"DIGTAL IMAGE WATERMARKING USING DWT & ARNOLD TRANSFORM"

DISSERTATION-II

Submitted in partial fulfillment of the

Requirement for the award of the

Degree of

MASTER OF TECHNOLOGY

IN

Digital Signal Processing

By

KAUSAV KUMAR

REG. No.-11201298

Under the Esteemed Guidance of

Mr. Vineet Kumar

School of Electrical and Electronics Engineering

Lovely Professional University

Punjab

DECEMBER 2016

CERTIFICATE

This is to certify that the Thesis titled "**Digital Image Watermarking Using DWT & Arnold Transform**" that is being submitted by "Kausav Kumar" is in partial fulfillment of the requirements for the award of MASTER OF TECHNOLOGY DEGREE (Digital Signal Processing), is a record of bonafide work done under my guidance. The contents of this Thesis, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Mr. Vineet Kumar

Assistant Professor

(Lovely Professional University)

Objective of the Thesis is satisfactory / unsatisfactory

Examiner I **Examiner II**

ACKNOWLEDGEMENT

I would like to thank **LOVELY PROFESSIONAL UNIVERSITY** for giving me opportunity to use their resources and work in such a challenging environment. I am grateful to the individuals who contributed their valuable time towards my thesis. I wish to express my sincere and heart full gratitude to my guide **Mr. Vineet Kumar** Assistant Professor, who guided me to take up this thesis in sync with global trends in scientific approach. I would also like to extend my gratitude to my friends and family who always encouraged and supported me in this thesis work. Last but not the least; I would like to thank all the staff members of Department of Electronics and Communication engineering who have been very patient and co-operative with us.

KAUSAVKUMAR

Reg. No. 11201298

CERTIFICATE

This is to certify that **Kausav Kumar** bearing Registration no. **11201298** has completed objective formulation of thesis titled, "**Digital Image Watermarking Using DWT & Arnold Transform**" under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the thesis has ever been submitted for any other degree at any University.

The thesis is fit for submission and the partial fulfillment of the conditions for the award of **MASTER OF TECHNOLOGY (Digital Signal Processing).**

Mr. Vineet Kumar
Assistant Professor
Lovely Professional University
Phagwara, Punjab.
Date :

DECLARATION

I, student of **MASTER OF TECHNOLOGY (Digital Signal Processing)** under Department of **ELECTRONICS AND COMMUNICATION ENGINEERING** of Lovely Professional University, Punjab, hereby declare that all the information furnished in this dissertation-II report is based on my own intensive research and is genuine.

This dissertation does, to the best of my knowledge, contain part of my work which has been submitted for the award of my degree either of this university or any other university without proper citation.

Date: **KAUSAV KUMAR**

Registration No. 11201298

ABSTRACT

Pictures and images are form of art, which is a way of connecting people and expressing their feelings and someone else try to steal that art, tamper that art or forge that art; it's got to be hurt on a profound level. Now a day, there are many tools to tamper with digital images. So, it is necessary to protect them. So, watermarking is one of the ways to protect and detect tampering in an image. This thesis deals with a robust watermarking. The commonly used watermarking applications include copyright related applications, medical forensics and military applications and content authentication applications. A discrete wavelet transform (DWT)-based watermarking scheme for this purpose is proposed in this communication. In, this thesis DWT of both RGB and gray scale image is taken and then apply watermarking on their HH1 portions, which will ultimately give desired watermarked images. The low frequency subband of wavelet domain and the rescaled version of original image are utilized in the watermark construction process. With the help of Arnold Transform a scrambled version of watermark is obtained. The operation of embedding and extraction of watermark is done in high frequency domain of DWT. The modifications are so small that it can't be perceived by human eyes. To measure image quality Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are computed. In addition, the accuracy of the proposed method is measured using common image processing operations. Then, a comparison is made against other techniques.

Table of Contents

Table of Contents Continues...

List of Tables

List of Figures

CHAPTER 1

INTRODUCTION

1.1 History of Image Processing

In ancient times, when people wanted to make their portraits or make the visual representation of any of their memories (good or bad), they went to painter and that person tried to capture their needs on canvas. It was a very time consuming process of taking image.

A visual representation of something is called image. In other words, a physical likeness or representation of anything (an animal, a person or a certain thing etc.) sculptured, painted or otherwise made visible is called image.

But it all changed in 1820s when the concept of **Camera Obscura** is discovered. Camera Obscura is a Latin word which means 'Dark Room' also referred as pinhole image. It is a natural optical concept when light passing through a small hole into a darkened room produces an image on the opposite wall, during a partial eclipse of the sun. The surroundings of the projected image have to be relatively dark for the image to be clear; so many camera obscura experiments were performed in literally dark rooms.

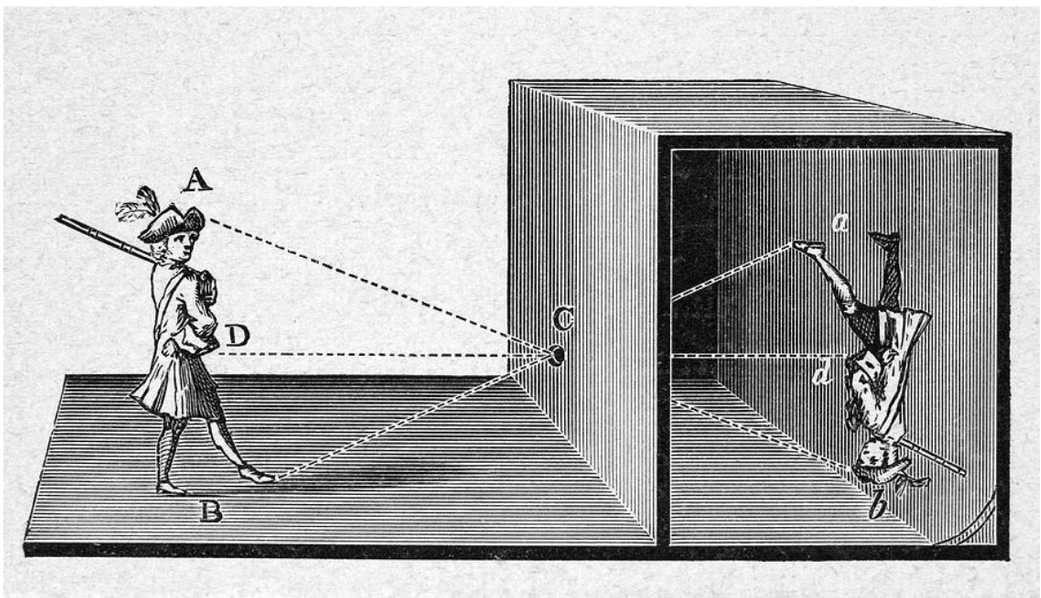


Fig. 1- Camera Obscura

When the concept of camera obscura is combined with other concept then the photography is produced. The other concept is an observation that some substances are visibly altered by exposure to light.

In 1816 Nicéphore Niépce, using paper coated with silver chloride, succeeded in photographing the images formed in a small camera. The photographs were negatives. That's how photography was introduced to the world.

1.1.1 Development Of Digital Photography

In 1957, a team led by Russell A. Kirsch at the National Institute of Standards and Technology developed a binary digital version of an existing technology, the wire photo drum scanner, so that alphanumeric characters, diagrams, photographs and other graphics could be transferred into digital computer memory. One of the first photographs scanned was a picture of Kirsch's infant son Walden. The resolution was 176x176 pixels with only one bit per pixel, i.e., stark black and white with no intermediate gray tones, but by combining multiple scans of the photograph done with different black-white threshold settings, grayscale information could also be acquired.

Fig. 2 - Walden Kirsch as scanned into the SEAC computer in 1957

The charge-coupled device (CCD) is the image-capturing optoelectronic component in first-generation digital cameras. It was invented in 1969 by Willard Boyle and George E. Smith at AT&T Bell Labs as a memory device. The lab was working on the Picture

phone and on the development of semiconductor bubble memory. Merging these two initiatives, Boyle and Smith conceived of the design of what they termed "Charge 'Bubble' Devices". The essence of the design was the ability to transfer charge along the surface of a semiconductor. It was Dr. Michael Tompsett from Bell Labs however, who discovered that the CCD could be used as an imaging sensor. The CCD has increasingly been replaced by the active pixel sensor (APS), commonly used in cell phone cameras.

- 1973 – Fairchild Semiconductor releases the first large image-capturing CCD chip: 100 rows and 100 columns.[36]
- 1975 – Bryce Bayer of Kodak develops the Bayer filter mosaic pattern for CCD color image sensors
- 1986 – Kodak scientists develop the world's first megapixel sensor.

