DIGITAL IMAGE WATERMARKING IN THE FREQUENCY DOMAIN

A report submitted after the completion of month-long summer training program

by

ANUSHKA PRAKASH

Under the guidance of

Ms. Aditi Zear
Dr. Kamlesh Dutta

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY HAMIRPUR
HAMIRPUR-177005, INDIA

July 2018

TABLE OF CONTENTS

NATIONAL INSTITUTE OF TECHNOLOGY
HAMIRPUR (H.P.)

CANDIDATE'S DECLARATION

I hereby certify that the work being presented in this report titled **'Digital Image Watermarking in the Frequency Domain'** has been done by me during the Summer Training Program at Department of Computer Science and Engineering, National Institute of Technology, Hamirpur (H.P.). It is an authentic record of the study and experiments carried out by me during a period from 11 June 2018 to 11 July 2018 under the supervision of Ms. Aditi Zear and Dr. Kamlesh Dutta.

The matter presented in this report has not been submitted by me or anyone else in any other university/institute for award of any certificate.

(ANUSHKA PRAKASH)

Mentor's Signature:

(DR. KAMLESH DUTTA)

MENTOR'S COMMENTS

I Aditi Zear, Former Lecturer (contract basis) in Department of Computer Science and Engineering, NIT Hamirpur, would like to inform that I had been assigned a student, Anushka Prakash for summer internship. She has worked on the topic Digital Image Watermarking in Frequency

domain. I am pleased with the work Anushka has accomplished in her internship. She has demonstrated a good moral character and working knowledge during her internship period.

(ADITI ZEAR)

ACKNOWLEDGEMENT

First and foremost, I wish to express my profound gratitude to my guide and mentor Ms. Aditi Zear for giving me an opportunity to work under her invaluable guidance. I wish to thank her for her encouragement and for providing me with necessary resources to complete my work. I would also like to thank my mentor Dr. Kamlesh Dutta for her vigilant supervision. Her tolerant and supportive nature accepted my shortcomings and fueled my curiosity.

I would like to thank all the faculty members and staff, for their help and support.

Last but not the least, I would like to thank my family and friends for their unwavering support and encouragement through thick and thin.

(ANUSHKA PRAKASH)

ABSTRACT

In this digital era, the expansion and advancement of technology has made it relatively easier to plagiarize and manipulate original content like images, audio, video. This has raised concerns towards the security and integrity of data present on the open network. Hence, there is a very strong need for a digital patenting system to be put into place. Digital watermarking is the answer to this problem. This report presents a study of the various techniques developed in the field of digital image watermarking, and proposes an algorithm based on LWT and DCT for the watermarking of color images, which uses Arnold transform for data encryption.

Keywords: Digital image watermarking, Image security and integrity, DWT, LWT, DCT

Chapter 1

INTRODUCTION

Digitization plays a huge role in our lives today, with extensive applications in the fields of medicine, science, engineering, entertainment, communication etc. With the widespread use of internet, a lot of digital data like images, text, audio, video is frequently transferred over the open network. Thus, the security and integrity of this humongous amount of data is of major concern. Intercepting data, unauthorized access, tampering with the data, plagiarism etc. has become easier over the time. A strong digital signature system can ensure that the above malpractices do not take place.

1.1 Digital Watermarking

Digital Watermarking is a method by which a marker is inconspicuously hidden in a noise- tolerant signal such as image, audio, video. That is, it hides some data related to the signal in the signal itself. The hidden message imparts a digital signature to the digital content, and identifies the owner or the authorized distributer, whichever be the case.

This concept is similar to steganography, the difference being in their goals. In steganography, any random message is hidden, and the cover signal is simply there to hide the message. But in watermarking, the message is related to the actual content of the cover signal.

1.2 Properties of Digital Image Watermarking

1. **Robustness**

   Fragile – If the watermark fails to be detectable after the slightest modification to the signal. Ideal in situations where tamper detection is required.

   Semi-fragile – If it resists benign transformations, but fails to be detectable after malignant ones. It can differentiate between malicious tampering and non-malicious modification to the image.

   Robust – If it resists a designated class of modifications. Ideal for copyright protection and authorization.

