Chapter 2

Background Study and Methodology

2.1 Preliminaries

In the era of digital technology, digital watermarking scheme is a engrossing field of multimedia communication where authentication, tamper detection, copyright protection and ownership identification are necessary. Digital watermarking scheme is a method for embedding digital information into digital media without degrading the quality of host media. The internet dependency of human beings increases the importance of this scheme in preventing copyright infringements, detection of tampered multimedia or identify the legitimate owner.

2.1.1 General Watermarking Framework

Any digital watermarking scheme can consist of two phases:- (i) embedding phase and (ii) extraction phase shown in Fig. 2.1. In first phase a secret information is being encoded within the cover image using shared secret key to generate watermarked image as depicted in Fig. 2.1(a). In second phase, the watermark can be extracted from watermarked image with he help of shared secret key. The extraction process has been depicted in Fig. 2.1(b). Mathematically

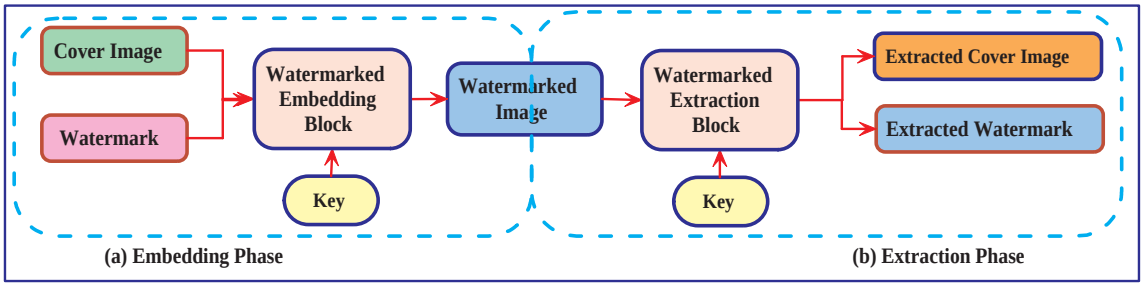

Figure 2.1: General Watermarking Framework

watermark embedding and extraction phase can be expressed as follows:

$W_{em} = \Phi(CI, W)$ and $W_{ex} = \Psi(W_{em}, CI)$

where CI, W, W_{em} and W_{ex} are the cover media, watermark, watermarked media and extracted watermark respectively. Also $\Phi()$ and $\Psi()$ are the embedding and extraction function respectively.

2.1.2 Key Features of Digital Watermarking Schemes

Some of the important performance parameters of digital watermarking schemes are as follows:

i) **Imperceptibility/visual quality**:- The first and foremost requirement of any watermarking algorithm is the imperceptibility. The imperceptibility mainly focuses on perceptual transparency of the watermark. The embedded information (watermark) within cover image should not cause any degradation in visual quality. The secret message should remain invisible, it should not be detectable to the human visual system (HVS) and there should not be any visual distortion within watermarked image so that it remains unsusceptible and safe. So an imperative virtue of any invisible watermarking scheme is to maintain good visual quality after embedding the watermark.

ii) **Payload**:-The payload is considered as the amount of information inserted within cover image. Though payload is not an essential characteristic of the watermarking scheme but from literature survey, it has been seen that many researchers are trying to increase the embedding capacity while maintaining a quality of the image. So the amount of information is mainly depends on area of application like authentication, tamper detection, copyright protection etc. The payload should be higher as much as possible with an acceptable resultant of perceptible image quality.

iii) **Robustness**:- Robustness is defined as if the watermark can be detected after media operations such as filtering, lossy compression or modification. The robustness criteria is mainly based on two major factors:- (1) whether a watermark detector can detect the watermark from the watermarked image. (2) whether a watermark can be found or not after any distortion. In some cases the watermark may need to be fragile. Fragile means that the watermark should not resist tampering or would resist only up to a certain, predetermined extent. This property of a watermarking scheme helps it to be useful in authentication, tamper detection and copyright protection. It is more a property and not a requirement of watermarking.

