Digital Watermarking of Image Using 3-Level Discrete Wavelet Transform (DWT), SVD & Median Filter

Submitted in partial fulfillment of the requirements for the

Degree of

Master of Technology (Signal Processing & Digital Design)

By

Lt Col Shiv Kamal Sinha

Under the Guidance of

Professor Rajiv Kapoor

Department of Electronics & Communication
Delhi Technological University
(Formerly Delhi College of Engineering)

Approval Sheet

Thesis Entitled : Digital Watermarking of Image Using 3-Level Discrete
Wavelet Transform (DWT), SVD & Median Filter

Submitted By : Lt Col Shiv Kamal Sinha
is approved for the award of the degree of **Master of Technology**
(Signal Processing and Digital Design)

Date:

Chairman:

Place:

Declaration

This is to certify that the dissertation report comprises of original work (except where indicated) carried out by me and due acknowledgments have been made in the text to all other material used. The dissertation does not contain any classified information that is detrimental to national security. The information contained therein has not been submitted in any form for award of another degree or diploma at any other institute/university.

(Lt Col SK Sinha)
Dept of Electronics & Communication
Delhi Technological University
Apr 2015

Countersigned By

Professor Rajiv Kapoor
Dept of Electronics & Communication
Delhi Technological University
Apr 2015

Acknowledgment

Preparing a project of this nature is an arduous task and I am fortunate enough to get support from a large number of people to whom we shall always remain grateful.

I would like to express my eternal appreciation to **Professor Rajiv Kapoor** for his support and guidance throughout the completion of this project.

Last but not the least, I am indeed grateful to my parents as also the entire faculty members for their kind co-operation and continued encouragement.

ABSTRACT

Consequent to the tremendous advancement in the field of Information technology and readily availability of tools, it has become increasingly easy for the unknown users to yield unauthorized copies of multimedia data that are easily accessible on the Internet. To genuinely shield those multimedia data on the internet, innumerable techniques including various encryption techniques, stenography techniques, watermarking techniques and information hiding techniques are available. Digital watermarking is a method in which a portion of digital information is embedded into an image and extracted at later stage for the purpose of ownership verification. Such of the watermarks that are very high on the parameters of integrity and robustness are particularly suitable for copyright protection. It is so because they remain inherent with the image under various stages of manipulations and interferences.

Digital data, it must be clearly noted, can be embedded both in spatial and frequency domain. In this paper, a new Singular Value Decomposition (SVD) and Discrete Wavelet Transformation (DWT) based technique is proposed for hiding watermark in full frequency band of images. Median filter is used to further accentuate the result. The quality of the watermarked image and extracted watermark is measured using Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) respectively. It is observed that the quality of the watermarked image is distinctly maintained with the PSNR value of 36dB.Robustness of proposed algorithm is tested for various attacks including salt and pepper noise and Gaussian noise, cropping and JPEG compression, amongst others.

Decomposition (SVD) based watermarking algorithms it must be noted, have always fascinated scientists and academia due to its inherent simplicity and some other striking mathematical properties. The subservience of this method has been analyzed and implicitly studied by ascertaining the robustness of this algorithm against administering of various geometric attacks to include rotation, scaling, translation (RST). Experimental results so obtained have been matched and deliberated with existing algorithm that visibly throws encouraging results and inferences.

CONTENTS

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

LIST OF FIGURES

LIST OF TABLES

Chapter 1

1.1 Introduction

Watermarking of images has recently acquired tremendous curiosity in a range of applications like, identification of image, copyright control, verification of image and data hiding, amongst others. Duplication and distribution of multimedia data have been rendered easy and virtually costless due to tremendous advances in networking and high speed processors. It also makes copyright protection of digital media stern challenge. Digital watermarking is a process, which embeds a watermark signal in the host signal to be protected. Watermarking is classified on the basis on two working domains: **Spatial Domain** in which pixels of one or two randomly selected subsets of an image are modified based on perceptual analysis of the original image and **Frequency Domain** in which values of certain frequencies change.

1.2 Scope

Scope of dissertation is to study in detail efficient method for robust watermarking by use of Discrete Wavelet Transform and Median filter.

1.3 Literature survey

Watermarking techniques are broadly classified based on two working domains. One is the Spatial Domain where the pixels of one or two randomly selected subsets of an image are modified on the basis of perceptual analysis of the original image and the other is the Frequency Domain in which values pertaining to certain frequencies undergo change.

1.3.1 Spatial watermarking

This type of watermark can also be applied using colour partition such that the watermark appears in only one of the colour bands. However, the watermark appears when the colour are separated for printing. Spatial domain process essentially entails addition of fixed amplitude pseudo-noise into the image. The least significant bits of original contents are modified in this process. The watermark can be concealed into the data to assume that the Least Significant Bit data are visually irrelevant.

1.3.2 Transformation based watermarking

Many techniques are suggested based on transformation based watermarking. Watermarking can be applied in the transform domain; such as Discrete Fourier Transform, Wavelet Transforms and Discrete Cosine Transform. In this initially the host or main data is transformed and then modifications are applied to transformed coefficients.

Watermark is embedded in DFT, DCT and DWT domain coefficients

A Wavelet-based Watermarking algorithm used for the purpose of Ownership Verification of Digital Image first adds the watermark into the middle-frequency range. For the watermark, embedding filter banks can be saved. The middle-frequency band to insert the watermark is selected such that he coefficient in that band of the image is substituted by the watermark.

The advantages of this approach are multifold:

It achieves advantages of both spatial and frequency localization.

It is both perceptual invisibility and robustness to compression.

It is robustness to noise, image processing techniques, median filter, geometric transform.

1.3.3 Hybrid Watermarking

In this methodology, the embedding is resorted to into both spatial and frequency domain. A hybrid image authentication watermark can be attained by amalgamation of fragile and a robust watermark. Good localization and security properties are the apparent benefits that accrue from fragile watermark. To precisely identify changes as well as differentiate malicious tamper from simple operations, hybrid watermarks are used.

1.3.4 DCT & DWT Domain Watermarking

The DCT Domain watermarking is known to be more robust in comparison to spatial domain Watermarking. This algorithm is greatly robust against modest image processing operations like low pass filtering, contrast and brightness correction, amongst others.

The DCT undertakes the task of transforming a signal to a frequency representation from a spatial representation. Lower frequencies are more obvious in an image than higher frequency. Hence if we transform an image into its frequency component and remove higher frequency coefficients, we can largely lessen the volume of data required to define the image without foregoing much degree of image quality.

DCT Domain Watermarking is more problematic to implement and are computationally more expensive. They are also known to be frail during geometric attacks to include scaling, rotation and cropping.

Study on secure digital watermarking methods has shown that the content of the images are used to increase the invisibility and robustness of a watermarking scheme. In DWT approach the watermark is fashioned from the content of the host image and discrete wavelet transform (DWT) is applied for embedding watermarks. DWT is an first-rate time-frequency analysis method which can be adapted well for pulling out the information content of the image.
A discrete-wavelet transform based multiple watermarking algorithms is proposed by Tao et al. Two significant tools, namely, encryption and watermarking can be utilized to the wart unlicensed consumption and duplication. Watermark is embedded into LL and HH sub bands to essentially increase the robustness. Embedding the watermark in lower frequencies is robust to variety of attacks such as JPEG compression, blurring, adding Gaussian noise, rescaling, rotation,

cropping, and pixilation & sharpening. Embedding the watermark in higher frequencies, on the other hand, is robust to another set of attacks such as histogram equalization, intensity adjustment and gamma correction.