2. **Perceptibility**

    Imperceptible – If cover signal and marked signal are perceptually indistinguishable. It takes advantage of human vision to hide the watermark in plain sight.

    Perceptible – If the presence of watermark in the cover signal is noticeable.

3. **Capacity**

    Number of bits of watermark image that can be embedded in cover image without causing much distortion.

4. **False Positive Rate**

    It can sometimes happen that a watermark is identified inside an image even when it is not present. This rate has to be minimised.

1.3 Embedding Methods

Spread spectrum – If the watermarked image is obtained by additive modification.

Quantization type – Watermarked image is obtained by quantization.

Spatial domain – These methods are applied directly on the individual pixels of an image. Advantages are easy implementation and low computational complexity. But it is less robust to certain types of attacks.

Frequency domain – Watermark information is embedded by modifying frequency coefficients of the original image after transforms. It has better imperceptibility and robustness. This class of techniques is explored in this report in detail.

1.4 Blind and Non-Blind Watermarking

Blind – Cover image is not required for extracting the watermark from the watermarked image.

Non-blind – Cover image is needed to separate the watermark from the watermarked image.

Chapter 2

WATERMARKING TECHNIQUES

Following are some of the commonly used spatial domain techniques for digital image watermarking.

2.1 Spatial Domain Techniques

A. Least Significant Bit Modification

This is the simplest spatial domain algorithm. The least significant bit of each 8-bit pixel is written over by a bit from the watermark. It may be carried out in two ways: either the watermark information can be inserted over each and every pixel of cover image, or the busier areas of the image can be calculated and the watermark is embedded there to enhance imperceptibility.

On the average, only half of the bits in an image will need to be modified to hide a secret message using a cover image. Because the quality of watermarked image is low, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human visibility system. However, a passive attacker can easily extract the changed bits since the watermark has been embedded using a simple procedure. This can be countered by modifying the third or fourth LSB instead of the first one.

The least significant bits are highly sensitive to noise, so that the watermark can easily be removed by image manipulations such as rotation and cropping. Thus, the LSB method provides high imperceptibility and less robustness.

B. Log-average Luminance Method for Color Images

A colored-image is divided into blocks after converting the RGB colored image to YC_bC_r color space. To embed the watermark, 16 blocks of size 8x8 are selected and used to embed the watermark image into the original image. The selected blocks are chosen spirally (beginning form the center of the image) among the blocks that have log-average luminance higher than or equal the log-average luminance of the entire image. Each byte of the monochrome watermark is added by updating a luminance value of a pixel of the image. The watermark is taken to be a monochrome image. If the byte of the watermark image represented white color (255) a value α is added to the image pixel luminance value, if it is black (0) the α is subtracted from the luminance value. To extract the watermark, the selected blocks are chosen as the above, if the difference between the luminance value of the watermarked image pixel and the original image pixel is greater than 0, the watermark pixel is supposed to be white, otherwise it supposed to be black.

C. Block Probability in Spatial Domain Method

A binary watermark image is permutated using sequence numbers generated by a secret key and Gray code, and then embedded four times in different positions by a secret key. Each bit of the binary encoded watermark is embedded by modifying the intensities of a non-overlapping block of 8x8 of the blue component of the host image. The extraction of the watermark is by comparing the intensities of a block of 8x8 of the watermarked and the original images and calculating the probability of detecting '0' or '1'.

2.2 Frequency Domain Techniques

Following are some of frequency domain transformation algorithms which can be used individually or in combination with each other to create robust and imperceptible digital watermarks on images.

A. Discrete Cosine Transform (DCT)

It is an orthogonal transformation that is used frequently in image compression and is widely accepted in multimedia standards.

It converts the signal into elementary frequency components. The image is represented as a sum of sinusoids of varying magnitudes and frequencies.

Inverse Discrete Cosine Transform gives us back the original image.

DCT breaks down the image into spectral sub-bands of differing importance. It is similar to Discrete Fourier Transform (DFT) in the way that DCT also converts the signal from spatial domain to frequency domain.

DCT may be global or block based.

Block based DCT

Image is segmented into non-overlapping blocks of 8x8.