iv) **Reversibility**:- Watermarking is one of the up-coming solutions for authentication. But after embedding, watermark can damage the cover information that has been present in the original cover media. So, it is difficult to get an exact cover media at the receiver end. But recently, recover of original cover media is essential in various human centric application areas such as military, medical etc. In such applications, instead of conventional watermarking, reversible watermarking scheme is employed.

v) **Security**:- Security of a scheme is measured by evaluating the strength of the scheme against existing attacks. From the existing work, it has been found that there are some security loopholes in the watermarking technique used in practical applications. The watermarked image should not reveal any clues of the presence of the watermark, with respect to unauthorized detection. The security level can vary depending on the area of application.

vi) **Integrity/Tamper detection**:- Tampering is an intentional modification of documents in a way that would make them harmful to the consumer. So it is essential to reveal the watermark as well as cover image during extraction process by authorized user.

vii) **Authentication**:- Authentication assurances that the interacting entity is the one which it claims to be. Authentication code (AC) is required to check the authentication of the object.

viii) **Time Complexity**:- The time complexity of any watermarking scheme mainly depends on time required for embedding and extracting watermark. The time required for any watermarking should be as less as possible as well as authorized person.

Depending on watermarking domain, digital image watermarking techniques can be categorized into many ways (i) Spatial domain, (ii) Transform domain, (iii) Compress domain, (iv) Random domain etc. In this thesis, proposed schemes have been developed in spatial domain.

2.2 Methodology

Before going to design an algorithm one should have the proper knowledge about some tools and methodologies which makes the algorithm more efficient and robust. In this section, some tools and methodologies which are used in the of development of proposed algorithms have been discussed.

2.2.1 Hamming Code (HC)

Richard Hamming [28] formulated a sophisticated pattern of parity checking code called Hamming code. It is linear code for error correction that can be used to detect and correct single bit

error. The length of linear code n with k dimension are represented as $[n, k]$ codes. Now if c is consider as a linear code of order $[n, k]$, then the dual of c will be a $[n, n-k]$ linear code. Again if, H is considered as a checker matrix for c then the matrix H will be $(n-k) \times k$ and the row of which are orthogonal to c and $\{x \mid H\ x^T = 0\} = c$ and

$$(m_1, m_2, \ldots, m_k)^T = H.(LSB(x_1), (LSB(x_2), \ldots, LSB(x_n))^T \tag{2.1}$$

Any secret message of k bits, say $(m_1, m_2, \ldots, m_k)$ can be embedded in the LSB of n pixel, say $(x_1, x_2, \ldots, x_n)$ by at most Q changes. Here, Q is the maximum number of changes and Q_a is the average number of changes. The embedding efficiency can be measured by (k/Q_a) and embedding rate will be (k/n). The position of erroneous bits must be determined to correct the error. For n-bit code $log_2(n)$ bits are required. The Table 2.1 depicts the parity check for the matrix of $(7, 4)$ Hamming code.

Table 2.1: Parity checking matrix of $(7, 4)$ Hamming code

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

The Hamming code is used by odd parity to allow the identification of a single bit error shown in Table 2.2. Creation of the codeword as follows:

(i) Parity bit positions are marked which are the power of two such as $2^0,\ 2^1,\ 2^2, \ldots$.

(ii) All remaining positions are allowed to embed secret data bits such as 3, 5, 6, ...

(iii) The sequence of bits for every parity or redundant bits are computed as follows:

Redundant bit r_1: One bit position is checked and skipped alternatively which are $(1, 3, 5, 7, 9, 11, \ldots)$

Redundant bit r_2: Two bit positions are checked and skipped alternatively which are $(2, 3, 6, 7, 10, 11, \ldots)$

Redundant bit r_4: Four bit positions are checked and skipped alternatively which are $(4, 5, 6, 7, \ldots)$

Redundant bit r_8: Eight bit positions are checked and skipped alternatively which are $(8-15, 24-31, 40-47, \ldots)$

(iv) Adjust parity bit through odd parity.