Integer wavelet based multiple logo watermarking scheme was presented by Yuan et al. Using Arnold transform the watermark is permutated and embedded by modifying the coefficients of the HH and LL sub bands. An integer wavelet based manifold logo-watermarking arrangements for copyright security of digital image is presented. A visual meaningful binary logo is used as watermark. The process of watermark embedding is carried out by altering the host image in the integer wavelet domain. Wavelet coefficients of HH and LL bands are adjusted depending on the watermark bits to effectively construct a blind watermarking arrangement. To enhance security, permutation is resorted to preprocess the watermark.

Chen et al., yet another distinguished scientist, offered two DWT-based audio watermarking algorithms .One such algorithm projected was based on optimization scheme by making use of group-amplitude quantization. Second algorithm inserts data by energy-proportion scheme. The normalized energy is, therefore, essentially utilized as against probability which basically redrafts the entropy in information theory as an energy proportion function.

1.3.5 Fragile Watermarking

A fragile watermark, as the name suggests, can be damaged easily. This obvious characteristic is beneficial to implicitly identify & ascertain if a multimedia has changed. The genuineness of multimedia can be ascertained by readily modulating fragile watermark into multimedia. Any amount of alteration on the multimedia will greatly abolish the resultant embedded fragile watermark.

1.3.6 Quantization-based Fragile Watermark

The precise position where malicious modification has taken place could be recognized by using this technique by examining the destroyed fragile watermark. The method recognizes the nature of distortion as JPEG compression, if the resultant ratio of the number of destroyed watermark over the number of all watermark decrease from high resolution to low resolution in wavelet transform. This approach, however, cannot identify the type of modification if both an instance of malicious tampering and an incidental distortion are applied at the same time. The specified quantization step administers the fragility or sensitivity to manipulations and the extent to which the distortion has actually taken place.

A unique watermark may be extracted from various different media in this method. This may be subjected to some forms of content-preserving operations or unauthorized manipulations. This one-to-many correspondence can be challenging in both terms false positives (i.e. a watermark, that was never embedded, is detected by the detector) and false negatives (i.e. the detector fails to detect an embedded watermark).

For maintaining low false positive and false negative rates no criteria is currently known. The tremendous challenge that semi-fragile schemes encounters is in its ability to distinguish content-preserving operations from attacks that are malicious by nature. A case in the point can be understood wherein, transposing may be deemed acceptable for one application while it may be seen as malicious for another. Semi-fragile watermarking is ordinarily not apt for applications involving vital issues like legal and state security.

1.3.7 Research Findings

The concept of correlation is applied to present approach in case of image watermarking algorithms as regards changes in watermarking forestalling properties like imperceptibility and robustness. For reasons of security, the binary watermark image is scrambled which is redesigned to a sequence and then a random binary arrangement is adopted to encrypt the watermark. A pseudo-random number generator is used to determine the pixel to be used on a specified key. The host image's RGB channel are converted to the desired channel and then the first channel amongst them is pre filtered amongst them to enhance the process of embedding.Low frequency sub-band of wavelet decomposition of its first channel is quantized and divided into diverse sub-blocks with the certain sub-block size to embed the encrypted watermark.

1.4 Types and Applications

The first amongst basically two types of watermark is the blind watermark which, as the name suggests, is invisible, and is extracted “blindly” without knowledge of the original host image or the watermark itself. The second watermark type of watermark is non-blind (also asymmetric marking or private), in which the watermark is embedded in the original host, and is intentionally visible to the human observer. An example is shown in figure below. There is a mandatory requirement of original data for watermark extraction. The subject of this dissertation is a blind watermark. The necessary requirements for the purpose of extracting the watermark are one the watermarked image and second the key used to embed the watermark in the image. It must be noted and understood that some watermarking mechanisms essentially require the original image, which largely restricts their usefulness. The watermarked image may have been subjects to modifications, such as those shown in section 2.1.

Figure 1.1.Example of non-blind digital Watermarking

1.5 Advantage of DWT over DCT

Watermark embedding is essentially that of the wavelet domain. The Discrete Wavelet Transform (DWT) implicitly separates a host image into lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can thereafter be repeated for multiple "scale" wavelet decomposition. The advantages of DWT over DCT are tersely below:

(a) Wavelet transformed image is a multi-resolution description of image under consideration. Hence an image is shown at different levels of resolution and can be continually processed from low resolution value to high resolution value.

(b) Visual artifacts introduced by wavelet-transformed images are relatively less marked compared to DCT because wavelet transform doesn't decompose the image into blocks for processing. Blocking artifacts are noticeable at high compression ratios in DCT; but in wavelet-coded images, its clarity is more pronounced.

(c) DFT and DCT are essentially full frame transform, and hence any change in the transform coefficients effects the entire image except when DCT is implemented using a block based approach. DWT, however, has spatial locality property that implies that if signal or any watermark is embedded it will significantly affect the image locally**.**

Hence a wavelet transform provides both frequency and spatial information for an image.

1.6 Applications

(a) **Authentication of Image and its Contents:** The intention in image authentication is essentially to ascertain with high degree of reliability modification to the data, if any. Should either any portion of the content is modified, in part or in full, its summary and signature will undergo change thus indicating that some tampering has been effected.

(b) **Fingerprinting:** Information about the owner permissions is contained in the watermarked image. Many fingerprints can be properly held in the same image the object could belong to large number of users.

(c) **Publication Monitoring and Copy Control:** Contents of the watermark is not only the owner data but also the details about the number of copies that are permissible, which enables hardware and software to update the watermark at every stage and use. it also obviates unauthorized distribution as the owner data is inherent in the watermark.

(d) **Protection of copyright:** The basic concept of copyright protection is to prevent other parties for wrongfully claiming its ownership by embedding certain information that enables the identification of authorized copyright owner.

(e) **Broadcasting Checking:** For primarily ascertaining the content that is intended to be transmitted this monitoring is resorted to. For instance, monitoring of commercial advertisements could be successfully undertaken through their watermarks to confirm its timing and count.

(f) **Covert Communication:** The signal embedded in this form is utilized for the purpose of transmission of such messages, which have high degree of security classification and are by nature secret. The point to note here is that all precautions need to be incorporated to ensure that no suspicion or doubt arises that suggests, even remotely, that a secret message is being transmitted.

(g) **Identification of owner:** Visual mark is the traditional form of intellectual ownership. This can be overcome by use of suitable and appropriate software that are now available to modify the images under consideration.

1.7 Attacks on watermarking

Loss of information on account of transmission of signals through its media is a matter of concern. Such losses, which may constitute attack on the information and signal intended to be communicated, may the either intentional or otherwise. Intentional attack use various available resources to destroy or modify the watermark, its extraction becomes extremely difficult. Some known methods to attempt extraction of watermark from such attacks are cryptanalysis, stag analysis and other signal processing techniques. Accidental attacks, in contrast are inevitable as distortions may inadvertently get introduced on account of transmission noise.

(a) **Removal and interference attack:** Removal attack is primarily aimed to implicitly remove from the watermark object, the watermark data. Watermark, it must be understood, is an additive noise inherently present in the host signal. Some examples of removal attack include remodulation, denoising, averaging, loss compression, quantization collusion and noise storm.

(b) **Geometric Attacks:** These attacks, which do not eradicate watermark but suitably manipulated in a manner to make it impossible for the detector to discern the data, are related to images and videos. Geometric attacks include rotation, scaling and translation, all of which are forms of affine transforms. Also included in this category of attack are line/column removal, cropping and warping. Mosaic attack is yet another form of geometric attack wherein watermark image is subdivided into various components and the rearranged using appropriate HTML code.

(c) **Cryptographic Attacks:** Removal and geometric attack, tersely discussed above, do not breach the security of watermarking algorithm. It is the cryptographic attack which is associated with acts of breaking of security. Oracle attack is an apt example of such attack. In this a non-watermarked object **is** created on the condition of availability of watermark detector.