A 2D block image (N X N) with pixel intensities s(n_1, n_2) is converted to a transform array of coefficients S(n_1, n_2) by using the equation (2.1):

$$S(k_1,k_2)=\sqrt{\frac{4}{N^2}}C(k_1)C(k_2)\sum_{n_1=0}^{N-1}\sum_{n_2=0}^{N-1}s(n_1,n_2)\cos\left(\frac{\pi(2n_1+1)k_1}{2N}\right)\cos\left(\frac{\pi(2n_2+1)k_2}{2N}\right).$$

where k_1, k_2, n_1, n_2 = 0, 1, 2 ……. N-1, and

$$C(k)=\begin{cases}1/\sqrt{2} & \text{for } k=0\\ 1 & \text{otherwise}\end{cases} \qquad \textbf{(2.1)}$$

The obtained transformation array is of the same size as the original image. Here, the transform domain indices k_1 and k_2 indicate spatial frequencies in the directions of n_1 and n_2 respectively. It is worth noting that $k_1 = k_2 = 0$ corresponds to the average or DC components of the image, while the remaining ones are the AC components which correspond to the higher frequency signals.

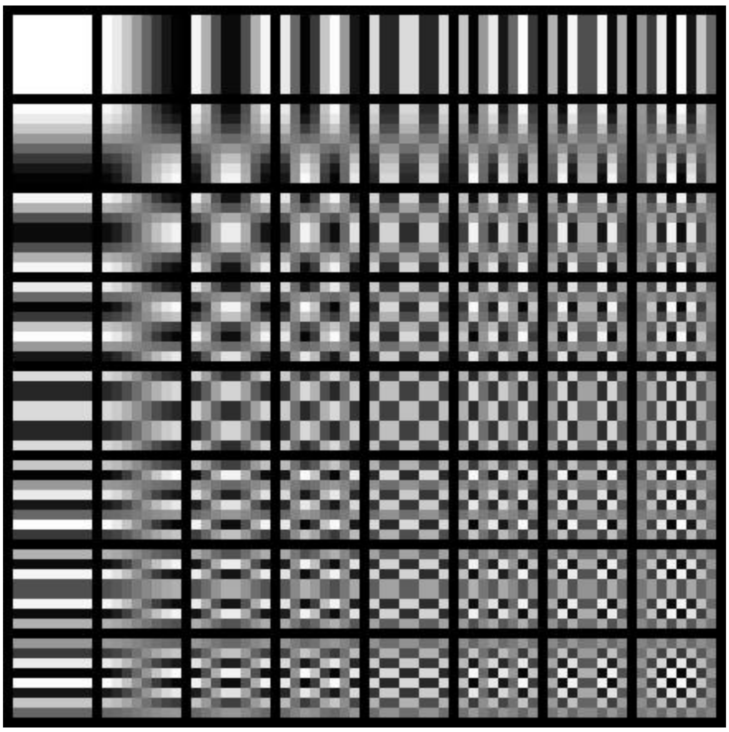

Fig. 2.1. DCT Basis Functions

B. Discrete Wavelet Transform (DWT)

DWT is the discretization of scaling and translation in basic wavelet theory, which has become a widespread transform in many fields such as signal analysis, image processing, computer recognition etc. It captures both the frequency and location information of the signal.

It decomposes the image into 4 sub-bands in by the following algorithm:

One-dimensional DWT is performed on the original image in the direction of every row, obtaining the low frequency component (L) and high frequency component (H) horizontally. Now, one-dimensional DWT is applied again on the obtained components in the direction of every column. Finally, low frequency component in horizontal and vertical directions (LL), low frequency in horizontal direction and high frequency in vertical direction (LH), the high frequency in horizontal direction and low frequency in vertical direction (HL), and high frequency in horizontal and vertical direction are obtained (Fig. 2.2).

Each of the 4 sub-images have half of the length and breadth of the original.