Table 2.2: Redundant bits adjustment using odd parity for error detection and correction

Highlighted bits with power of 2	01	02	03	04	05	06	07	08	09	10	11
Insert data	1	1	1	1	0	0	0	0	0	0	1
Highlight the check bit	1	1	1	1	0	0	0	0	0	0	1
Odd parity of 2^0	1		1		0		0		0		1
Odd parity of 2^1		1	1			0	0			0	1
Odd parity of 2^2				1	0	0	0				
Odd parity of 2^3								0	0	0	1

Recently watermarking through Hamming code has become a very interesting field in current research which is used in security and online application. Design a secured reversible watermarking algorithm without compromising the visual quality using Hamming code is still a significant research issue. So far in the literature, it is found that a few such scheme exists, where reversibility has been achieved through Hamming code. In addition, the utilization of shared secret key in watermarking through HC is also rarely available. In the present research, dual image based reversible watermarking schemes using (15, 11) Hamming code has been proposed.

2.2.2 Cellular Automata (CA)

Cellular automata is one of the most promising area of interest for the current researcher in the field of VLSI design, coding theory, cryptography and image processing. Many interesting problems related with security and privacy of digital information can be addressed by CA. The usage of CA characteristics is still not much explored in the field of watermarking. The complex discrete structure with complex behaviour deducted from simple rules makes CA more acceptable. Therefore, we use chaotic behavior of CA to produce unpredictable configurations and use them as inputs of the proposed algorithms.

Cellular automata can be described as a four tuples G, S, N, f, where, "G" represents grid or set of cells, "S" represents set of possible cells states, "N" represents set of neighborhood indices of size $|N|$ = n and "f" represents transition function or rules of the automaton. CA follow the

Table 2.3: CA rule with its next state update strategy

Rules	7	6	5	4	3	2	1	0
	111	110	101	100	011	010	001	000
90	0	1	0	1	1	0	1	0
150	1	0	0	1	0	1	1	0
238	1	1	1	0	0	1	0	0

basic automata theory that is the state of every cell relies on state of its neighbouring cell and its present state. Depending on the dimension cellular automata can be categorised into 1D cellular automata and 2D cellular automata. In 1D CA, there is a 3-neighbourhood association and the next state ($S_k(u+1)$) is dependent on itself and its left and right neighbours and formulated as:

$$S_k(u+1) \quad = \Phi(S_{k-1}(u), S_k(u), S_{u+1}(u)) \tag{2.2}$$

where, $S_k(u)$ denotes the k^{th} cell state at u^{th} time, Φ is the next state function. Wolfram coined rule number of CA corresponds to the decimal equivalent of state functions. There are total 2^{2^3} that is, 256 different state functions in an elementary CA. Among these 256 rules, only three rules 90, 150 and 238 are illustrated here:

Rule 90 : $S_k(u+1) = (S_{k-1}(u) \oplus S_{k+1}(u))$

Rule 150 : $S_k(u+1) = (S_{k-1}(u) \oplus S_k(u) \oplus S_{k+1}(u))$

Rule 238 : $S_k(u+1) = (S_k(u) \vee (S_{k+1}(u)))$

A special type of elementary CA is called Cellular Automata Attractor (CAA). It has the property of periodicity which makes it more easy to developed proposed algorithms.

2.2.3 Local Binary Pattern (LBP)

LBP is a very impressive tools for texture and pattern analysis and classification. The invariance property and the computational simplicity of the LBP operator make it more acceptable. LBP was first described in 1994 by Ojala et al. [63]. LBP operator basis on complementary aspect and strength of the pattern introduced by Ojala et al. [62]. This operator becomes more popular due to its discriminative power and computational simplicity. In this method the pixels of an image is considered as a binary number depending on some threshold values of the neighbour

pixels. The simplest form of LBP vector shown in Fig. 2.2 is designed by the following manner: Consider a (3×3) window and the center pixel as threshold value. Then 8-neighbours