(d) **Protocol Attacks:** This attack, unlike those discussed above, work on the loopholes of the watermarking concept. This attack embeds several watermarks thus making it difficult to discern the original watermark of the owner.

(e) **Simple Attacks:** Without, in any case, attempting to mark the watermarked location, simple attack modifies the data of the cover image. Attacks such as cropping, noise addition and wavelet-based compression are some examples of this kind of attack.

(f) **Disabling Attacks:** With the aim to prevent extraction, correlation between cover image and watermark is broken in this kind of attack. Example includes rotation, cropping, geometric distortion, insertion of pixels, amongst others.

(g) **Ambiguity Attacks:** These attacks blur the image by embedding a false watermark and it is impossible to determine the original embedded mark in the host image.

Features of Watermark

1.8.1 Robustness

If the digital watermark is not discernable against small modifications, it is referred to as “fragile”. These watermarks are mostly used for the purpose of tampering detection. Noticeable modifications are not referred to as watermark if any kind of changes to an original work occurs, but as generalized barcodes.

It is referred as semi-fragile if it repels benevolent transformations, but invariably fails detection after malicious transformations. To successfully detect malignant transformations semi-fragile watermarks are made use of. When it resists a selected class of transformations, a digital watermark is called robust which may be used in copy protection applications.

1.8.2 Perceptibility

If the original cover signal and the marked signal are perceptually indistinguishable it is referred to as imperceptible. It is perceptible when its occurrence in the discernible signal is noticeable. Content Bug Network Logo, Codes, and Opaque images are a few examples of these.

This should not be confused with perceptual, that is watermarking which uses the limitations of human perception to be imperceptible.

1.8.3 Capacity

Capacity is the quantum or degree of watermark information in an image. When multiple watermarks are embedded in the same image, then the capacity of image is sum of all individual watermarks data payload.

1.8.4 Security

Ability to resist the malicious and malignant attack on the part of the watermark is referred to as security.

1.8.5 Computational cost

It is degree of the sum total of computing resources essential to undertake watermark embedding as well as detection process. For a given computer configuration it can be accurately ascertained using processing time.

1.9 Recovery with or without the original data:

In majority of watermarking applications, the requirement of the original host image to extract the watermark is not mandatory. However, there is no denying that should the said image is accessible and it surely will greatly enhance the robustness and imperceptibility of the watermark. There is no requirement of original image data in the watermarking algorithm to extract the watermark.

1.10 Extraction or verification of a given watermark:

If it not be successfully extracted, the watermark despite its robustness and imperceptibility is useless. The PSNR will be calculation of PSNR is then carried out for the watermark and the extracted watermark.

1.11 Aim

The aims of this research are as under:

(a) To study and determine the strength and precincts of prevalent watermarking schemes

(b) To tersely design and develop schemes to surmount the existing limitations

(c) To appraise the new schemes by using application scenarios of copyright protection, authentication & tamper detection

1.12 Research scope

Here in this thesis we study robust, semi-fragile watermarking and hybrid methods. Examination of hybrid methods that is known to draw the advantages of both the robust and semi-fragile watermarks is also undertaken. With the intent to preserve the appearance of images, we pay particular attention to invisible watermarks. To focus on the fundamentals of data embedding the experiments are performed using grayscale images.

This thesis will, therefore, focus on watermark robustness, and place less emphasis on watermark security. Watermark security has become a new branch of watermarking research. We also need to consider trade-off between watermark properties that have conflicting characteristics i.e. robustness, capacity, and imperceptibility. We also emphasized the computational efficiency of the algorithms, in reasonable detail.

Chapter 2

2.1 Digital watermarking

Digital watermarking is the process that embeds data called a watermark into a multimedia object in such a way that the watermark can be later on detected or extracted for object assertion purposes. The multimedia objects, in which the watermark is embedded, are usually called the original, cover signal, host signal or simply the work.

A digital watermark is a distinguishing piece of information that is assigned to the data to be protected. One important requirement by this is that the watermark cannot be easily extracted or removed from the watermarked object.

Watermarks and watermarking techniques can be classified into several categories taking into account by this various criteria. As it can be noted, one of the criteria is embedding domain in which the watermarking is implemented. For example, watermarking can be done in the spatial domain. An alternative possibility is the watermarking in the frequency domain.

2.2 Watermark requirements for still images

In the open literature various watermarking techniques have been proposed in the past. In order to be effective, a watermark should have the main features, as outlined below:

2.2.1 Fidelity:

It the embedding algorithm must embed the watermark in such a way that this does not affect the quality of the host image. If the humans cannot distinguish the original data from the data with the inserted watermark, the watermark-embedding procedure is considered truly imperceptible. Even the smallest modification in the host image may become apparent when the original data is compared with watermarked data. Usually the users of the watermarked data do not have access to the original data. Thus, the aforementioned comparison cannot be performed. It may be sufficient that the modifications in the watermarked data stay unnoticed, as long as the data are not compared with the original image.

2.2.2 Payload encoding

Before starting, the watermark embedding procedure a message intended to be used as a watermark can be encoded into a robust form. Using the error correction coding, modulation or both can accomplish the encoding. The error correction coding is a conversion of the original bit sequence into a longer sequence where the additional bits can be used for error detection and correction. The modulation is the process of converting each bit into a waveform, which is sent across the channel. Here the following encoding techniques will be presented.

Spread Spectrum Since watermarking systems can be modeled as communication systems, where the watermark represents a message and the image represents communications channel, a spread spectrum technique can be applied in the watermarking. Spread spectrum technique is based on spreading the message energy over a bandwidth much larger than the min bandwidth required.

2.2.3 Robustness:

Low power spectral density relates to the fact that the transmitted energy is spread over a wide band, and consequently the amount of energy for any specific frequency band is low. The effect is that such a signal will not interfere with other signals sharing the same frequency band. Assuming that a watermark represents a message, the low power density means that the watermark will introduce negligible changes to the image and therefore the embedded watermark should be imperceptible. Redundancy relates to the fact that the message is present at different frequency bands, so that if there is an error in one band, the message could still be recovered from other bands. Redundancy maps to robustness, and means that a watermark will be recoverable even if it suffered certain level of intentional or unintentional distortion/attack.

One example of a watermarking system based on the Direct-Sequence Spread Spectrum (DSSS) communications techniques is proposed in [50]. A watermark, representing an individual message bit} 1, 1{−∈jb, is created in two steps. Firstly, the bit is spread by a large spreading factor cr, in an analogy to spread spectrum communications equivalent called the chip-rate. The purpose of spreading is to distribute one bit of information across many pixels of an image. The spread bit is then modulated with a pseudo-noise sequence, yielding one watermark. This procedure is repeated for each information bit of a message, and the created watermarks are added together yielding a final watermark which represents the whole watermarked message.

The recovery of the multi-bit message is accomplished by correlating the watermarked image with the same pseudo-noise sequence being used on the message encoding side. If the peak of the correlation is positive, the current information bit is 1+. Contrary, if the peak of the correlation is negative, the current information bit is 1−. After decoding of one bit, the next crpixels are processed in the same way to recover the next bit. This scheme works only if both the message encoder and the message decoder use the same key (the same pseudo-noise sequence).

Low power spectral density relates to the fact that the transmitted energy is spread over a wide band, and consequently the amount of energy for any specific frequency band is low. The effect is that such a signal will not interfere with other signals sharing the same frequency band. Assuming that a watermark represents a message, the low power density means that the watermark will introduce negligible changes to the image and therefore the embedded watermark should be imperceptible.

2.2.4 Unambiguousness

Identification of the owner should be unambiguously through recovery of watermark.