The web has been a popular medium for storing and sharing photos ever since the first photograph was published on the web by Tim Berners-Lee in 1992 (an image of the CERN house band Les Horribles Cernettes). Today popular sites such as Flickr, Picasa, Instagram and PhotoBucket are used by millions of people to share their pictures.

1.2 Definition of Image

A digital image is a numeric representation of (normally binary) a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. By itself, the term "digital image" usually refers to raster images or bitmapped images.

An image f(x,y) that has been digitized both in spatial coordinates and intensity values. The value of f at any point (x,y) is proportional to the brightness (or gray level) of the image at that point. A digital image can be considered a matrix (or 2-D array) whose row and column indices identify a point in the image and the corresponding matrix element value identifies the gray level at that point. Fig.3 shows digital representation of an image.

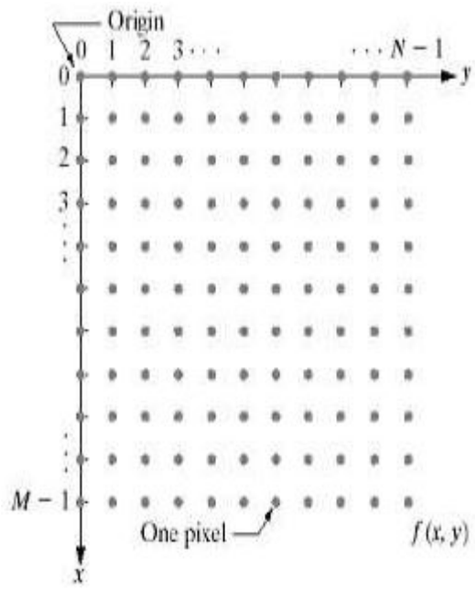


Fig. 3:- Digital Image Representation

1.3 Image Tampering

Modern digital technology and the availability of increasingly powerful image processing tools can easily manipulate the digital images without leaving obvious visual traces of having been tampered, so there is an urgent need to identify the authenticity of images. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In this research work, a comprehensive study has been undertaken for accessing and analyzing the threat of Digital Image tampering for security. Various methods and research issues involving the tampering detection and image authentication have been discussed and suitable recommendations for security scenario have been presented.

Digital media like digital images and documents should be authenticated against the forgery due to the availability of powerful tools in the field of editing and manipulating these media. Digital imaging has matured to become the dominant technology for creating, processing, and storing pictorial memory and evidence. Though this technology brings many advantages, it can be used as a misleading tool for hiding facts and evidences. This is because today digital images can be manipulated in such perfection that forgery cannot be detected visually. In fact, the security concern of digital content has arisen a long time ago and

different techniques for validating the integrity of digital images have been developed. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In medical field physicians and researchers make diagnoses based on imaging. The introduction and rapid spread of digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity. With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media. This motivates the need for detection tools that are transparent to tampering and can tell whether an image has been tampered just by inspecting the tampered image.

1.3.1 Types of Image Tampering

Image tampering is a digital art which needs understanding of image properties and good visual creativity. One tampers images for various reasons either to enjoy fun of digital works creating incredible photos or to produce false evidence. No matter whatever the cause of act might be, the forger should use a single or a combination series of image processing operations. The various commonly used image tampering techniques are as follows.

a.) **Copy-move:** This is the most common kind of image tampering technique used, where one needs to cover a part of the image in order to add or remove information. Textured regions are used as ideal parts for copy-move forgery. Since textured areas have similar color, dynamic range, noise variation properties to that of the image, it will be unperceivable for human eye investigating for incompatibilities in image statistical properties. For Example:- An image of clock is forged using copy-move as shown in Fig. 4

Fig. 4:- Copy- Move Forgery

b.) **Image-splicing:** It is defined as a paste-up produced by sticking together photographic images. While the term photomontage was first used for referring to

an art form or the act of creating composite photograph can be traced back to the time of camera invention.

c.) **Resize:** This operation performs a geometric transformation which can be used to shrink or enlarge the size of an image or part of an image. Image reduction is performed by interpolating between pixel values in local neighborhoods.

d.) **Cropping:** It is a technique to cut-off borders of an image or reduces the canvas on which an image is displayed. Generally this kind of operation is used to remove border information which is not very important for display.

e.) **Noising or Blurring:** Tampering images with operations described above like image splicing, scaling, rotating can be clear to a viewer in the form of artifacts like improper edges, aliasing defects and tone variations. These obvious traces of tampering can be made imperceptible by applying small amount of noise or blur operations in the portions where the tampering defects are visible.

Some of the known image tampering techniques and tamper detection techniques are tabulated in table 1.1 given below:

Table 1.1- Some Image Tampering Techniques & Detection Techniques

Image Tamper Technique	**Image Operations/Tools Used**	**Tamper Detection Techniques**
Copy-Move	Copy, Move,	Paste, Selection
Exhaustive Search, Block Matching	(Using DCT Or PCA),	Autocorrelation
Image-Splicing	Copy, Resize, Move,	Paste, Selection
Bi-Spectral Analysis, Bi-Coherence	Analysis, Noise Variation Estimation	Alpha Variance Estimation,
Higher Order Statistics	Re-Sampling Resize, Crop, Rotate,	Scale, Skew, Stretch
Expectation And Maximization	(EM) Algorithm	Double JPEG Compression JPEG Encoding JPEG Artifact Estimation

1.4 Effects of Tampering In Different Areas of Society

Tampering is normally done to cover objects in an image in order to either produce false proof or to make the image more pleasant for appearance.

In the field of medicine, reports of patients are highly confidential and are always supposed to be authentic. Medical images are produced in most of the cases as proof for unhealthiness and claim of disease. Since medical images are dealing with huge amounts of money, people can get lured to tamper images for claiming medical insurance. Also medical results are generally placed as proofs or alternatives for avoiding punishments in courts. So this type of tampering with medical images disturbs the security of the common individual.

In the field of education, different tampering techniques give us false information which in turns leads to the delivery of incorrect data to the organization. Students carried out large amount of forgery with their documents for their own benefit. This disturbs the security of the management which is an urgent issue to be solved.

In the field of agriculture, tampering is also done with the different images used during the training of the farmers which results to the misguidance to the agricultural students. This type of forgery imbalance the security management which is to be solve soon.

In the field of e-commerce, most of the transactions are carried out through internet whether it is money transfer, Shopping purpose, bill payment etc. In this, Security of the customer's details is the prime focus of the government. But many unauthorized users manipulate the data which results in serious crime. This corrupted or disturbed security management leads to serious crime. So in the era of digital technology, tampering is a major threat to the technology which requires immediate attention.

1.5 Image Watermarking

Watermark is an invisible signature embedded inside an image to show authenticity or proof of ownership. It discourages unauthorized copying and distribution of images over the internet. Watermarking Ensures a digital picture has not been altered. Software can be used to search for a specific watermark.

Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song and video) within the signal itself. It is a concept closely related to

steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence.

Originally a watermark is a more or less transparent image or text that has been applied to a piece of paper, another image to either protects the original image or to make it harder to copy the item e.g. money watermarks or stamp watermarks.

A transparent watermark is added to a photo by changing the image on the pixel level (a pixel is one dot of image). The pixels that will make up the resulting watermark is changed more or less in the direction of the watermarking image, if e.g. the watermark is 50% transparent, 50% of the RGB(Red, Green & Blue) values are deducted from the original image and 50% of the RGB values from the watermark is added to the image.

When adding a watermark to a photo a clear signal is implied that this photo should not be copied or used without proper consent. Also if both a highly visible watermark and an almost hidden watermark is added, it will be much easy for the thief to overlook the invisible and thereby adding more protection to the images.

1.5.1 Aspects of Watermarking

The major aspect of watermarking is to find the balance among different-2 traits such as robustness to various attacks, security and invisibility. Invisibility of watermark depends upon intensity of embedded watermark. Good invisibility is achieved from less intensity watermark. So we must select the minimum yet balanced intensity to embed a watermark. For robustness to increase it requires a stronger embedding, which in turn increases the visual quality of an image. For a watermark to be effective, it should meet the following features:

1.) **Imperceptibility** - Watermark should be invisible as so that data quality is not degraded and attackers are prevented from finding and deleting it. A watermark is called imperceptible if the watermarked content is almost equivalent to the original content.

2.) **Readily Extractable** - The data owner or an independent control authority should be able to easily extract the watermark.

3.) **Unambiguous** - The watermark retrieval should unambiguously identify the data owner.

4.) **Robustness** – It should tolerate some of the common image processing attacks. A watermark is called robust if it resists some class of transformations. Robust watermarks may be used in copyright protection applications to carry copy and access control information.