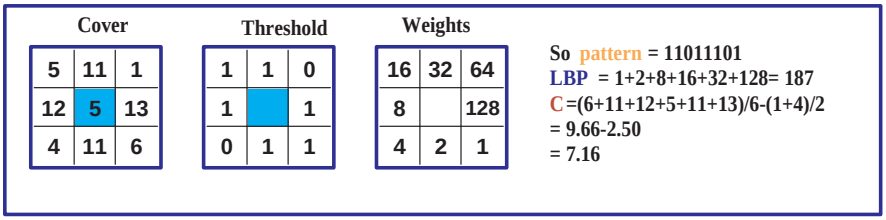

Figure 2.2: Basic Diagram of LBP Operator

pixels are compared with the threshold value which has been constructed by putting "0" or "1" in place of neighbour pixels. Put "0", if the neighbourhood pixel's value is less than the threshold value otherwise put "1". Now LBP vector is produced by performing sum of entry-wise-multiplication with the threshold matrix and its corresponding weights. Now the contrast (C) value can be achieved by differentiate of average value of greater or equal to the center pixel and that of lesser than center pixel. The contrast is set to "0" if all the threshold value are same. The two dimensional distribution of LBP code and local contrast are used to feature classification. Such classifiers can be used for face recognition or texture analysis.

2.2.4 Weighted Matrix (WM)

A weighted matrix (WM) is simply a $(i \times j)$ integer matrix which is used in our proposed algorithms. Before watermarking, this matrix must be shared between the sender and receiver and can be used for secrecy purpose. Any arbitrary values can be chosen as the element of WM from the combination of $(0, 1, \ldots (2^{k-1} + 1))$ where k indicates the total number of secret bits $(p_1 p_2 \ldots p_k)$ which will be embedded within the cover image (CI). Now a new value v is generated by following equation:

$$v = (p_1 p_2 \ldots p_k)_2 - \sum (CI \otimes WM)(mod\ 2^k) \tag{2.3}$$

where, entry-wise multiplication operator is represented by $\otimes$. If v is equal to "0", then CI is unalter; otherwise, change CI to CI' satisfying the equation follows:

$$\sum (CI' \otimes WM) = p_1 p_2 \ldots p_k (mod\ 2^k) \tag{2.4}$$

The receiver can derive $(p_1 p_2 \ldots p_k)$ by computing $\sum (CI' \otimes WM)(mod 2^k)$.

2.3 Evaluation Metric and Datasets

This section describes some standard evaluation metrics which are used to assess the developed schemes this thesis. A brief description of standard image databases are included. Moreover, a short description about various attacks that are employed in our schemes have been summarized.

2.3.1 Subjective and Objective Quality Evaluation Metric

In this portion, a brief description of subjective and objective performance parameters have been explained that are carried out to judge the quality of watermarked image. The various evaluation metrics that are used in this thesis have been summarized as follows:

2.3.1.1 Mean Square Error (MSE)

Mean Square Error [35] is used to find the average squared intensity of the cover and watermarked image. It measures how much a pixel is degraded from its original. MSE is calculated as using the following formula:

$$MSE = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}[CI - WI]^2}{(M \times N)}, \tag{2.5}$$

where M and N represents size of cover image (CI) and watermarked image (WI) respectively.

2.3.1.2 Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) [35] is a frequently used visual quality evaluation metric in the field of image processing. The PSNR (dB) value between two images represents the average error between two images. It is mainly measured with the help of MSE of two images as illustrated in equation (2.6).

$$PSNR = 10\ log_{10}\frac{255^2}{MSE}, \tag{2.6}$$

To find the PSNR of color image, an average MSE is considered for different RGB color component. A watermark algorithm is said to be better if the PSNR (dB) of the proposed work is as much as possible but atleast 30 dB.

2.3.1.3 Embedding Capacity (EC)

The embedding capacity (EC) or payload (bpp) of a scheme is depended by the rate of bits are embedded within the cover image and is calculated by:

$$EC = \frac{MEB}{L} \tag{2.7}$$

where, $MEB =$ Maximum number of bits are embedded into the cover image.
$L =$ Total number of bits in cover image.

2.3.1.4 Structural Similarity Index Measurement (SSIM)

Structural Similarity Index Measurement (SSIM) [79] is a parameter for finding the resemblance between two images. SSIM basically focuses on the degradation of structural information based quality assessment. The structural information is found through local luminance and contrast rather than average luminance and contrast. The SSIM value lies between -1 and +1. Its value approaches to +1 when two images are indistinguishable. The mathematical formula for finding the value of SSIM is shown in equation (2.8):

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{2.8}$$

where, μ_x and μ_y have been considering the mean, ${\sigma^2}_x$ and ${\sigma^2}_y$ represents the variance and σ_{xy} indicates the covariance of x and y respectively; $c_1 = (k_1 L)^2$ and $c_2 = (k_2 L)^2$ are two variables and range of the pixels is denoted by L.