2.2.5 Content recovery

Content recovery entails reversing the changes in the image in order to recover the original content. It is a new challenge in watermarking. A perfect content recovery cannot be made in theory became of introduction of distortion and occupation of a subspace of an image by watermark. However to a certain degree of approximation recovery can be realized. One way of recovery is that watermark itself contains a condensed set of image information. This information can be detected and used for recovery or reconstruction and self-recovery.

The image can be condensed by downscaling original one with only retaining certain significant features which could edges, luminance, texture etc of the image Adequate caution should be exercised while selecting the image features for watermarking because this is detrimental on not only watermark capacity but the content recoverability too. For example if we choose features such robust hashes, visual hashes and digital signatures it will not be suitable for our aim of content recovery as it contains too little information. Another thing to take care is that watermark should not be embedded in same region otherwise it may get lost in cropping and content may be rendered irrecoverable. Although fragile watermarks may offer a little recoverability ideally a watermark should be robust to endure maximum tempering so that the initial message encoded in the watermark can be utilized for recovery.

Chapter 3

3.1 Robust Watermarking Flow

Typical Component of watermarking system

Watermarking system comprises at least two of the different units given below:

(a) Host image’s Wavelet Transform

(b) The watermark embedding unit

(c) Host image’s Inverse Wavelet Transform

(d) Unit for watermark detection/extraction.

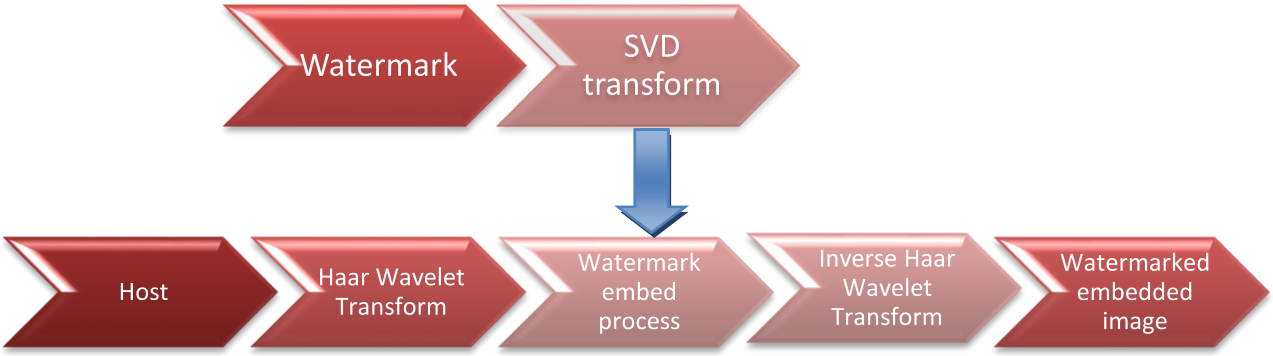


Figure 3.1 Watermark embedding process

Figure 3.2 Watermark extraction in host image

3.2.1 Wavelet: The Concept

A wave usually with energy transformation propagates through space and time in form of periodic oscillating disturbance. On the contrary, wavelets are made of localized waved which are used to analysis of transient signals due to having energy concentrated in time or space. In 1-D, it is a localized change of a sound signal and in 2-D image, detailed change with localized variations occurs. It can be used for a wide variety of signal processing tasks including compression, detecting edges, removing noise, and enhancing images or sound.

There are mathematical functions available which break up continuous time signal data into different frequency components. If there is a rapid change in the parts of the signal then they are of high frequency and if there is a slowly smoothly changing then they are of low frequency. A portion which does not change contains zero, or no frequency.

Easiest ways to predict scale is to use the analogy of the piano. The eight notes in an octave occur continually. In the translation of notes, each of the octaves move from left of the keyboarder to the right of the ivories. Each of them represents the concept of a tone, C with the low C, a high C and a middle C. There is also a relationship between musical compositions that shows set of notes. Every component played in a certain order at a certain speed with the combination of one another. A chord is combination of individual notes. The branch of knowledge can even be further refined if one only wishes to view information about the Discrete Wavelet Transform.

Wavelet transform is like to the Fourier transform. Like the Fourier transform, for representing the input data, wavelet transforms satisfy particular mathematical criteria. However, while the Fourier transform uses sinusoids to analyze signals, the wavelet transform uses wavelets of finite energy.
For single wavelet, there is a function (ψ) called the mother wavelet describe by

$$\psi_{j,k}(x) = \sqrt{2^j}\,\psi(2^j x - k), \qquad j,k = 0, \pm 1, \dots .$$

The mother wavelet is the prototype that generates the functions, used in the wavelet transformation process. Mother Wavelet has children, grandchildren, great grandchildren. Only constrained by mother wavelet is the size of the original signal. If the signal has 2n samples, she can give birth to n generations.

For any mother ψ(x) there is a function φ(x) called the scaling function. It is also known as father wavelet. Its dilations and translations are denoted by φj, k. As the interval of the signal examined is shifted, then the translation is the location of the interval. The scale is the dilation or the contraction. For example, Haar mother wavelet ψ and scaling wavelet φ are shown below:

The 1-D wavelet transform is described by:

$$W_f(x,y) = \int f(t)\psi(xt + y)dt$$

3.2.2 History of Wavelet

The concept of wavelets generated independently from the variety of fields including electrical engineering, mathematics, quantum physics and seismic geology. In 1910, Wavelets have been traced all the way back to Alfred Haar. In the late 1980s, two publications by Ingrid Daubechies were the starting point of their modern history.

For explaining and defining the subject, innovators developed a solid mathematical foundation. The first orthogonal wavelet bases, constructed by Ingrid Daubechies were compactly supported.

3.2.3 Utility of Wavelet

There are many reasons are known to use wavelets. The reasons can vary according the application. For example, some wavelet transforms perform in a way which divides a signal into those components which are noteworthy in time and space, and those that contribute less. This feature enables wavelets to be very useful in applications such as noise removal, edge detection and data compression. In general, wavelets are useful when used to obtain further information from that signal that is not readily available in the raw signal. The transform of a signal is just another way of representing the signal. It does not change the information content present in the signal.

3.3 Haar wavelet

Wavelet is rescaled square shaped functions together forming a basis of family. Wavelet analysis is action to Fourier analysis considering that it allows the orthonormal function representation of the target function over an interval.

Haar sequence, proposed in 1909, used these functions as an example of orthonormal system for the space of square integrals functions on the unit interval [0, 1]. The study of wavelet came much later and as a special case of Daubechies wavelet, the Haar wavelet is also known D2.

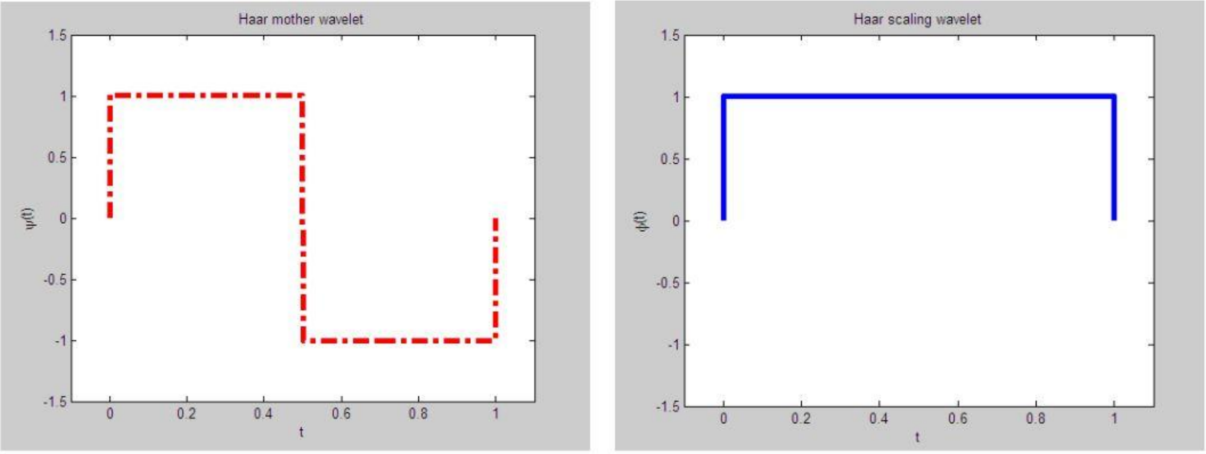
The disadvantage of the Haar wavelet lies in the fact that it is not continuous and hence not differentiable. This can however, be an advantage in analysis of signals with sudden transitions like the monitoring of tool failure in machines.