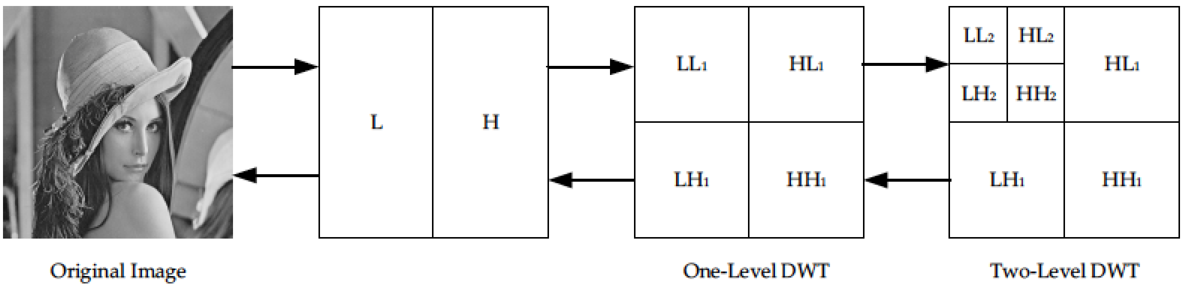

Fig. 2.2. DWT Transform

C. Lifting Wavelet Transform (LWT)

LWT based on the tradition wavelet transform was developed by Wim Sweldens for the construction of biorthogonal wavelets. It uses a simple relationship among all multi-resolution analyses with the same scaling function.

It requires three phases for its implementation:

1. Split – The original dataset x[n] is divided into two subsets with no common elements, whose lengths are half of the original data. Generally

speaking, the signal is divided into odd subset $x_o[n] = x[2n+1]$ and even subset $x_e[n] = x[2n]$.

2. Predict – Odd series is predicted according to even series by the predict operator P, and the errors are called wavelet coefficients d[n].

$$d[n] = x_o[n] - P(x_e[n]) \qquad \textbf{(2.2)}$$

3. Update – Update operator U is put on wavelet coefficients, even series are added to in and the result c[n] is known as scale coefficients.

$$c[n] = x_e[n] + U(d[n]) \qquad \textbf{(2.3)}$$

These 3 stages form the lifting stage. As long as the same P and U are chosen for the forward and inverse transforms, the construction of the original signal will be perfect.

LWT decomposition of the original image produces four bands of data (same as in DWT) namely approximation coefficients matrix (LL) and detail coefficients matrices HL, LH and HH.

LWT has certain advantages over the traditional wavelet transforms:

- More effective
- Requires less memory space
- Transform coefficients are integers, which overcomes the weakness of quantization errors.

D. Singular Value Decomposition (SVD)

The singular-value decomposition (SVD) is a factorization of a real or complex matrix. It is the generalization of the Eigen decomposition of a positive semidefinite normal matrix to any m x n matrix via an extension of the polar decomposition.

SVD theorem states that given a rectangular matrix A with dimensions m x n, it can be written as follows:

$$\mathbf{A = U_{nxn}\, S_{nxm}\, V_{mxm}^{T}} \qquad \mathbf{(2.4)}$$

Where

$U^TU = I_{nxn}$

$V^TV = I_{mxm}$

Columns of U are left singular vectors, U is an orthogonal matrix

S is a diagonal matrix containing singular values

V^T has rows that are right singular vectors, V is an orthogonal matrix

E. Scale Invariant Feature Transform (SIFT)

It is a computer vision algorithm developed and patented in 1999 by David Lowe of the University of British Colombia. It has diverse applications like object recognition, robotic mapping and navigation, image stitching, 3D modeling, gesture recognition, video tracking, individual identification of wildlife and match moving.

It detects the salient, stable feature points in an image. For every such point, it also provides a set of "features" that "characterize/describe" a small image region around the point. These features are invariant to rotation and scale.

These features must not change with:

- Object position/pose
- Scale
- Illumination
- Minor image artifacts/noise/blur

This implies that watermarking done using this algorithm will be have improved robustness towards a variety of geometrical attacks as well.