2.3.1.5 Standard Deviation (SD)

Standard Deviation (SD) [35] represents that how an image deviates from others. It is calculated by equation (2.9).

$$SD = \sqrt{\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(CI - \overline{CI})^2}{(M-1)(N-1)}} \tag{2.9}$$

where, CI is the cover image of size $(M \times N)$ and CI is the mean of pixels.

2.3.1.6 Correlation Coefficient (CC)

The Correlation Coefficient (CC) [35] between two digital images represents the similarities and dissimilarity. The equation 2.10 shows the CC values between any two images. The range of

CC varies from -1 to $+1$ and CC value of 0 represents that the two images are undistinguishable and the value tends to the border represents that the two images are different. The equation 2.10 shows the mathematical formulation of CC values between any two images.

$$CC = \frac{\sum_{m=1}^{M}\sum_{n=1}^{M}(CI - \overline{CI})(WI - \overline{WI})}{\sqrt{(\sum_{m=1}^{M}\sum_{n=1}^{M}(CI - \overline{CI})^2)(\sum_{m=1}^{M}\sum_{n=1}^{M}(WI - \overline{WI})^2}} \tag{2.10}$$

2.3.1.7 Normalize Correlation Coefficient (NCC)

The Normalized correlation coefficient (NCC) [94] is accustomed to determine robustness. The mathematical formulation of NCC is as follows:

$$NCC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(CI \times WI)}{\sum_{i=1}^{M}\sum_{j=1}^{N}|CI|^2} \tag{2.11}$$

Where M and N represents the number of row and column respectively, CI is the original image and WI is the corresponding watermarked image.

2.3.1.8 Universal Quality Index (Q-Index)

The Universal quality index or Q-Index [79] measures the distortion within an image. Q-Index can be measure with the help of 3 parameters: i) Correlation Loss ii) Distortion of Luminance iii) Distortion of Contrast. It is measured by using the following formula:

$$Q = \frac{\sigma_{fg}}{\sigma_f \cdot \sigma_g} \cdot \frac{2\overline{f} \cdot \overline{g}}{(\overline{f})^2 + (\overline{g})^2} \cdot \frac{2\sigma_f \cdot \sigma_g}{\sigma_f^2 + \sigma_g^2} \tag{2.12}$$

Where, $\overline{f} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} CI;$ $\overline{g} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} WI;$

$\sigma_{fg} = \frac{1}{M+N-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[CI - \overline{f}][WI - \overline{g}]$

$\sigma_f^2 = \frac{1}{M+N-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[CI - \overline{f}]^2;$

$\sigma_g^2 = \frac{1}{M+N-1}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[WI - \overline{g}]^2$

where CI represents the original image and WI represent the watermarked image of size $(M \times$

N) containing pixel values (m, n) respectively $(0 \geq m > M, 0 \geq n > N)$. The first component is the CC, which is used to find the degree of correlation between two images. The second component calculates the luminance between two images and it range is $[0, 1]$. The third component is used to measures the similarity of contrast between two images. The range of this component is $[0, 1]$. Finally, it is seen that the range for Q-Index is $[-1, 1]$ and one can say the two images are identical if it gives the results 1.

2.3.1.9 Bit Error Rate (BER)

At the time of transmission some error may occurred within the image. This rate of errors are calculated by Bit Error Rate (BER) [65]. The mathematical formulation for BER is given in equation (2.13):

$$BER = \frac{TE}{L} \tag{2.13}$$

where, $TE =$ Total number of corrupted bits.
$L =$ Total number of bits in cover image.