The Haar wavelet's mother wavelet function $\psi(t)$can be described as:

$$\psi(t) = \begin{cases} 1 & 0 \le t < 1/2, \\ -1 & 1/2 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Its scaling function$\phi(t)$can be described as

$$\phi(t) = \begin{cases} 1 & 0 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$



(a) The Haar mother wavelet ($\psi(t)$)　　(b) The Haar scaling wavelet ($\phi(t)$)

Figure 3.3 Haar basis

The Haar transform decomposes a discrete signal into 2 sub signals each sub signal is half of s's original length. The first half is the approximation (or average) of the original signals and the second half indicates the detail (or change), d, from the spectrum s. The frequency spectrum of a signal is basically the frequency components (spectral components) of that signal.

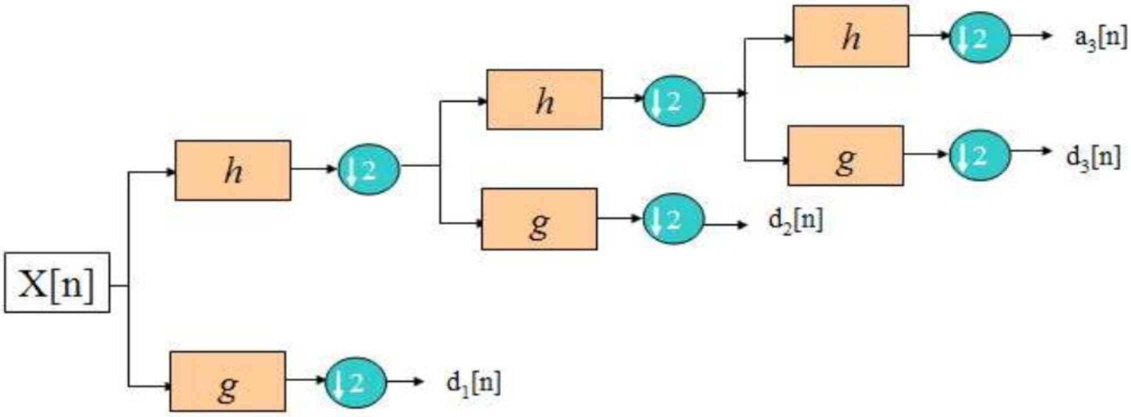


Figure 3.4 1-D DWT Analysis or Decomposition Tree

Figure 3.5 1-D DWT Analysis or Decomposition tree

Input signal is = {4, −2, 3, 7}.

We take scalar product of the input vector in the each of the basis vector to project this with the wavelets.

$$\{4,-2,3,7\}\cdot\{\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2},\tfrac{1}{2}\}=6$$

$$\{4,-2,3,7\}\cdot\{\tfrac{1}{2},\tfrac{1}{2},\tfrac{-1}{2},\tfrac{-1}{2}\}=-4$$

$$\{4,-2,3,7\}\cdot\{\tfrac{1}{\sqrt{2}},\tfrac{-1}{\sqrt{2}},0,0\}=\tfrac{6}{\sqrt{2}}$$

$$\{4,-2,3,7\}\cdot\{0,0,\tfrac{1}{\sqrt{2}},\tfrac{-1}{\sqrt{2}}\}=\tfrac{-4}{\sqrt{2}}$$

3.3.2 Reconstruction

1. Signals can be decomposed or analyzed by DWT. However since there is no loss of any piece of info or components the same can be used to assemble original signal while suffering no loss in the process. The finite impulse filters have their coefficients set to match the perfect reconstruction criteria, thus they do not need any scaling and efficiently negate aliasing to confirm to the criteria of embedding a watermark is essential vis-avis the accurate reconstruction capability of original image, save the regions where the watermark is embedded. Thus if transform is undone the signal can be reconstructed.

2. There is a lot of similarity between approximation and original Addition of higher frequency we reach the starting point. This mathematical operation is termed as inverse discrete wavelet transforms (IDWT). Please refer figure illustrated for a single octave only.

Thus the input vector got transformed into {6, −4, 6/√2, −4/√2}.

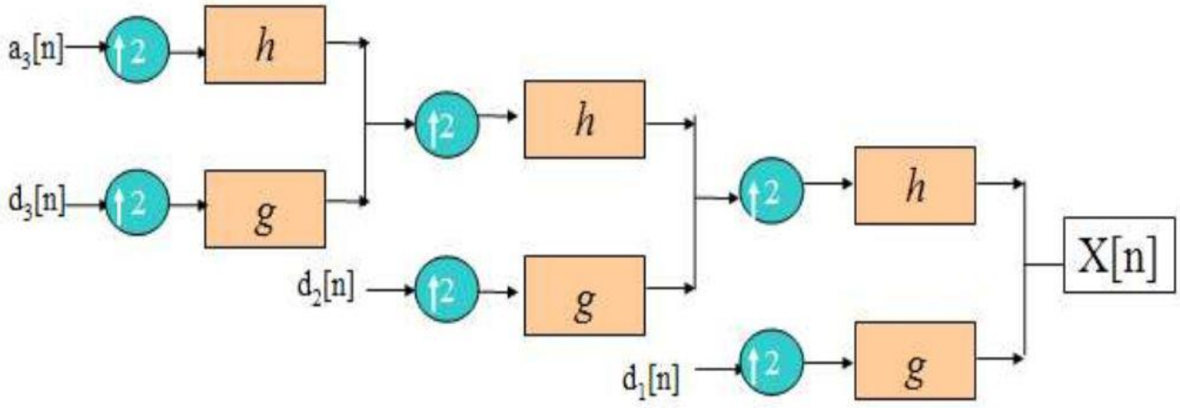


Figure 3.5 2-D IDWT Synthesis or Reconstruction Tree

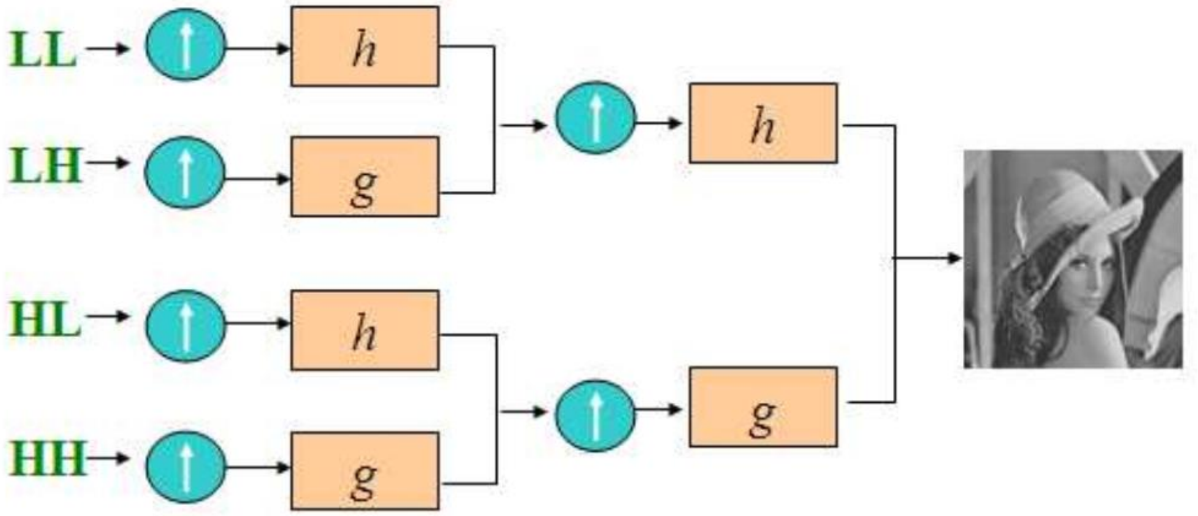


Figure 3.6 2-D IDWT Synthesis or Reconstruction Tree

Now the original input vector can be reconstructed using the four basis vectors

$$6 \cdot \{\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{1}{2}\} = \{3, 3, 3, 3\}$$