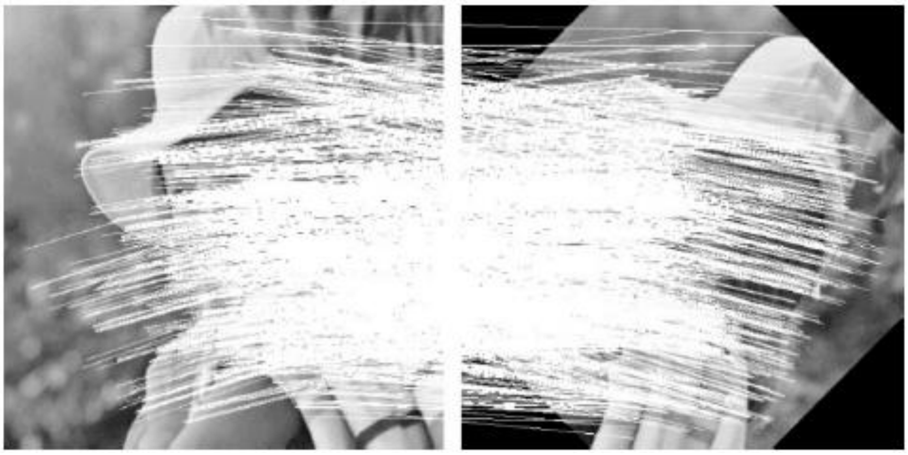

Fig. 2.3. Matching points between image and the same image rotated by 45^o

Fig. 2.4. Matching points between watermarked image and translated image vertically (256 pixels)

Fig. 2.5. Matching feature points between watermarked image and scaled image (0.5)

2.3 Comparison

Spatial domain techniques are easier to implement and have lower computational complexity. But as images are embedded using a simple method, it is relatively easier for a third person to separate out the watermark, thus defeating the whole purpose. It also very susceptible to a wide range of attacks, hence not robust.

Frequency domain techniques, on the other hand, has better imperceptibility and robustness. But the computational cost is higher. For e.g. watermarking in the DCT domain needs preprocessing operations such as inverse entropy coding and inverse quantization. Also, we can combine more than one frequency domain methods to get better results.

An algorithm, combining LWT and DCT, has been proposed in this report because of superior imperceptibility and robustness performance of frequency domain techniques.

Chapter 3

PROPOSED ALGORITHM

The proposed algorithm embeds the watermark into the cover image using second level LWT and DCT. The main properties that we need to keep in mind while image watermarking are imperceptibility and robustness. The watermarking procedure is often a tradeoff between the two. Embedding an image in the perceptually significant components ensures robustness, but the it may be perceptible by the naked eye. On the other hand, if it is hidden in perceptually insignificant components, robustness may be compromised. The right balance between these two factors is to be found.

Applying LWT on the cover image splits it into 4 sub-bands: LL1, LH1, HL1, HH1. LWT is applied on the LL1 sub-band which splits it further into LL2, LH2, HL2, HH2. Then apply DCT is applied on LL2. Watermark is encrypted using Arnold Transform, DCT is applied to it and it is embedded in the LL2 sub-band of the cover image. The extraction process is logically the reverse of the embedding process. As it is non-blind watermarking algorithm, the original cover image will be needed for extraction of the watermark.

Gain Factor – It is a constant which denotes the strength with which the watermark is embedded in the cover image. Its value generally ranges between 0 to 1, where 0 means that no watermark has been embedded. Higher gain values will generally result in reduced invisibility of the watermark, and increased robustness.

Results are obtained by varying the gain factor, and using different cover images. PSNR (Peak Signal-Noise Ratio) values indicate the quality of the watermarked image.

PSNR – It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel scale. It is easily defined using the mean square error (MSE).

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \quad \textbf{(3.1)}$$

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \quad \textbf{(3.2)}$$

Where,

I1 = original image
I2 = modified image
m, n = dimensions of the image
R = Maximum fluctuation in the input image data type

The watermarked image is tested against various attacks, and the corresponding NC (Normalized Coefficient) are noted, which indicate the robustness.

NC – It is a measure of similarity between the original watermark and the extracted watermark.

$$norm\_corr(x,y) = \frac{\sum_{n=0}^{n-1} x[n] * y[n]}{\sqrt{\sum_{n=0}^{n-1} x[n]^2 * \sum_{n=0}^{n-1} y[n]^2}} \quad \textbf{(3.3)}$$