2.3.1.10 Regular-Singular (RS) Analysis

The watermarked image has been analysed by using RS analysis proposed by Jessica Fridrich [25] for exploiting the correlation between the images. The RS analysis divides an images into disjoint groups G of n contiguous pixels $(l_1, l_2, \ldots, l_n)$. Then a discrimination function ϕ is used to find the smoothness or regularity of every groups and formulated as.

$$\phi(l_1, l_2, \ldots, l_n) = \sum_{i=1}^{n-1} |l_{i+1} - l_i|$$

Now an invertible flipping function (ϖ) is used to change the pixel value based on three condition. i) ϖ_1 is the permutation $2k \leftrightarrow 2k + 1$ where $k = 0 \ldots 127$. ii) ϖ_{-1} is the permutation $2k - 1 \leftrightarrow 2k$ where $k = 0 \ldots 128$; such that $\varpi_{-1}(x) = \varpi_1(x + 1) - 1$. iii) ϖ_0 is the identity permutation $k \leftrightarrow k$ where $k = 0 \ldots 127$. It represents an identical pixels. Now Regular (R), Singular (S) and Unusable (U) groups are separated depending on ϕ and the flipping function

ϖ depending on the following conditions.

$$\begin{cases} G \in R & \text{if } \phi(\varpi(G)) > \phi(G) \\ G \in S & \text{if } \phi(\varpi(G)) < \phi(G) \\ G \in U & \text{if } \phi(\varpi(G)) = \phi(G) \end{cases}$$

where $\varpi(G) = \varpi(l_1), \ldots, \varpi(l_n)$.

Then we calculate the value of RS analysis depending on some mask value (Z) as follows

$$(|R_Z - R_{-Z}| + |S_Z - S_{-Z}|)/(R_Z + S_Z) \tag{2.14}$$

where R_Z and R_{-Z} denotes the regular group number, S_Z and S_{-Z} denotes the singular group number with mask Z and $-Z$ respectively. One scheme can withstand against RS-attacks if the RS gives result closed to zero.

2.3.1.11 Computational Time

The most significant parameters for any watermarking scheme are the computational complexity and computation time. The computational time represents the efficient algorithm. In this work, the computational time is evaluated in a standard computational platform such as a Personal Computer with 64-bit Intel Core $i5 - 6200U$ processor of 2.40 GHz speed, 4 GB RAM and windows 10 Operating System. Moreover, all the algorithms have been designed in JAVA-9 software.

2.3.2 Standard Image Datasets

In this thesis four benchmark image database [26] [90] [89] [61] have been used for experiment and analysis of proposed scheme. USC-SIPI [90] is an image dataset of the university of Southern California. It is consisting a big size of image database with different sizes. UCID [61] is an Uncompressed Color Image Database of SPIE digital library, containing 1338 uncompressed colour images of different size. In HDR [26] image of 105 scenes captured using a Nikon $D700$ digital still camera. The STARE (STructured Analysis of the Retina) [89] image databases is basically consist of various types of medical images of Human Retina. It has been collected from the University of California, San Diego. The Fig. 2.3 depicts the corresponding image of said databases.

Figure 2.3: Standard color images of (512×512) pixels used as host image collected from standard benchmark databases

2.4 Brief Overview of Attacks in Watermarking Scheme

A various attacks are possible on any watermarking scheme by which a watermarked image can be distorted, tampered or watermark can be removed from copyrighted material. So a technique by which a watermark or watermarked image can be distorted is called a watermarking attack. The watermarking attacks are classified into the following headings: Geometric, additive, editing, copy-move forgery, compression and others which are as follows:

2.4.1 Salt and Pepper Noise ($0.01, 0.1$ and 0.5 noise density)

Salt and pepper noise is just like an image gingerly filled by black and white pixels. This types of noise appears at the time of data transmission. In this noise the black and white pixels

are randomly distributed over the image depending on the density function. In this work we consider noise density as $0.01, 0.1$ and 0.5 respectively. It is clear that the watermarked image is fully damaged after applying salt pepper noise with noise density 0.5. But after extraction procedure one can recover the watermark successfully which proves the robustness of our work. The mathematical formulation of salt and pepper noise is as follows.

$$\begin{cases} f(x) & = F_m \quad \text{if, } x = m \\ & = F_n \quad \text{if, } x = n \\ & = 0 \quad \text{Otherwise} \end{cases} \tag{2.15}$$

where, $F(x)$ denotes the probability density function, x is a random variable for pixel values and x, y are the intensity level of pixels.