1.5.2 Types of Watermarking

The digital image watermarking scheme can be divided into following two categories:

1.) Visible digital image watermarking
2.) Invisible image watermarking

Visible digital image watermarking: - In visible watermarking, the information can be seen in the picture or video. Basically, the information is a text or a logo which identifies the owner of the original document.

Invisible image watermarking: - In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be seen with naked eyes. Further, the invisible watermarking is categorized into two categories:-

1. **Robust watermarking: -** a robust watermark is generally used for copyright protection and ownership identification because it is designed to withstand attacks such as common image processing operations attempting to remove or destroy the watermark. These algorithms ensure that the image processing operations cannot delete the embedded watermark signal.
2. **Fragile watermarking: -** A fragile or semi-fragile watermark is mainly applied to content authentication and integrity verification because it is very sensitive to attacks, i.e., it can detect slight changes to the watermarked image with high probability.

1.6 Image Tampering Detection Algorithms

These algorithms use various techniques for tamper detection. These include Principal component Analysis (PCA), Discrete Cosine Transform (DCT), Discrete Wavelet Transforms (DWT), Singular Value Decomposition (SVD) etc. PCA frequently used statistical technique for data dimension reduction. This method divided the image in multiple principal components to analyze different desired components. PCA based algorithms are applied in

the areas of Image Color Reduction and Object Orientation. However, the major drawback of PCA is its insensitivity to relative scaling of the original variables. DCT works in frequency domain. It expresses a sequence of finitely data points in terms of a sum of cosine functions oscillating at different frequencies. DCT has numerous applications as in lossy compression of audio (e.g. MP3) and images (e.g. JPEG), image compression etc. However, DCT based methods do not produce well results in case of image blurring and video frame reconstruction applications.

DWT is wavelet transform for which the wavelets are discretely sampled. An approximation to DWT is used for data compression if signal is already sampled. It is an efficient approach to lossless compression. As compared to above methods, DWT has numerous drawbacks. Unlike PCA, DWT has high cost of computing. In contrast to DCT, DWT has certain limitations like signal blurring, ringing noise near edge regions in images or video frames, longer compression time, lower quality than JPEG at low compression rates etc.

Another method called Singular Value Decomposition (SVD) is being increasingly used for tampering detection. SVD is a very robust technique. The technique involves refactoring of given digital image in three different feature based matrices. The small set called singular values preserve the useful features of the original image. The advantages of SVD include lesser memory requirement. It has many applications in data analysis, signal processing, pattern recognition, image compression, noise reduction, image blurring, face recognition, forensics, embedding watermarking to an image.

1.7 Discrete Wavelet Transform

1.7.1 Wavelet Transform

The wavelet transform is a transform similar to the Fourier transform (or much more to the windowed Fourier one as we see later) with a completely different merit function. The main difference is this: Fourier transform decomposes the signal into sines and cosines - e. g. the functions localized in Fourier space; in contrary the wavelet transform uses functions that are localized in both the real and Fourier space. The dependence on the merit function and the localization can be seen from the next table. All the mentioned transforms in the table are

simply defined using convolutions with a given functions, but their meaning in terms of time and frequency resolution is different.

Table 1.2: Different Transforms and Their Resolutions

Definition	**Merit Function in Real Space**	**Merit Function in Fourier Space**	**Resolution in real space**	**Resolution in Fourier space**
$f(x) = \int_{-\infty}^{\infty} f(u)\delta(x-u)du$	Delta Function	Sine and Cosine	Maximal: transform returns the same signal	None
$f(x) = \int_{-\infty}^{\infty} f(u)\exp(iux)\exp(-x^2)\,du$	Damped Sine and cosine	Shifted gauss-like	Depends on Damping	Depends on Damping
$f(x) = \int_{-\infty}^{\infty} f(u)\exp(iux)\,du$	Sine and cosine	Delta Function	None	Maximal: transform returns Frequency Spectrum

In the table three different similar transforms are introduced.

1. First one, a Dirac function is completely localized in the real space - transform using this function gives simply the identical function with the input signal.
2. The next merit function is a damped sine and cosine function (e. g. small wave - wavelet) - transform using this function is a mentioned Wavelet transform. As the merit function, also transform result will be localized in both the spaces.
3. Last one is the sine and cosine function - transform using this function is a Fourier Transform.

As it is seen from the table, for the Fourier transform we don't get any resolution in real space (for time series it means the time resolution). For the stationary signals this doesn't represent any problem. As we need to analyze also non-stationary signals (most of the sounds for example), we have to use something else. The easiest way is to use the Short-Time Fourier Transform (or Windowed Fourier Transform).

Short-time Fourier transform simply uses a window function to choose the time area for which the frequencies are computed. Its main disadvantage is the fact that by this way we always have: poor frequency and good time resolution for the low frequencies; good

frequency and poor time resolution for the high frequencies. This is the contrary of what we usually need for the non-stationary signals.

The solution is to use the wavelet transform, which uses widows of different size for computing the high and low frequencies. Therefore, it can improve the frequency resolution of the low frequencies and the time resolution of the high frequencies. However, the uncertainty principle is valid here, so we cannot expect improvement of both time and frequency resolution for a given point in time-frequency plane; we can only vary the ratio between its time and frequency uncertainty.

The wavelet transform, which we have already seen in the previous Table, can be generally written as

$$F(a,b) = \int_{-\infty}^{\infty} f(x)\varphi^{*}_{(a,b)}(x)dx \quad \text{..... (1)}$$

Where the * is the complex conjugate symbol and function \psi is some function which can be different obeying some rules.

1.7.2 Implementation of Wavelet Transform

As it is seen, the Wavelet transform is in fact an infinite set of various transforms, depending on the merit function used for its computation. This is the main reason, why we can hear the term "wavelets transform" in very different situations and applications. There are also many ways how to sort the types of the wavelet transforms. Here is the division based on the wavelet orthogonality.

- **Orthogonal wavelets** are used to develop the discrete wavelet transform
- **Non-orthogonal wavelets** are used to develop the continuous wavelet transform

There are more wavelet types and transforms, but those two are most widely used and can serve as examples of two main types of the wavelet transform: redundant and non-redundant ones.

- **The discrete wavelet transform** returns a data vector of the same length as the input is. Usually, even in this vector many data are almost zero. This corresponds to the fact

that it decomposes into a set of wavelets (functions) that are orthogonal to its translations and scaling. Therefore we decompose such a signal to a same or lower number of the wavelet coefficient spectrum as is the number of signal data points. Such a wavelet spectrum is very good for signal processing and compression, for example, as we get no redundant information here.

- **The continuous wavelet transform** in contrary returns an array one dimension larger than the input data. For a 1D data we obtain an image of the time-frequency plane. We can easily see the signal frequencies evolution during the duration of the signal and compare the spectrum with other signals spectra. As here is used the non-orthogonal set of wavelets, data are correlated highly, so big redundancy is seen here. This helps to see the results in a more humane form.

1.7.3 Discrete Wavelet Transform (DWT)

The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. In other words, this transform decomposes the signal into mutually orthogonal set of wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for the discrete time series sometimes called discrete-time continuous wavelet transform (DT-CWT).

The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned everywhere e. g. the dilation equation.

$$\emptyset(x) = \sum_{k=-\infty}^{\infty} a_k \, \emptyset(Sx - k) \quad \text{..... (2)}$$

Where S is a scaling factor (usually chosen as 2). Moreover, the area between the function must be normalized and scaling function must be orthogonal to its integer translates e. g.

$$\int_{-\infty}^{\infty} \emptyset(x)\emptyset(x + l)dx = \delta_{0,l} \quad \text{..... (3)}$$

After introducing some more conditions (as the restrictions above goes not produce unique solution) we can obtain results of all this equations, e. g. finite set of coefficients which define the scaling function and also the wavelet. The wavelet is obtained from the scaling function as

$$\varphi(x) = \sum_{k=-\infty}^{\infty} (-1)^k \, a_{N-1-k} \varphi(2x - k) \quad \text{..... (4)}$$

Where N is an even integer. The set of wavelets then forms an orthogonal basis which we use to decompose signal. Note that usually only few of the coefficients are nonzero which simplifies the calculations.

Examples

Here, some wavelet scaling functions and wavelets are plotted. The most known family of orthonormal wavelets is a family of Daubechies. These wavelets are usually denominated by the number of nonzero coefficients, so we usually talk about Daubechies 4(as shown in Fig.9 & Fig.8), Daubechies 6 etc. wavelets Roughly said, with the increasing number of wavelet coefficients the functions become more smooth. See the comparison of wavelets Daubechies 4. Another mentioned wavelet is the simplest one, the Haar wavelet (as shown in fig.5 & fig.6), which uses a box function as the scaling function.