$$-4 \cdot \{\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{-1}{2}, \tfrac{-1}{2}\} = \{-2, -2, 2, 2\}$$

$$\frac{6}{\sqrt{2}} \cdot \{\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}, 0, 0\} = \{3, -3, 0, 0\}$$

$$\frac{-4}{\sqrt{2}} \cdot \{0, 0, \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}\} = \{0, 0, -2, 2\}$$

Add the vectors receiving

s= {4, −2, 3, 7}

Haar wavelets for a sample that contains four instances of data can be further expanded to contain information to n items. To determine one level wavelet of Haar and scaling singles the simplest wavelet basis (1/√2, 1/√2) and (1/√2, −1/√2) can be used. Haar wavelets are:

$$\{\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}, 0, 0, ..., 0\}$$

$$\{0, 0, \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}, 0, 0, ...0\}$$

$$\{0, 0, 0, 0, \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}, 0, 0, ...0\}$$

$$\vdots$$

$$\{0, 0, ...0, \frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}\}$$

Therefore N Haar scaling signals are:

$$\{\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0, ..., 0\}$$

$$\{0, 0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0, ...0\}$$

$$\{0, 0, 0, 0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0, 0, ...0\}$$

$$\vdots$$

$$\{0, 0, ...0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\}$$

For 1-D signals declared the Haar scaling are:
α1=1/√2, α2=1/√2and the wavelet filters for 1-D signals areβ1=1/√2, β2=−1/√2.
As well, α12+α22=1, α1+α2=√2, β12+β22=1 andβ1+β2=0

Advantages of Haar Transform:

(a) Faster

(b) Simpler

(c) It is proficient in terms of memory since calculations can be undertaken by obviating the use of temporary storage

(d) The original signal can be reproduces by the synthesis of the transform, It is based on the requirement of the application reconstruction can be lossy.

Two-dimensional wavelets are required for the application of image processing. By designing the 2D filters this problem can be reduce by the theories of multi resolution analysis and wavelets can be comprehensive to higher dimensions. There are two types of classes. One is separable and other is non-separable. The separable filters can directly constructed from their 1D counterparts and the non-separable filters provide the same result. The main use of this is to ease the clarification.

Practically, the common choice for a 2-D scaling function is a product of 1-D functions.

Such as:

φ (x,y [illegible] the form:

$$\phi(x, y) = 2 \sum_{k,l} h(k, l)\phi(2x - k, 2y - l)$$

φ(x) φ (y) both satisfy the dilation equation

h (k, l) =h (k) h (l)

Now as a substitute of one wavelet function, we have three wavelet functions.

$$\phi^{(I)}(x,y) = \phi(x)\psi(y)$$

$$\phi^{(II)}(x,y) = \psi(y)\phi(x)$$

$$\phi^{(III)}(x,y) = \psi(y)\psi(x)$$

The corresponding dilation equations are:

$$output[n] = \sum_{m=0}^{M-1} input[n-m] \times coefficient[m]$$

$$\phi^{(I)}(x,y) = 2\sum_{k,l} g^{(I)}(k,l)\phi(2x-k,2y-l)$$

$$\phi^{(II)}(x,y) = 2\sum_{k,l} g^{(II)}(k,l)\phi(2x-k,2y-l)$$

$$\phi^{(III)}(x,y) = 2\sum_{k,l} g^{(III)}(k,l)\phi(2x-k,2y-l)$$

$$\text{where } g^{(I)}(k,l) = h(k)g(l),\ g^{(II)}(k,l) = g(k)h(l), \text{ and } g^{(III)}(k,l) = g(k)g(l)$$

The principles discussed for 1-D wavelet analysis still hold true in the 2-D world. For example, the approximation image contains the highest frequency values, and the details are lower frequency values. The energy of a 2-D image is the sum of the energies of each of the rows or columns in the image. The third octave will also contain the same energy as the second and first octaves.

3.3.3 Singular value Decomposition (SVD)

To solve several mathematical problems, a linear algebra technique is used. Without compromising the quality of image, a small value is added. This technique is referred as Singular Value Decomposition.

(a) The Singular Values of an image contain good stability due to small value is added to an image, this affect the quality with very minute variation.

(b) SVD is proficient to effectively show the essential algebraic properties of an image, where singular values and singular vectors represent the brightness of the image and geometric characteristics of the image respectively. Image matrix contains several tiny singular values, which is compared with the first singular value. In the reconstruction of the image does not affect the quality of the image if these tiny singular values ignored. That’s why without the loss of generality any image can be considered as square matrix. So this technique can be applied to any type of image. Matrix values are considered as intensity values if it is a gray scale image.

The quality of the image that is reconstructed does not get affected even by ignoring the small singular values. Without any loss of generality any image may be considered as a square matrix. The technique involving SVD can be successfully applied to any kind of image. The matrix values, if it is a grey scale image, are considered as intensity values. This could be modified directly or changes could be affected after changing images into frequency domain. The SVD that decomposes matrix into three matrix of the same size belongs to orthogonal transform.

It is not mandatory for the matrix to be a square one for the purpose of decomposing it using SVD technique. Let us denote the image as matrix A and the SVD decomposition of matrix A is denoted using

$A = USV^T$ U and V are known to be unitary matrices such that

$UU^T = I$, $VV^T = I$, where I is an Identity matrix.

$U = [u_1, u_2, u_3 \ldots\ldots u_n]$,

$V = [v_1, v_2, v_3, \ldots\ldots v_n]$,

U matrix is referred to as left singular values and V matrix is accordingly referred to as right singular values. The decomposition of matrix A is obtained using.
$\text{SVD}(A) = U\,S\,V^T = U\,[D\ 0;\ 0,\ 0]\,V^T$
$S = [D\ 0;\ 0,\ 0]$

Such that all the elements in main diagonal are in decreasing order like $\sigma 1 \geq \sigma 2 \geq \sigma 3 \geq \ldots \sigma n \geq 0$ .Here S that has its main diagonal all positive singular values of A, is a diagonal matrix. The rank of the matrix is equal to the number of non zero values. Number of nonzero values equals the rank of the matrix. To embed watermark these singular values can be used. Since the order of singular matrix is same as A, and hence the resultant matrix is also square. Hence images of equal size can be taken as cover object.

3.4 Discrete Wavelet Transform Level 3

Once the 2-D DWT is applied to the image, it results in four quadrants. Each quadrant is a quarter the size of the original image. It produces the two matrices of coefficients the horizontal details (HL) and vertical details (LH). Using secret key as seed, a pseudo random noise pattern is generated. Using this pattern, the bits of the watermark are embedded in the horizontal (HL) and vertical (LH) coefficient sub-bands. The equation from which is used to embed one of the three watermarks is as given below:

$W'i = Wi + \alpha\, Wixi$, for all pixels in sub band LH, HL

$W'i = Wi$ for all pixels in sub band HH, LL.