2.4.2 Cropping ($10\%, 20\%$ and 50%)

Cropping is a geometric attack which deletes some region of images by selection procedure. The images can be cropped by different percentage. In this work three different label of cropping such as $10\%, 25\%$ and 50% have been considered to proves the robustness of proposed schemes.

2.4.3 Copy-Move Forgery ($5\%, 10\%$ and 20%)

Copy Move Forgery (CMF) is one of the important unintentional attack. In this scheme an image portion is copied and then it moves to the other region of the same image. In complicated types of CMF one can modify the copy portion by using general transformation like scaling, rotation, distortion and combination. The percent of CMF used in this thesis is $5\%, 10\%$ and 20% respectively. It is seen that after applying the maximum degree of CMF one can successfully recover the watermark which proves the robustness of our scheme.

2.4.4 Opaque (10%)

Opacity defines how much an image will obscure the background. In this work we have applied different label of opaque like 10%, 20% and 50% upon the watermarked image. After that extraction process has been studied and analyzed the robustness against opaque attacks.

2.4.5 Blurring (Sigma = 0.4)

Blurring means emphasise or suppress some features of an image. It can be made by large frequency attenuation. The mathematical formulation of image blurring is as follows.

$$X(i,j) \quad = e^{-\frac{P(i,j)^2}{2\sigma^2}} \tag{2.16}$$

where, $X(i,j)$ denotes the frequency domain filter, $P(i,j)$ denotes distance from centre of frequency rectangle and σ denotes deviation of spread about the centre. The image blurring quality is depended on the σ value. In this work, it is seen that after applying $\sigma = 0.4$ the successful extraction of watermark is possible which provides the robustness under blurring attack.

2.4.6 Median Filtering (3 x 3 block filtering)

Filtering means to modify image with respect to certain threshold value. In this thesis, (3×3) block median filtering has been considered and applied on the watermarked image. The evaluation results proves the robustness under median filtering.

2.4.7 Flipping (Vertical)

Flipping is the another attacks used in image processing. The control depends on two switch i.e., horizontal and vertical modes. In this work only vertical flipping has been introduced in watermarked images and the experimental outcomes shows that the successful extraction of watermark is possible which proves the robustness of the work under flipping.

2.4.8 JPEG Compression (QF=70)

A compression attacks is an unintentional attacks used in multimedia communication. The JPEG compression is basically a lossy compression technique, which minimizes the image integrity as a result a large amount of image information will be lost after applying this compression technique. So to check the robustness of a scheme JPEG compression takes an important factor. Any scheme is said to be robust if watermark can withstand after applying JPEG compression. The measure of compression depends compression ration which is treated as Quality

Factor (QF). In this whole work, QF has been taken as 70% and results proves that the suggested schemes are robust under compression attacks.

2.4.9 Inversion (Negative invert to all)

Color inverting is another important unintentional attack which may occurs at the time of data transmission. The watermarked images are inverted in separated by only RED channel inversion, only GREEN channel inversion, only BLUE channel inversion, all channel inversion is nothing but the negative inversion. In this investigation we use negative inversion and experimental results confirm the robustness under inversion attack.

2.4.10 Rotation (1 degree, 90 degree)

Rotation means spinning an image with certain angle. In case of rotation of an image we must consider three important parameters. (i) axis of rotation, (ii) direction of rotation and (iii) angle of rotation. The image will be rotate with respect to a particular axis which will be denoted by axis of rotation. The direction of rotation may be clockwise or anti-clockwise and the angle of rotation defines the amount of degree in which the image will be rotated. In this thesis we are presenting the outcomes after rotating the watermarked image by an angle 1 degree and 90 degree in clockwise direction with respect to z-axis.

2.4.11 Brute Force Attacks:

Brute Force Attack (BFA) is basically a trial-and-error technique which can be used for information extraction. In BFA, a large random number is generated which may match with the required keys when unauthorized person extract the watermark from the watermarked image. All proposed schemes are tested through BFA and shows that the developed schemes are robust in some extent.

In this chapter, basics of digital image watermarking, performance metrics, types of attacks, image databases have been described. In the subsequent three chapters, proposed digital watermarking schemes have been elaborated. Proposed schemes can be employed for image authentication, verification, tamper detection and tamper localization.