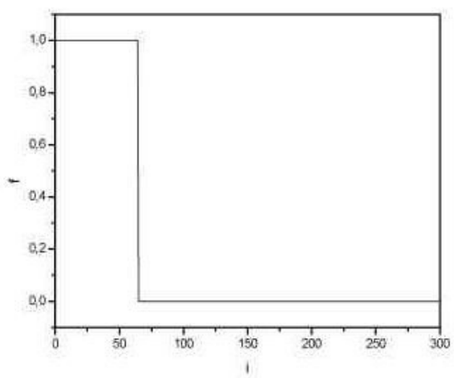


Fig. 5:- Haar Scaling Function

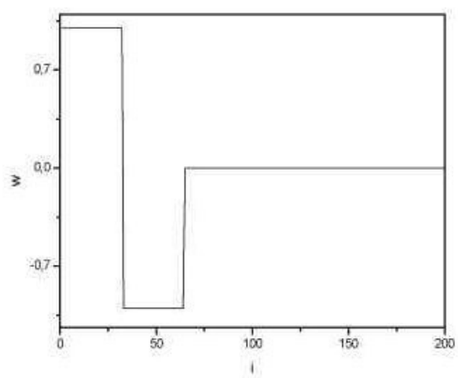


Fig. 6:-Haar wavelet

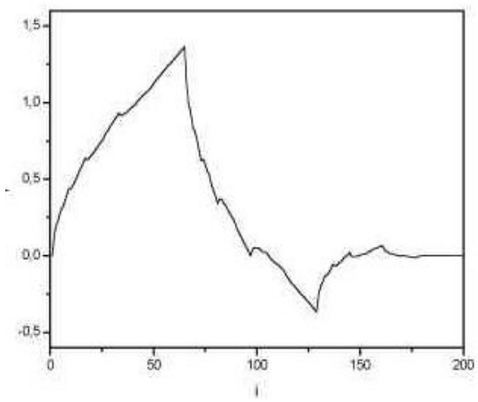


Fig. 7:- Daubchies 4 scaling Function

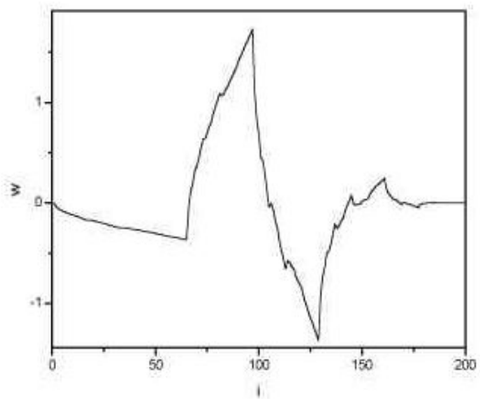


Fig. 8:- Daubchies 4 Wavelet

Discrete wavelet transform algorithm

There are several types of implementation of the DWT algorithm. The oldest and most known one is the Malaat (pyramidal) algorithm. In this algorithm two filters - smoothing and non-smoothing one are constructed from the wavelet coefficients and those filters are recurrently used to obtain data for all the scales. If the total number of data D=2^N is used and signal length is L, first D/2 data at scale L/2^ (N-1) are computed, than (D/2)/2 data at scale L/2^ (N-2) ... etc up to finally obtaining 2 data at scale L/2. The result of this algorithm is an array of the same length as the input one, where the data are usually sorted from the largest scales to the smallest ones.

Similarly the inverse DWT can reconstruct the original signal from the wavelet spectrum. Note that the wavelet that is used as a base for decomposition cannot be changed if we want to reconstruct the original signal, e. g. by using Haar wavelet we obtain a wavelet spectrum; it can be used for signal reconstruction using the same (Haar) wavelet.

Examples

In the next picture a 1024 data long sine signal with linearly increasing frequency. In the next three images there are discrete wavelet spectra obtained using the Haar (in fig.10), Daubechies 4 (in fig. 11) wavelets as a basis functions.

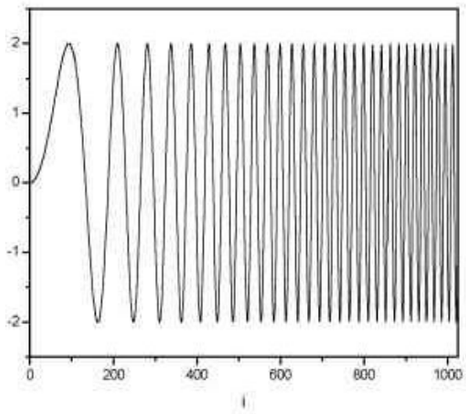


Fig. 9: Sine Function With Increasing Frequency

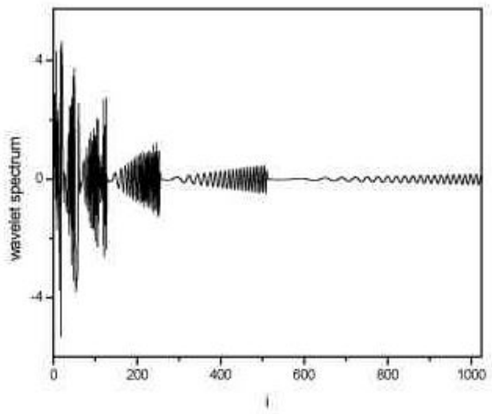


Fig.10:- DWT spectrum using Haar Wavelet

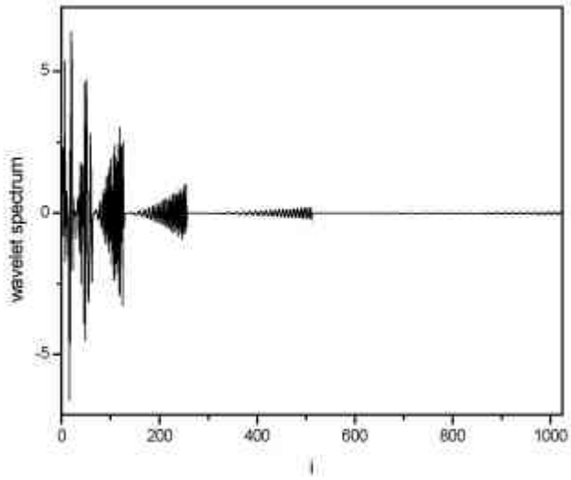


Fig. 11:- DWT Spectrum using Daubchies 4 wavelets

1.7.4 1D-DWT

The 1D-DWT can be viewed as the multi-resolution decomposition of a sequence. It takes a length N sequence LN (n)], and generates and output sequence of length N. The output is a multi-resolution representation of LN (n). The highest resolution level is of length N/2, the next resolution level is of length N/4, and so on. We denote the number of frequencies or resolutions levels or levels with the symbol L. The 1D-DWTfilter bank structure, realizing the 1D-DWTdyadic decomposition, is illustrated in Fig. 12

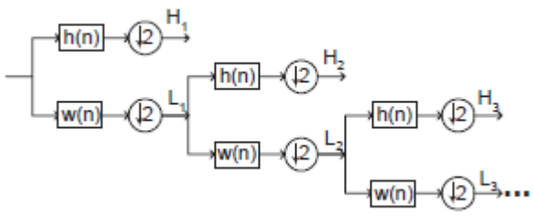


Fig.12:- 1D-DWT Decomposition

Typically, h(n) and w(n) of Fig. 10 are convolutional Quadrature Mirror Filters (QMF).We denote N_H and N_LL the number of taps of the high-pass h(n) and low-pass w(n) filters respectively, and define N_W=max{ N_H, N_L} For the sequence of low and high frequency coefficients of decomposition layer j we use the symbols L_j(n) and H_j(n)] respectively. Hence, using mathematical notations the low and high frequency coefficients of decomposition level j are computed as follows:

$$L_{j+1}[n] = \sum_{i=0}^{N_L-1} w[i] \times L_j\,[2n-i] \quad \text{..... (5)}$$

$$H_{j+1}[n] = \sum_{i=0}^{N_H-1} h[i] \times L_j\,[2n-1-i] \quad \text{..... (6)}$$

Where j={0,1,…….,L-1}, n={0,1,….,(N/2^{j+1}-1} and L_0[n] =lN(n)

1.7.5 2D-DWT

The 2D-DWT binary-tree decomposition is illustrated in Fig. 11. For each level the input signal is filtered along rows and the resulted signal is filtered along columns.

$$L_{j+1}[row][m] = \sum_{i=0}^{N_L-1} w[i] \times LL_J\,[row][2m-i] \quad \text{..... (7)}$$

$$H_{j+1}[row][m] = \sum_{i=0}^{N_H-1} h[i] \times LL_J\,[row][2m-1-i] \quad \text{..... (8)}$$

In this way, the 2D decomposition of an input signal lN[M][N], with M columns and N rows, is described by the following equations:

$$LL_{j+1}[n][col] = \sum_{i=0}^{N_L-1} w[i] \times L_j[2n-i][col] \quad \text{..... (9)}$$

$$LH_{j+1}[n][col] = \sum_{i=0}^{N_H-1} h[i] \times L_j[2n-1-i][col] \quad \text{..... (10)}$$

$$HL_{j+1}[n][col] = \sum_{i=0}^{N_L-1} w[i] \times H_j[2n-i][col] \quad (11)$$

$$HH_{j+1}[n][col] = \sum_{i=0}^{N_H-1} h[i] \times H_j[2n-1-i][col] \quad (12)$$

Where j={0,1,…L-1}, row={0,1,….,N/2^j-1}, m={0,1,…,M/2^{j+1}-1}, col={0,1,….,M/2^{j+1}-1}, n={0,1,…,N/2^{j+1}-1} and LL_0[n][m]=lN[n][m].

