & Laser Technology*, vol. 75, pp. 138–145, 2015.

- [14] A. AlHaj, M. E. Farfoura, and A. Mohammad, “Transform-based watermarking of 3D depth image based rendering images,” *Measurement*, vol. 95, pp. 405–417, 2017.
- [15] M. Q. Fan, H. X. Wang, and S. K. Li, “Restudy on SVD based watermarking scheme,” *Applied Mathematics and Computation*, vol. 203, no. 2, pp. 926–930, 2008.
- [16] K. Deepa Mathew, “SVD based image watermarking scheme,” 2010, pp. 21–24.
- [17] R. S. Run, S. J. Horng, J. L. Lai, T. W. Kao, and R. J. Chen, “An improved SVD based watermarking technique for copyright protection,” *Expert Systems with applications*, vol. 39, no. 1, pp. 673–689, 2012.
- [18] S. I. Jia, “A novel blind color images watermarking based on SVD,” *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 12, pp. 2868–2874, 2014.
- [19] S. Jose, R. C. Roy, and S. S. Nambiar, “Robust image watermarking based on DCT-DWT-SVD method,” *International journal of Computer Applications*, vol. 58, no. 21, 2012.
- [20] M. Rahman, “A DWT, DCT and SVD based watermarking technique to protect the image piracy,” *arXiv preprint arXiv:1307.3294*, 2013.
- [21] A. Rani, A. K. Bhullar, D. Dangwal, and S. Kumar, “A zero-watermarking scheme using discrete wavelet transform,” *Procedia Computer Science*, vol. 70, pp. 603–609, 2015.

- [22] M. Rabizadeh, M. Amirmazlaghani, and M. Ahmadian Attari, "A new detector for contourlet domain multiplicative image watermarking using Bessel K form distribution," *Journal of Visual Communication and Image Representation*, vol. 40, pp. 324–334, 2016.
- [23] S. Natsu, P. Natsu, and T. Sarode, "Improved robust digital image watermarking with SVD and hybrid transform," in *Intelligent Communication and Computational Techniques, 2017 International Conference on*. IEEE, 2017, pp. 177–181.
- [24] E. B. Tarif, S. Wibowo, S. Wasimi, and A. Tareef, "A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2485–2503, 2018.
- [25] M. S. Subhedar and V. H. Mankar, "Curvelet transform and cover selection for secure steganography," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8115–8138, 2018.
- [26] R. Ahmed, M. M. Riaz, and A. Ghafoor, "Attack resistant watermarking technique based on fast curvelet transform and robust principal component analysis," *Multimedia Tools and Applications*, pp. 1–11, 2018.
- [27] M. N. Do and M. Vetterli, "The finite ridgelet transform for image representation," *IEEE Transactions on Image Processing*, vol. 12, no. 1, pp. 16–28, 2003.

- [28] W. Lulu and Z. Chong, “Arnold scrambling based on digital image encryption technique,” *National Defense Technology Base*, vol. 10, 2010.
- [29] H. Fangyuan, “Arnold scrambling based on image scrambling algorithm and implementation,” *J. Gui Zhou University (Natural Science)*, vol. 25, no. 3, 2008.

Plagiarism Report

jds

ORIGINALITY REPORT

13%

SIMILARITY INDEX

7%

INTERNET SOURCES

9%

PUBLICATIONS

4%

STUDENT PAPERS

PRIMARY SOURCES

1

www.ijert.org

Internet Source

1%

2

www.ijritcc.org

Internet Source

1%

3

Lecture Notes in Computer Science, 2009.

Publication

1%

4

"Medical Image Watermarking", Springer
Nature, 2017

Publication

1%

5

Submitted to Universiti Teknologi Malaysia

Student Paper

1%

6

Submitted to University of North Texas

Student Paper

1%

7

Submitted to Sreenidhi International School

Student Paper

1%

8

Mousavi, Seyed Mojtaba, Alireza Naghsh, and
S. A. R. Abu-Bakar. "Watermarking Techniques
used in Medical Images: a Survey", Journal of
Digital Imaging, 2014.

1%

List of Publications

1. Jashanjot, Singara Singh ”*A brief Review: Digital Image Watermarking Based on DWT and SVD*”, in International Journal of Scientific Research in Computer Science Applications and Management Studies *IJSRCSAMS*, 2018 [Published]
2. Jashanjot, Singara Singh ”*Ridgelet Transform based Robust Image Watermarking Technique*”, in IGI Global, Scopus 2018 [under review]