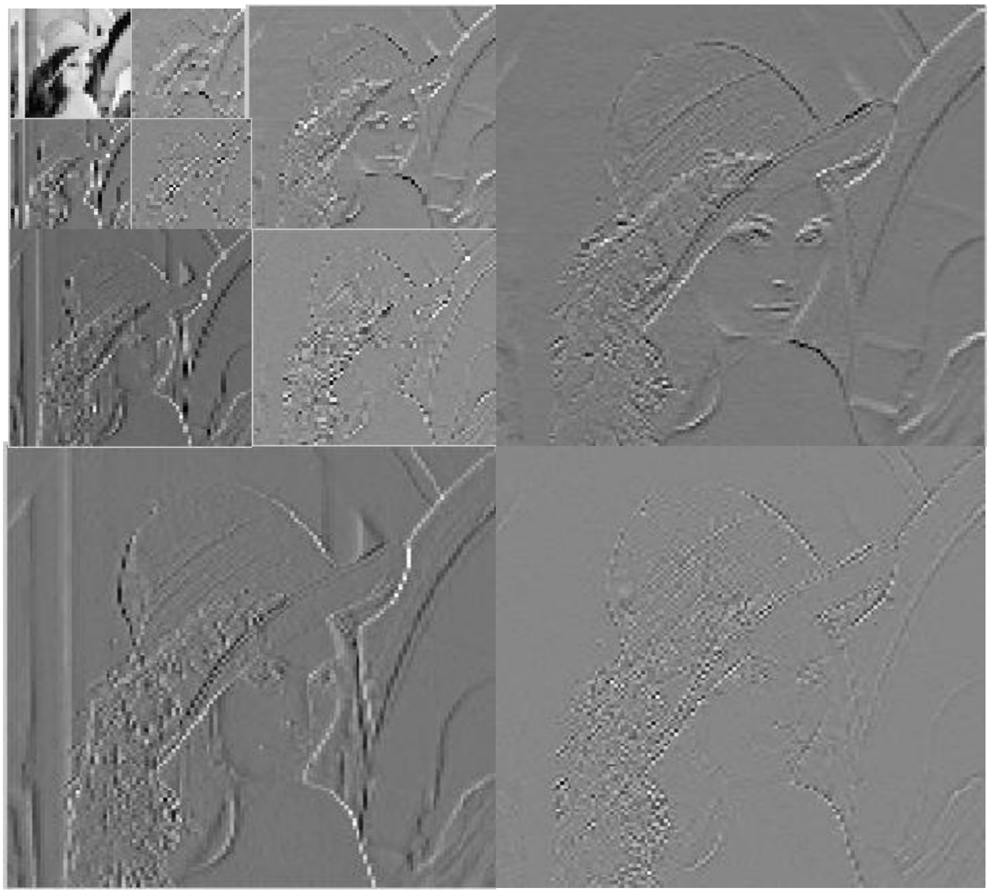


Figure 3.7 Discrete Wavelet Transform Level 3

3.5Algorithm for Embedding Watermark

1. In this method, the watermark in all the channels of the YUV space is hidden by selecting the full band frequency. The energy of the watermark is controlled using the embedding factor. It is represented by < and varies from 0 to 1 ($0 \leq \alpha \leq 1$).

The algorithm used for hiding information is given below :

Step 1 RGB components of the image is transformed into Matrix.

Step 2 DWT is used to decompose the matrices into frequency bands.

Step 3 SVD techniques is applied on each band of host data as well as on watermark using

[U, S, V] = SVD (Band)

[U’, S’, V’] = SVD (W)

Let U, V be orthogonal matrices, S is a diagonal matrix. The diagonal matrix S is used to embed watermark in its diagonal elements using (7). Here Band represents any one of the frequency band such as LL, LH, HL and HH

$$S''=S+alpha*S'$$

The watermark is embedded into the non-zero elements of the diagonal matrix S to obtain the watermarked diagonal matrix S''

Step 4 Inverse SVD is applied on watermarked matrix to get the modified Image Band using

$$Band'=[U*S''*V]$$

Step 5 Inverse transformation Technique is applied to get the watermarked image matrices of R, G, B using

$$[R', G', B']=DWT(LL', LH', HL', HH')$$

3.6 Algorithm for Extracting Watermark

During Extraction process, the RGB components of the watermarked color image are changed into RGB color spaces that can further be transformed into frequency coefficients of four bands. Each band of frequency is SVD transformed to extract watermark from the diagonal elements.

Step 1 Wavelet transformation Technique is applied to YUV matrices to break it into various range of bands of frequency.

$$[LL, LH, HL, HH] = DWT(R, G, B)$$

Step 2 SVD transformation is applied on full band of wavelet transformed YUV matrices

$$\{U, S'', V\}= SVD(Band')$$

Where means one of wavelet transformed frequency bands of YUV matrices frequency bands of YUV matrices

Step 3 Watermark is extracted using

$$S'=(S''-S)/alpha$$

Step 4 Apply inverse SVD on retrieved watermark using unitary matrices U and V

$$W'=US'V$$

3.7 Advantage of SVD algorithm

Expansion of the original data in a coordinate system is represented by SVD. Here, the covariance matrix is diagonal. It must be noted that one can determine the matrix range which is often referred to as rank of the matrix, which is basically equal to the number of linear independent rows or columns, which is commonly referred to as a minimum spanning set. It is also simply referred to as basis. With an intent to quantify accurately the sensitivity of a linear system to numerical error SVD, is used obtain a matrix inverse. In addition to what is spelt out above, it generates solutions to problems associated with least-squares. It also addresses situations when matrices are singular and/or numerically very close to being singular.

3.8 Disadvantage of DWT and SVD algorithm

When watermark is extracted it is less robust at low alpha parameter (transparency). Therefore, this reduces the watermark correlation.

Figure 3.8 Extracted Watermark

Chapter4

Proposed Work

4.1 Structure of a typical watermarking system

Every watermarking system consists of at least two different units:

(a) Host image's Wavelet transform
(b) The watermark embedding unit and
(c) Host image's Inverse Wavelet transform
(d) watermark detection/extraction unit with median of sub bands.