In the rest of this document we use the term layer to indicate both intermediate and output signals, i.e. L_j, H_j, LL_j, LH_j, HH_j and HL_j , while level is used for each decomposition stage.

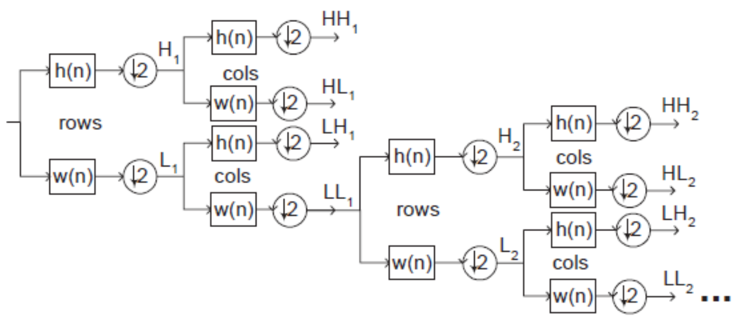


Fig.13- The 2D-DWT Decomposition

1.8 Arnold Scrambler

Digital image scrambling can make an image into a completely different meaningless image during transformation, and it is a preprocessing during hiding information of the digital image, which also known as information disguise. Image scrambling technology depends on data hiding technology which provides non-password security algorithm for information hiding. Data hiding technology led to a revolution in the warfare of network information, because it brought a series of new combat algorithms, and a lot of countries pay a lot of attentions on this area. Network information warfare is an important part of information warfare, and its core idea is to use public network for confidential data transmission. The image after scrambling encryption algorithms is chaotic, so attacker cannot decipher it.

Arnold scrambling algorithm has the feature of simplicity and periodicity, so it is used widely in the digital watermarking technology (Arnold transform is proposed by V. I. Arnold in the research of Ergodic theory, it is also called cat-mapping, and then it is applied

to digital image). According to the periodicity of Arnold scrambling, the original image can be restored after several cycles. Because the periodicity of Arnold scrambling depends on the image size, it has to wait for a long time to restore an image. Generally, the cycle of Arnold transformation is not directly proportional to the image degree.

Arnold scrambling algorithm is base on square digital image in most literature, and these images are mostly $N \times N$ pixels of the digital image. However, most of the digital images are non-square in the real world, so that we cannot use Arnold scrambling algorithm widely

A digital image can be considered as a two unit function f(x,y) in the plane Z. It can be represented as Z = f(x, y) where x, y ∈ [0, 1, 2, 3....N −1] and N represents order of digital image. The image matrix can be changed into a new matrix by the Arnold transform which results in a scrambled version to offer security. It is a mapping function which changes a point (x, y) to another point (x′, y′) by the equation (13).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (13)$$

For example: - An original image as shown in fig. 14 is scrambled after one iteration as in fig. 15 shown below:-

Fig. 14:- Original Image

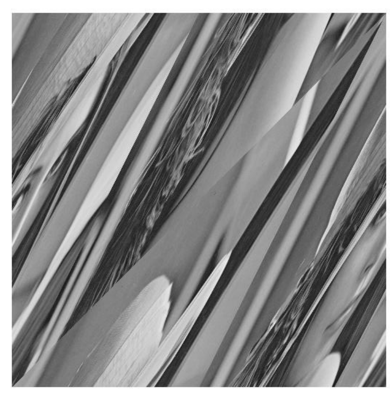


Fig. 15:- Scrambled Image

CHAPTER 2

LITERATURE SURVEY

Base Paper: - Madhuri Rajawat, D S Tomar, "A Secure Watermarking and Tampering detection technique on RGB Image using 2-Level DWT", Fifth International Conference on Communication Systems and Network Technologies, IEEE 2015

Digital watermarking is a method of combining data into a digital signal. In digital watermarking we work on two images one is for watermark image, which is cover on the original image (secondary image) that gives security to the image. It acts as a digital mark, providing the image a good decision of ownership or authenticity. Digital watermarking method is very inspiring for image authentication or security for attacks. This paper presents digital watermarking for their classification, application, techniques, attacks and also tampering detection in digital watermarking. Paper proposed a new algorithm for digital watermarking and tampering detection technique, by combining these techniques, we can improve the security of image. The paper worked on RGB components such as red, green and blue for enhancing security and robustness. 2-DWT applied on RGB components for better results. In the tampering process, researchers used watermarked image as a reference image for detecting tampering. The experimental results gave good PSNR value which is reached up to 55%.

1. **Xiaojun Qi, Xing Xin, and Ran Chang "Image Authentication And Tamper Detection Using Two Complementary Watermarks", Computer Science Department, UT 84322-4205, IEEE 2009.**

This paper presents a novel semi-fragile watermarking scheme for image authentication and tamper detection. The proposed scheme extracts content-based image features from the approximation sub-band in the wavelet domain to generate two complementary watermarks. Specifically, we generate an edge-based watermark sequence to

detect any changes after manipulations. This edge-based watermark encodes the invariant relationship between quantized wavelet coefficients after incidental distortions. We also generate the content-based watermark to localize tampered regions. Both watermarks are embedded into the high frequency wavelet domain to ensure the watermark invisibility. The proposed scheme outperforms the peer scheme and can successfully identify intentional tampering and incidental modification, and localize maliciously tampered regions.

2. **Sandipbhai Mangroliya, Ketki Pathak, " Tamper Localization in Wavelet Domain Using Semi-Fragile Watermarking", Volume 2, Issue 2, ISSN: 2321-9939, IJEDR,2014**

This paper proposes a novel image authentication scheme in the DWT domain. The scheme uses a semi-fragile watermark to detect and precisely locate malicious tampering region in images. The wavelet coefficients selected for embedding are randomly permuted with a secret key, achieving high security. A bit of the watermark is embedded in a group of coefficients by means of quantization. The experimental results show, that algorithm achieves good image quality and high tampering detection resolution at a low watermark payload, compared to block-based authentication schemes. The watermark is protected against local attacks. Paper has also conducted experiments to demonstrate the robustness of the watermark against mild to moderate JPEG compression.

3. **Shinfeng D. Lin, Jia Hong Lin & Chun-Yen Chen, "A ROI-Based Semi-Fragile Watermarking For Image Tamper Detection And Recovery", Volume 7, Number 12, ICIC International, December 2011**

A ROI-based semi-fragile watermarking technique for image tamper detection and recovery is proposed. In the proposed method, the image is divided into ROI and ROB regions first. The authentication watermark is constructed based on ROI content and embedded back to ROI region. Recovery information obtained from ROI and embedded to the ROI region. If the ROI region is tampered, the tampered areas can be recovered from the information embedded in ROB. The unique features of proposed method are it is robust to

both the mild modification, such as JPEG compression and malicious attacks, such as collusion attack and counterfeiting attack.

4. **Jobenjit Singh Chahal, Shivani Khurana, "Digital Image Watermarking using Spread Spectrum Technique under DWT Domain", International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 3, March 2014**

This paper highlights a new scheme for Digital Image Watermarking using Spread Spectrum Technique under DWT Domain. It starts with the general watermarking procedure, the attributes and applications of Digital Image Watermarking and attacks on Digital Image Watermarking. Moreover, the experimental results showed that the proposed scheme provides better quality of watermarked images in terms of watermark invisibility to human eyes and low data payload during embedding and extraction process. In addition, some possible attacks on watermarked images are discussed. To check the Imperceptibility and Robustness, Peak Signal Noise Ratio (PSNR) is being used.