Where,

x = original image
y = modified image
n, n = dimensions of the image

3.1 Embedding Algorithm

1. Apply LWT on the cover image and select LL1 sub-band.
2. Apply LWT on LL1 to obtain LL2 sub-band, where our watermark is supposed to be embedded.
3. As it is a color image, split the LL2 into 3 channels and apply DCT on each one individually to obtain the coefficient matrices.
4. Encrypt the watermark using Arnold Transform for additional security.
5. Split the encrypted watermark into 3 channels and apply DCT on each one.
6. Embed the watermark using the following:

   $$I_{new} = I_{original} + k * I_{watermark}$$

   Where,

   $I_{original}$ = DCT matrix of LH2
   $I_{watermark}$ = Watermark image
   I_{new} = LH2 sub-band of watermarked image
   k = gain factor

7. Apply inverse DCT on the I_{new} to obtain $LL2_{new}$

8. Use $LL2_{new}$ in place of LL2 while applying inverse LWT to obtain $LL1_{new}$.
9. Apply inverse LWT using $LL1_{new}$ in place of LL1 to obtain the watermarked image.

3.2 Extraction Algorithm

1. Apply second level LWT on the watermarked image and cover image, and select the LLw2 and LLc2 sub-bands.
2. Apply DCT on both these sub-bands to obtain the respective coefficient matrices.
3. Extract the watermark using the following:

   $$I_{extracted\_watermark} = (I_{watermarked\_image} - I_{original})/k$$

   Where,

   $I_{watermarked\_image}$ = DCT matrix of LLw2

   $I_{original}$ = DCT matrix of LLc2
4. Apply inverse Arnold Transform to $I_{extracted\_watermark}$.
5. The resultant image is the extracted watermark.

3.3 Experimental Results and Analysis

Performance of the proposed algorithm is analyzed on the basis of PSNR and NC values.

A. The PSNR value is noted at various values of gain factor, in absence of any attack (Table 1)

Cover Image: lena.jpg **Size:** 512x512
Watermark: moon.jpg **Size:** 128x128

Table 3.1

S. No.	Gain factor	PSNR(dB)	NC values
1.	0.01	67.3942	0.1263
2.	0.04	51.0695	0.9615
3.	0.05	48.8669	0.9974
4.	0.08	44.9222	0.9958
5.	0.1	43.0308	0.9913
6.	0.12	41.4007	0.9982
7.	0.15	39.4881	0.9967
8.	0.18	37.9070	0.9982
9.	0.2	37.0125	0.9955
10.	0.25	35.0814	0.9957

(a) Cover image, 'lena.png' (size 512x512)

(b) Watermark, 'moon.png' (size 128x128)

(c) Watermarked image

(d) Extracted Watermark

Fig 3.1. The watermarking procedure (at gain value = 0.15)

B. The PSNR values are noted at gain value of 0.10 for different cover images (Table 2)

Watermark: moon.jpg **Size:** 128x128

Table 3.2

S. No.	Cover Image	PSNR(dB)	NC values
1.	Baboon	43.0729	0.9834
2.	Yosemite	43.0389	0.9901
3.	Peppers	44.9307	0.6533
4.	Colosseum	43.0663	0.9853
5.	Mona Lisa	43.0366	0.9910

C. NC values of extracted watermark against original watermark are noted after various attacks on the watermarked image.
Observations are made at two different gain values of 0.10 and 0.15 (Table 3)

Table 3.3

S. No.	Attack	Gain Factor	NC values
1.	JPEG compression	0.10	0.9811
		0.15	0.9769
2.	Salt and pepper noise (density=0.001)	0.10	0.9940
		0.15	0.9967
3.	Salt and pepper noise (density=0.01)	0.10	0.9967
		0.15	0.9985
4.	Salt and pepper noise (density=0.02)	0.10	0.9975
		0.15	0.9993
5.	Speckle (variance = 0.005)	0.10	0.9816
		0.15	0.9873
6.	Speckle (variance = 0.01)	0.10	0.9911
		0.15	0.9802
7.	Speckle (variance = 0.02)	0.10	0.9663
		0.15	0.9656
8.	Gaussian (sigma = 0.5)	0.10	0.9294
		0.15	0.9318
9.	Gaussian (sigma = 1)	0.10	0.8077
		0.15	0.7976
10.	Gaussian (sigma = 2)	0.10	0.6889
		0.15	0.6542
11.	Averaging filter	0.10	0.7180
		0.15	0.6901
12.	Median filter	0.10	0.7924
		0.15	0.8023
13.	Histogram equalization (in RGB space)	0.10	0.8378
		0.15	0.8312
14.	Histogram equalization (in HSV space)	0.10	0.5599