5. **Chen-Kuei Yang and Chang-Sheng Huang, "A Novel Watermarking Technique for Tampering Detection in Digital Images", Electronic Letters on Computer Vision and Image Analysis 3(1):1-12, 2004**

A novel fragile watermarking technique is proposed for hiding logo information into an image by tuning block pixels based on a bitmap parity checking approach. A secure key and a random number generator are used to hide the logo information in a secret, undetectable, and unambiguous way. The characteristics of the mean gray value and the bitmap in a block are exploited for performing the embedding work efficiently and for hiding a logo into an image imperceptibly. The logo can be extracted without referencing the original image. The proposed method is useful for authentication of original digital products. The extracted logo not only can be used to identify tampered locations in digital images but also can resist JPEG compression to a certain degree. Good experimental results have been conducted and resulting images show the feasibility and effectiveness of the proposed method.

6. **Kwang-Fu Li, Tung-Shou Chen, Seng-Cheng Wu, "Image Tamper Detection and Recovery System Based on Discrete Wavelet Transformation", IEEE 2001**

This paper proposes an image tamper detection and recovery system based on the Discrete Wavelet Transformation (DWT) technique. When the system receives an image from a user input, this system will transform the image from its spatial domain to the frequency domain based on the DWT, and extract some information from the frequency domain as the Eigen value of this image. Then, hide this Eigen value in the middle frequency band of the frequency domain

as an evidence for the tamper detection in the future. When we doubt a protected image that may be tampered by other users, we can input this image into the Tamper Recovery System. If this image was tempered by other users, we can use the Eigen value that was hidden in the image to recover this image. This system not only can recover the tampered area but also need no original image to ascertain the image was tampered or not, and need no extra disk space to store extra information to recover the tampered area of the image.

7. **Min-Jen Tsai and Chih-Cheng Chien, "A Wavelet-Based Semi-Fragile Watermarking with Recovery Mechanism", IEEE 2008**

This paper studied the wavelet transformation based watermarking tamper detection and recovery scheme. By the property of discrete wavelet transform, we design the semi-fragile watermark from low-frequency band and embedding the watermark into the high frequency band by the help of Human Visual System (HVS). The watermarked image still preserves high image quality after the embedding of the semi-fragile watermark and the image authentication system is able to locate precisely any malicious alteration made to the image. This novel design can restore the altered or destroyed regions from the attacked images and allow the users to know what the original content was in the manipulated areas. We also analyze the robustness for mild modification like JPEG compression and channel additive white Gaussian noise (AWGN) and fragility to malicious attack. In summary, this

scheme can resist the mild modifications of digital image and be able to detect the malicious modifications precisely.

8. **Hu Yuping & Guo Guangjun, "Watermarking-Based Authentication with Recovery Mechanism", Second International Workshop on Computer Science and Engineering, IEEE 2009**

This paper studied the wavelet transformation based watermarking tamper detection and recovery scheme. By the property of discrete wavelet transform, we design two watermarks from the low-frequency band and embed the watermarks into the high-frequency bands. One watermark is used for detecting the intentional content modification and indicating the modified location, and anther watermark is used for recovering the image. The watermark generation and watermark embedding are disposed in the image itself, and the received image authentication needs no information about the original image or watermark, so it will increase the security of watermark and prevent forged watermark. Experimental results show the algorithm guarantees a good classification for intentional content modification and incidental tampering, localization of content modification area and recovery of image.

9. **Sukalyan Som, Sarbani Palit, Kashinath Dey, Dipabali Sarkar, Jayeeta Sarkar and Kheyali Sarkar, "A DWT-based Digital Watermarking Scheme for Image Tamper Detection, Localization, and Restoration", Springer India 2015**

The provision of image tamper detection, localization and restoration forms an important requirement for modern multimedia and communication systems. A discrete wavelet transform (DWT)-based watermarking scheme for this purpose is proposed in this communication. In our scheme, the original image is first partitioned into blocks of size 2*2 in which a 1D DWT is applied to produce a watermark which is embedded in four disjoint partitions of the image to enhance the chance of restoration of the image from different cropping attack-based tampers. The validity and superiority of the proposed scheme is

verified through extensive simulations using different images of two extensively used image databases.

10. **Tiago José de Carvalho, Christian Riess, Elli Angelopoulou & Hélio Pedrini, "Exposing Digital Image Forgeries by Illumination Color Classification", IEEE Transactions on Information Forensics And Security, VOL. 8, NO. 7, July 2013**

For decades, photographs have been used to document space-time events and they have often served as evidence in courts. Although photographers are able to create composites of analog pictures, this process is very time consuming and requires expert knowledge. Today, however, powerful digital image editing software makes image modifications straightforward. This undermines our trust in photographs and, in particular, questions pictures as evidence for real-world events. This paper analyzes one of the most common forms of photographic manipulation, known as image composition or splicing. Paper proposes a forgery detection method that exploits subtle inconsistencies in the color of the illumination of images. The approach is machine-learning based and requires minimal user interaction. The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. To achieve this, researchers incorporate information from physics- and statistical-based illuminant estimators on image regions of similar material. From these illuminant estimates, we extract texture- and edge-based features which are then provided to a machine-learning approach for automatic decision-making. The classification performance using an SVM meta-fusion classifier is promising. It yields detection rates of 86% on a new benchmark dataset consisting of 200 images, and 83% on 50 images that were collected from the Internet.

11. **Songpon Teerakanok & Uehara Tetsutaro, "Enhancement of Image Tampering Detection Using JPEG's Quantization and Re-Interpolation Processes", IEEE 2015**

This paper proposed a novel technique using 2-dimensional cross product in combining two existing image forgery detection techniques: JPEG quantization noise and interpolation based techniques. By combining two existing methods, efficiency of detection

method and accuracy of locating of the tampered areas within the suspect image are increased. As results, it is shown that, in experiments on real tampered images, proposed algorithm give the better results in detection with lesser amount of noise and higher contrast between tampered region and the rest of the image. Considering the use of automatic image forgery detection system, with our proposed mechanism, the accuracy of the automatic forgery detection system will be increased significantly.

12. Abhishek Kashyap, B. Suresh, Megha Aggrawal, Hariom Gupta, "Detection of Splicing Forgery Using Wavelet Decomposition", ICCCA 2015

Authenticity of an image is an important issue in many social areas such as Journalism, Forensic investigation, Criminal investigation and Security services etc. and digital images can be easily manipulated with the help of sophisticated photo editing software and high-resolution digital cameras. So there is a requirement for the implementation of new powerful and efficient algorithms for forgery detection of tampered images. The splicing is the common forgery in which two images are combining and make a single composite and the duplicated region is retouched by performing operations like edge blurring to get the appearance of the authentic image. This paper proposed a new computationally efficient algorithm for splicing (copy-create) forgery detection of an image using block matching method. The proposed method achieves an accuracy of 87.75% within a small processing time by modeling the threshold.

13. M. K. Bashar, K. Noda, N. Ohnishi & K. Mori, "Exploring Duplicated Regions in Natural Images", IEEE 2010

Duplication of image regions is a common method for manipulating original images, using typical software like Adobe Photoshop, 3DS MAX, etc. This study proposes a duplication detection approach that can adopt two robust features based on discrete wavelet transform (DWT) and kernel principal component analysis (KPCA). Both schemes provide excellent representations of the image data for robust block matching. Multi resolution wavelet coefficients and KPCA-based projected vectors corresponding to image-blocks are arranged into a matrix for lexicographic sorting. Sorted blocks are used for making a list of

similar point-pairs and for computing their offset frequencies. Duplicated regions are then segmented by an automatic technique that refines the list of corresponding point pairs and eliminates the minimum offset-frequency threshold parameter in the usual detection method. A new technique that extends the basic algorithm for detecting 'Flip' and 'Rotation' types of forgeries is also proposed. This method uses global geometric transformation and the labeling technique to indentify the mentioned forgeries. Experiments with a good number of natural images show very promising results, when compared with the conventional PCA-based approach. A quantitative analysis indicate that the wavelet-based feature outperforms PCA-or KPCA-based features in terms of average precision and recall in the noiseless, or uncompressed domain, while KPCA-based feature obtains excellent performance in the additive noise and lossy JPEG compression environments.

14. Fuxing Zhao, Rong Zhang, Haolong Guo, Yanhua Zhang, "Effective Digital Image Copy-Move Location Algorithm Robust to Geometric Transformations", IEEE 2015

To make the tampered image more deceivable, rotation and scaling of the duplicated image region, as simple and common image forgery techniques, are often employed. In this paper, a novel approach of copy-move location is presented for copy-move forgery which combines with the key point-based method and the block-based method. For a tampered image, researchers use the split-half recursion matching strategy to match SIFT key points. In this step, researchers obtain the preliminary detection results which indicate the suspected copy-move regions with matching relation. In order to obtain an accurate localization, the proposed method introduces block-based method. First, the affine transformation between two matched regions is estimated. Then, one of the two matched regions is transformed. And then, the ZNCC coefficients are calculated to measure the correlation between the transformed and the matched regions. Experimental results indicate that the presented algorithm can not only localize the tampered regions accurately, but also deal with operations such as rotation, scaling and multiple copy operations. At the same time it also can resist post-processing operations effectively like white Gaussian noise and JPEG compression.

15. Hareesh Ravi, A.V. Subramanyam, Sabu Emmanuel, "Spatial Domain Quantization Noise Based Image Filtering Detection", IEEE 2015

Smart image editing and processing techniques make it easier to manipulate an image convincingly and also hide any artifacts of tampering. Common real world forgeries can be accompanied by enhancement operations like filtering, compression and/or format conversion to suppress forgery artifacts. Out of these enhancement operations, filtering is very common and has received a lot of attention in forensics research lately. However, different filtering operations and image formats are not investigated deeply and simultaneously. Paper propose an algorithm to detect if a given image has undergone filtering based enhancement irrespective of the format of image or the type of filter applied. In the proposed algorithm, researchers exploit the correlation of spatial domain quantization noise of an image by extracting transition probability features and classify the image as filtered or unfiltered. Experiments are performed to evaluate the robustness and compare the performance of the proposed technique with popular forensic filtering detection algorithms and are found to be superior in most of the cases.

CHAPTER 3
PROBLEM FORMULATION & METHODOLOGY

3.1 SCOPE

Powerful publicly available image processing software packages such as Adobe Photoshop or PaintShop Pro make digital forgeries a reality. Feathered cropping enables replacing or adding features without causing detectable edges. It is also possible to carefully cut out portions of several images and combine them together while leaving barely detectable traces. Techniques such as careful analysis of the noise component of different image segments, comparing histograms of disjoint image blocks, or searching for discontinuities could probably reveal some cases of tampering, but a capable attacker with enough expertise can always avoid such traps and come up with an almost perfect forgery given enough time and resources. This is one of the reasons why digital imagery is not acceptable as evidence in establishing the chain of custody in the court of law. There are other instances, of mostly military character where image integrity is of paramount importance. Digital watermarking can be used as a means for efficient tamper detection. One could mark small blocks of an image with watermarks that depend on a secret ID of that particular digital camera and later check the presence of those watermarks. The “fragility” of the watermark against various image distortions determines our ability to measure the extent of tampering.

3.2 OBJECTIVE

The objective this thesis is to efficiently get better tampering detection technique in a digital image. The algorithm to be used is the 2D-Discrete Wavelet Transform. Discrete Cosine Transform is also taken in to account for better results. DWT is combined with Arnold scrambler to obtain better watermarking. There are several techniques purposed by several authors for noise reduction but all of them are application specific. I will use the most suitable technique according to my topic. Over all I will try to get better tampering detection technique.

3.3 METHODOLOGY

In the proposed scheme, there are three significant steps:

1.) Watermark Generation
2.) Watermark Embedding
3.) Watermark Detection

3.3.1 Watermark Generation

The watermark pattern is obtained from the content information of host image. Watermark generation can be divided into two stages.

1. **Stage 1-** In stage-1 two processes run parallel to each other.

Process 1:- This process has following steps:-

1.) Consider the original image P(x, y) of size M x M.
2.) Perform 1-level DWT on the original image.
3.) By applying DWT on image, four portions each of size M/2 x M/2 is obtained. Let these portions be named as LL, LH, HL, HH; so that LL has highest intensity values and HH has lowest intensity values as shown in fig. 16.

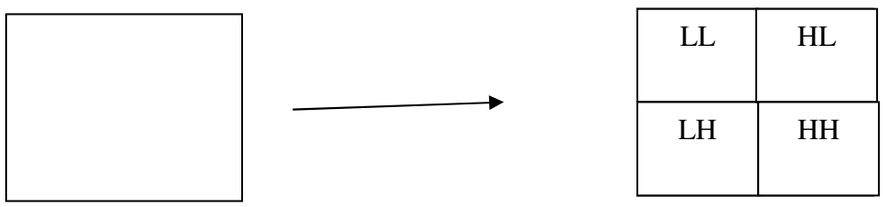


Fig. 16:- Original image of size M x M divided into 4 parts each of size M/2 x M/2 using DWT.

Process 2:- This process has following steps:-

1.) Take the same image P and partition the image into non- overlapping blocks of size 2x2.
2.) One feature value from each block is calculated according to equation (14)

$$B(x,y) = \frac{\sum_{i=1}^{2}\sum_{j=1}^{2} P(x*2+i, y*2+j)}{4} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (14)$$

3.) The matrix B is of size M/2 x M/2

After these two processes completed then the next stage of watermarking generation begins.

2. <u>Stage 2</u>- This stage contains following steps:-

1.) Find the difference between LL and B. Let this difference be C (where C is also of size M/2 x M/2).

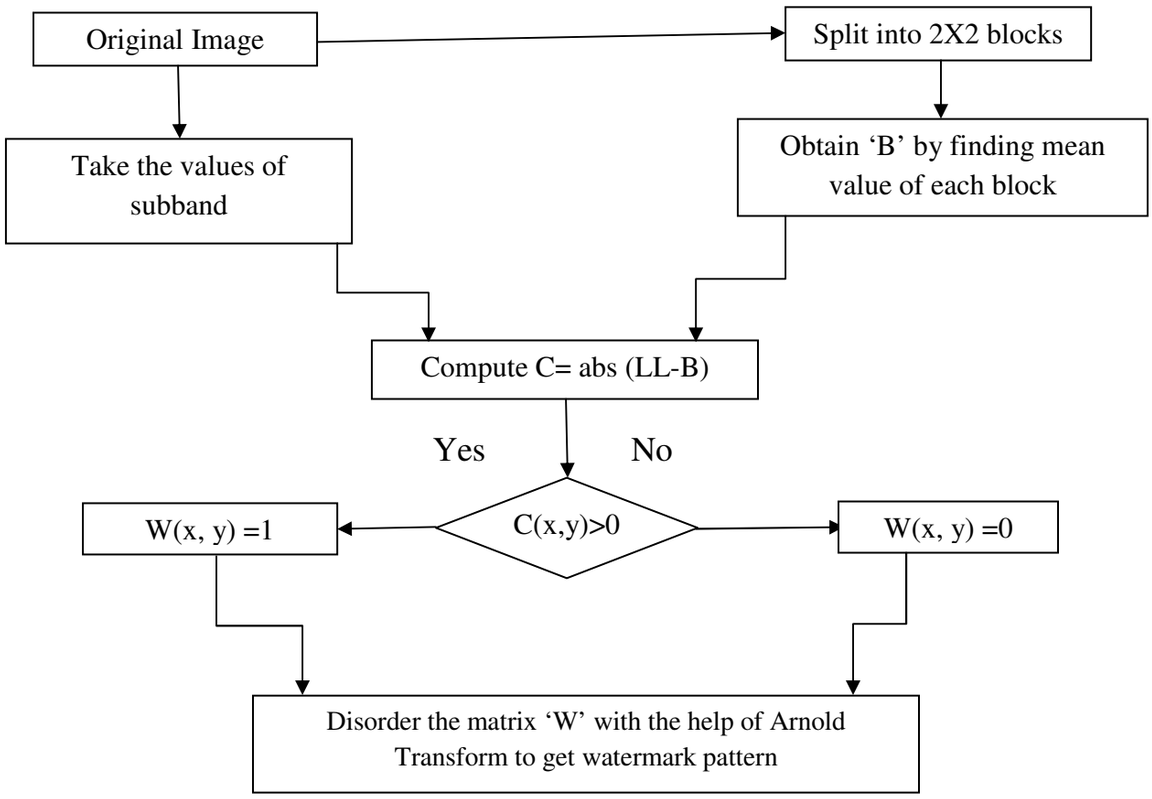
2.) From here, obtain a new matrix of size M/2 x M/2(let it be W) by using following equation.

$$W(x,y) = \begin{cases} 1 & if\ LL > B \\ 0 & otherwise \end{cases} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (15)$$

3.) But sometimes due to calculations W matrix gets all its elements either 0 or 1. In this case, follow this equation.

$$W(x,y) = \begin{cases} 0 & if\ C(x,y) is\ even \\ 1 & otherwise \end{cases} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (16)$$

4.) Disorder the matrix 'W' with the help of Arnold Transform, the resultant is the required watermark pattern to be embedded in to the host image.



Flow Chart:-Watermark Generation

3.3.2 Watermark Embedding

The watermark is embedded in the high frequency subband of DWT as follows:

1.) Replace the HH portion of image by W matrix.
2.) Perform inverse DWT on remaining 3 portions and W matrix.
3.) A new image will be obtained which is required watermark image.