		0.15	0.5734
15.	Rotation (2^0)	0.10	0.7737
		0.15	0.7215
16.	Rotation (5^o)	0.10	0.7635
		0.15	0.7256
17.	Crop	0.10	0.8943
		0.15	0.8741
18.	Resize (0.75)	0.10	0.3922
		0.15	0.3941
19.	Salt and pepper noise (density=0.01) + Gaussian (sigma = 1)	0.10	0.8426
		0.15	0.8235
20.	Speckle (variance = 0.02) + Median filter	0.10	0.8570
		0.15	0.8246

We can see from Table 1 that higher the gain value, lower is the PSNR value. i.e. as the degree of embedding of watermark in the cover image increases, its imperceptibility decreases. Highest PSNR value is obtained at a gain factor of 0.01.

In Table 3, we notice that the NC values are satisfactorily high for most types of attacks, but are low for geometric attacks. That means the algorithm performs well for most common attacks like image compression, filtering, noise addition, but the algorithm is not optimal in the case of geometric attacks.

Also, we notice that, generally, higher NC values are obtained in case of a higher gain factor for the same attack on the watermarked image. Thus, we can conclude that higher the gain factor, more is the robustness, and lower the gain factor, better is the visual quality of the watermarked image.

CONCLUSION

This report is a study of digital image watermarking, its importance, real life applications, and its various techniques. Digital image watermarking is the answer to numerous problems related to image security, privacy, copyright issues etc.

An algorithm based on Lifting Wavelet Transform and Discrete Cosine transform is proposed for watermarking of color images. Color images a greater space for embedding the watermark as compared to grayscale images. Here, both the cover image and the watermark are taken as color images, but a grayscale watermark can also be embedded in a color image.

Combined usage of LWT and DCT results in better performance as compared to applying the two methods individually. Robustness and visual quality both are improved. To provide additional security and confidentiality, the watermark is encrypted using Arnold transform before being embedded in the cover image.

We analyze the results of image watermarking by using PSNR values (for image quality) and NC values (for robustness).

This algorithm can be used to secure images in various sectors like medicine, professional photography, education, entertainment etc. It can be further improved to enhance its robustness against geometrical attacks.

REFERENCES

1. Aditi Zear, Amit Kumar Singh, Pardeep Kumar (2016) A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine.
2. Chunxing Wang, Fei Han, Xiaomei Zhuang (2015) Robust Digital Watermarking Scheme of Anaglyphic 3D for RGB Color Images.
3. Rashmi Shrivastava (2017) DWT based invisible watermarking on images
4. S.E. Tsai, K.C. Liu, S.M. Yang (2017) An Efficient Image Watermarking Method Based on Fast Discrete Cosine Transform Algorithm
5. Yunpeng Zhang, Chengyou Wang, Xiaoli Wang and Min Wang (2017) Feature-Based Image Watermarking Algorithm Using SVD and APBT for Copyright Protection
6. Chengyou Wang, Yunpeng Zhang, Xiao Zhou (2018) Robust Image Watermarking Algorithm Based on ASIFT against Geometric Attacks
7. Gaurav Gupta, Amit Mahesh Joshi, Kanika Sharma (2015) An efficient robust image watermarking based on AC prediction technique using DCT technique
8. Amy Tun, Yadana Thein (2013) Digital Image Watermarking Scheme Based on LWT and DCT.
9. Palak Jain, Umesh Ghanekar (2018) Robust watermarking technique for textured images
10. Min Li, Ting Liang, Yu-jie He (2013) Arnold Transform Based Image Scrambling Method
11. S. Thabasu Kannan, S. Azhagu Senthil (2015) A Frame Work for Various Watermarking Algorithms
12. Abdullah Bamatraf, Mohd. Najeeb B. Mohd. Salleh, Rosziati Ibrahim (2011) Digital watermarking algorithm using LSB
13. Jamal A. Hussein (2010) Spatial Domain Watermarking Scheme for Colored Images Based on Log-average Luminance