3.3.3 Watermark Detection

Proposed watermarking scheme extracts and generates watermark information from watermarked image and so original image is not required. So it can be considered as blind watermarking. The authentication process includes the following steps:

1.) Watermark is derived from the content of watermarked image using the steps described under watermark generation in section 3.3.1.

2.) Apply 1-level DWT to the watermarked image and extract the HH subband of that image and replace it with original HH subband.

3.) Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.

.

CHAPTER 4

RESULTS AND CONCLUSION

4.1 Results

The proposed thesis, the images are considered with number of rows and columns are of equal size since the embedded watermark is a square matrix. For testing, the size of the original image is taken as 128x128. Figure 17 shows original image. A 64x64 binary watermark signal is constructed from original image and is embedded within itself. The proposed method is tested using MATLAB.

After watermark embedding, there was no visual difference between the original and watermarked images. Figure 18 shows watermarked image. The difference of the pixel intensities of the watermarked image and the original image is shown in Figure 19. The difference image shows that high degree of fidelity is ensured using the technique.

Fig. 17:- Original Image

Fig. 18:- Watermarked Image

Fig. 19:- Difference Image

The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio, which is defined in equation (17). The PSNR value of watermarked image is 59.1168, which indicates that there is very little distortion in the quality of original image.

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right) \dots \dots \dots (17)$$

Where MSE is Mean Squared Error between original and distorted images, which is defined in equation (18).

$$MSE = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[OI(i,j) - DI(i,j)]^2}{M * N} \dots \dots \dots (18)$$

Where OI (i, j) is original image and DI (i, j) represents distorted or watermarked image of order MxN.

Similarity Factor is measure of the similarity of pixel intensities between the original image and the watermarked image. This helps us to calculate the changes in the perceptual quality of the image more precisely. If SM = 1 then the embedded watermark and the extracted watermark are same. Generally value of SM>.75 is accepted as reasonable watermark extraction. Extracted and original watermark can be compared by computing Similarity Ratio (SR) between these two patterns as defined in equation (19).

$$SF = (\sum_{i}\sum_{j} OI(i,j) * DI(i,j))/\sum_{i}\sum_{j} DI(i,j)^2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (19)$$

By using above equation, SM comes out is 0.9034 which is above required limit.

The watermarked image is subjected to six types of distortions: compression, noise, filter, image adjustment, scaling and rotation. Watermarked image has compressed using JPEG compression with different quality factors. Additive Gaussian Noise and Salt& pepper noise has been added to the watermarked image. Also filtering such as median filtering, Linear filtering, histogram equalization and blurring has been applied on the watermarked image. The intensity values of watermarked image are adjusted to new values such that 1% of data are saturated at low and high intensities. Also a clockwise rotation with cropping operation is applied on the image. Results of the metrics Peak Signal to Noise Ratio and Similarity Ratio on the test image cameraman against both methods are shown in Table 4.1 respectively.

Fig. 20:-Watermarked Image after Adding Gaussian Noise from 0 to 0.001

Fig. 21:- Watermarked Image after Adding Salt & Pepper Noise of Factor 0.002

Fig. 22:- Watermarked Image after Rotating 5°

Fig. 23:- Watermarked Image after Rotating 10°

Table 4.1:- Assessment of PSNR & SR under Attacks

Attacks		PSNR(db)		Similarity Ratio	
		Method	Proposed	Method	Proposed
Adding Gaussian Noise(mean, variance)	0,0.01	32.8092	38.3272	1	0.8371
	0,0.001	30.0730	30.0997	0.5188	0.5042
Adding Salt & Pepper Noise	0.002	32.0513	32.1381	0.9898	0.8370
Median Filtering	3×3	29.5819	29.5727	0.5218	0.6629
Linear Filtering	3×3	27,2292	27.7761	0.5359	0.6696
Image Adjustment		18.7003	18.5312	0.8433	0.8435
Blurring		37.8281	37.8322	0.6712	0.8083
Histogram Equalization		19.0192	19.0944	0.7573	0.7598
JPEG(quality factor)	90	43.013	43.1448	0.4659	0.6488
	70	36.4452	37.4799	0.4753	0.6956
	50	35.2058	35.4799	0.4745	0.7418
	30	33.1859	33.2002	0.4759	0.7736
	10	29.1818	29.1867	0.4746	0.8158
Scaling		51.0944	56.1065	0.4985	0.8463
Rotation	5°	13.9478	13.9492	0.5071	0.7135
	10°	12.0324	12.0325	0.4648	0.6957

4.3 Conclusion

This proposed study has discussed a new improved watermarking scheme, which provides a complete algorithm that embeds and extracts the watermark information effectively. In this method, a binary watermark pattern is constructed from host image itself and is disordered with the help of Arnold Transform. The watermark embedding process does not degrade the visual quality of the image. The designed method makes use of the Discrete Wavelet Transform which provides a frequency spread of the watermark within the host image. Moreover the authentication process provides qualities like imperceptibility, robustness and security.

The performance of the watermarking scheme is evaluated with common image processing attacks such as additive noises, filtering, intensity adjustment, histogram equalization, JPEG compression, Scaling and rotation. Experimental results demonstrate that watermark is robust against those attacks. The results obtained show that the proposed technique is highly robust against attacks such as image adjustment, blurring, histogram equalization, compression, scaling and rotation.

REFERENCES

1. Madhuri Rajawat, D S Tomar, “A Secure Watermarking and Tampering detection technique on RGB Image using 2-Level DWT”, Fifth International Conference on Communication Systems and Network Technologies, IEEE 2015.

2. Xiaojun Qi, Xing Xin, and Ran Chang “Image Authentication And Tamper Detection Using Two Complementary Watermarks”, Computer Science Department, UT 84322-4205, IEEE 2009.

3. Sandipbhai Mangroliya, Ketki Pathak, “ Tamper Localization in Wavelet Domain Using Semi-Fragile Watermarking”, Volume 2, Issue 2, ISSN: 2321-9939, IJEDR,2014

4. Shinfeng D. Lin, Jia Hong Lin & Chun-Yen Chen, “A ROI-Based Semi-Fragile Watermarking For Image Tamper Detection And Recovery”, Volume 7, Number 12, ICIC International, December 2011

5. Jobenjit Singh Chahal, Shivani Khurana, “Digital Image Watermarking using Spread Spectrum Technique under DWT Domain”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 3 Issue 3, March 2014

6. Chen-Kuei Yang and Chang-Sheng Huang, “A Novel Watermarking Technique for Tampering Detection in Digital Images”, Electronic Letters on Computer Vision and Image Analysis 3(1):1-12, 2004

7. Kwang-Fu Li, Tung-Shou Chen, Seng-Cheng Wu, “Image Tamper Detection and Recovery System Based on Discrete Wavelet Transformation”, IEEE 2001

8. Min-Jen Tsai and Chih-Cheng Chien, “A Wavelet-Based Semi-Fragile Watermarking with Recovery Mechanism”, IEEE 2008

9. Hu Yuping & Guo Guangjun, “Watermarking-Based Authentication with Recovery Mechanism”, Second International Workshop on Computer Science and Engineering, IEEE 2009

10. Sukalyan Som, Sarbani Palit, Kashinath Dey, Dipabali Sarkar, Jayeeta Sarkar and Kheyali Sarkar, “A DWT-based Digital Watermarking Scheme for Image Tamper Detection, Localization, and Restoration”, Springer India 2015

11. Tiago José de Carvalho, Christian Riess, Elli Angelopoulou & Hélio Pedrini, “Exposing Digital Image Forgeries by Illumination Color Classification”, IEEE Transactions On Information Forensics And Security, VOL. 8, NO. 7, July 2013

12. Songpon Teerakanok & Uehara Tetsutaro, “Enhancment of Image Tampering Detection Using JPEG’s Quantization and Re-Interpolation Processes”, IEEE 2015

13. Abhishek Kashyap, B. Suresh, Megha Agrawal, Hariom Gupta, “Detection of Splicing Forgery Using Wavelet Decomposition”, ICCCA 2015

14. M. K. Bashar, K. Noda, N. Ohnishi & K. Mori, “Exploring Duplicated Regions in Natural Images”, IEEE 2010

15. Fuxing Zhao, Rong Zhang, Haolong Guo, Yanhua Zhang, “Effective Digital Image Copy-Move Location Algorithm Robust to Geometric Transformations”, IEEE 2015

16. Hareesh Ravi, A.V. Subramanyam, Sabu Emmanuel, “Spatial Domain Quantization Noise Based Image Filtering Detection”, IEEE 2015

17. http://eeweb.poly.edu/iselesni/WaveletSoftware/standard2D.html

Plagiarism Report

without_content3.pdf

ORIGINALITY REPORT

%0	%0	%0	%0
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	< 70 WORDS
EXCLUDE BIBLIOGRAPHY	ON		