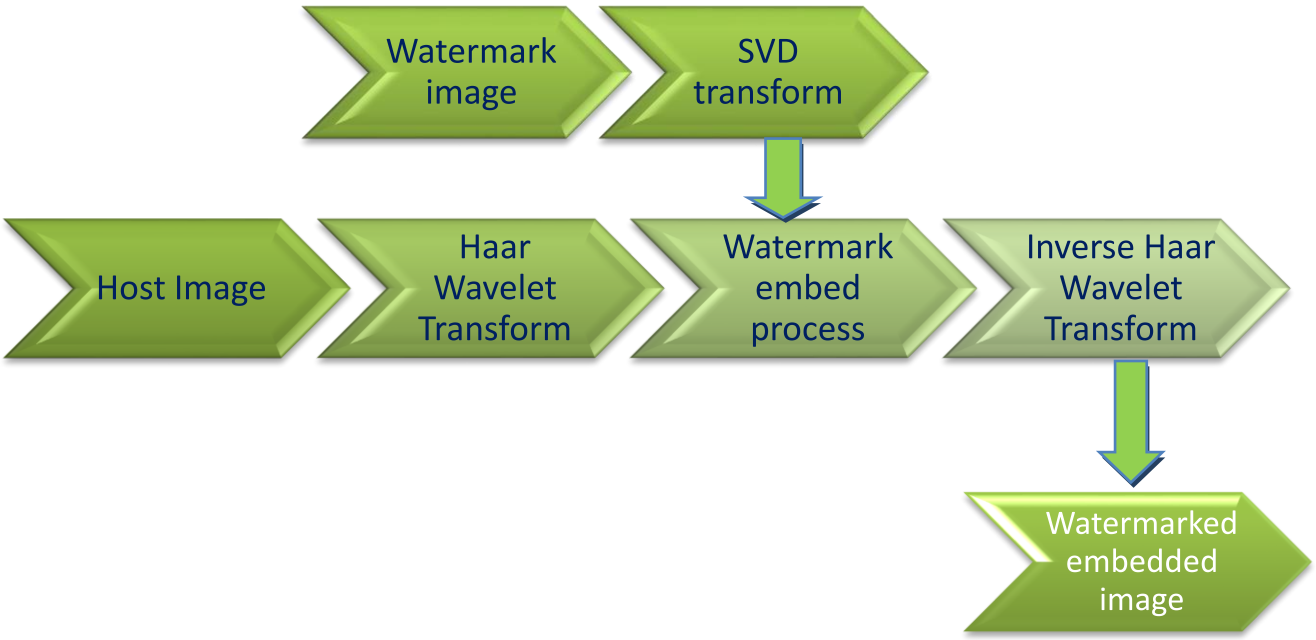


Figure 4.1 Watermark embedding

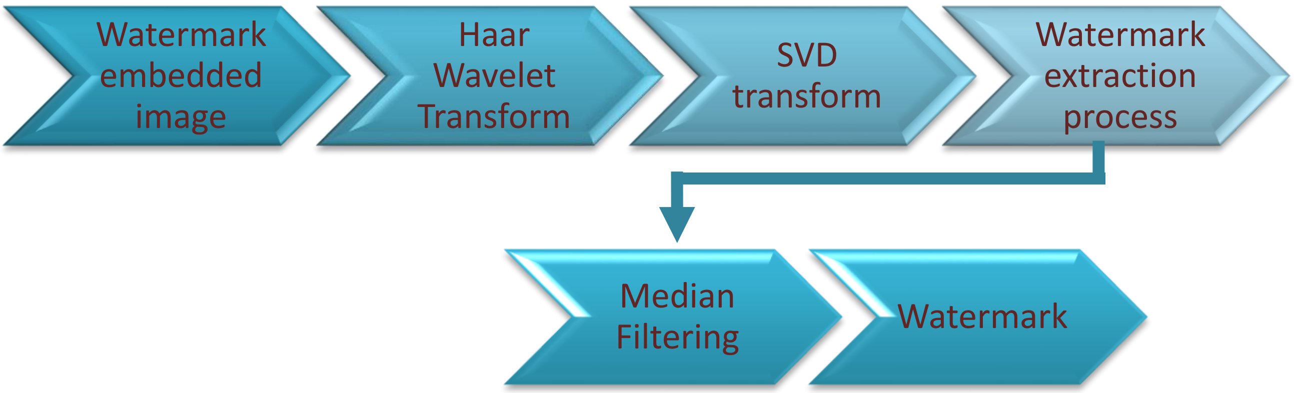


Figure 4.2 Watermark extraction in host image

4.2 Algorithm for Embedding Watermark

In this method, with an aim to hide watermarks, full band frequency is chosen in the channels of YUV color space. To control energy, the embedding factor or control factor is utilized. It is denoted by α and its value lie between 0 to 1 ($0 \le \alpha \le 1$). The algorithm, as spelt out below, is used for hiding information:

Step 1 Conversion in matrix form, the RGB components of color image A.

Step 2 Discrete wavelet transformation technique is utilized in YUV matrices to decompose it into different range bands of frequency. For each level of decomposition, input image matrix Y is transformed into four band of frequency named LLY,LHY,HLY,HHY(5). Similarly U and V image matrices are also transformed into four bands of frequencies using

[LL, LH, HL, HH] = DWT (R, G, B)

Step 3 SVD techniques is applied on each band of host data as well as on watermark using

[U, S, V] = SVD (Band)

[U’, S’, V’] = SVD (W)

Let U, V be orthogonal matrices. Let S be a diagonal matrix. The diagonal matrix S is used to embed watermark in its diagonal elements using (7). Here Band represents any one of the bands of frequency such as LL, LH, HL and HH

S’’=S+alpha*S’

The watermark ‘is embedded into the non-zero elements of the diagonal matrix S to obtain the watermarked diagonal matrix S’’

Step 4 Inverse SVD is applied on watermarked matrix to obtain the modified Image Band using

Band’= [U*S’’*V]

Step 5 Inverse transformation Technique is applied to get the watermarked image matrices of sub bands using

Embed image=DWT (LL’, LH’, HL’, HH’)

4.3 Algorithm for Extracting Watermark

During Extraction process, the RGB constituents of the colour image of watermark are converted into RGB colour spaces that in turn can be transformed into frequency coefficients of four bands. Each band of frequency is SVD transformed to extract watermark from the diagonal elements.

Step 1 Wavelet transformation Technique is applied to YUV matrices to decompose it into different range of frequency bands

[LL, LH, HL, HH] = DWT (R, G, B)

Step 2 SVD transformation is applied on full band of wavelet transformed YUV matrices

{U, S'', V}= SVD (Band')

Where means one of wavelet transformed frequency bands of YUV matrices frequency bands of YUV matrices

Step 3 Watermark is extracted using

S'=(S''-S)/alpha

Step 4 Apply inverse SVD on retrieved watermark using unitary matrices U and V

W'=US'V

Step 5 Apply median filter on watermark extracted from all subbands.

4.4 Median filter application

Image filtering is used to Remove noise, Sharpen contrast, Highlight contours, Detect Edges, Other uses?

Image filters can be classified as linear or nonlinear. Linear filters are also known as convolution filter as they can be represented using a matrix multiplication.

Median filtering is a nonlinear method used to remove noise from images. It is widely used as it is very effective at removing noise while preserving edges. It is particularly effective at removing 'salt and pepper' type noise. The median filter works by moving through the image pixel by pxel, replacing each value with the median value of neighbouring pixels. The pattern of neighbours is called the "Windows", which slides, pixel by pixel, over the entire image. The median is calculated by first sorting all the pixel values from the window into numerical order, and then replacing the pixel being considered with the media (median) pixel value.

4.4.1 Median filter

Noise reduction of the image of the signal is most vital during signal processing. Median filtering is a non-linear digital filtering method. This method is often used to reduce noise. Such reduction in noise is a preprocessing step that is often aimed to improve the result of subsequent processing. It is widely used since it is used to preserve edges, while successfully removing noise.

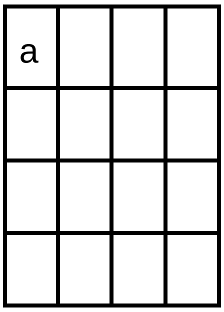
4.4.2 Algorithm description

To run through the signal entry by entry is the main idea of median filter. In this one replaces each entry with the median of its neighborhood. The pattern of neighborhood pattern is referred to as "window". Here window slides, entry by entry, over the entire signal.

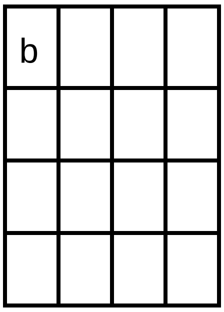
The most evident window for 1D signals is just the first few preceding and following entries. For 2D (or higher-dimensional) signals, such as images, however, more complex window patterns are possible (such as "box" or "cross" patterns). It must be noted that should the window have an odd number of entries, then the median is pretty simple to define. After all the entries in the window are sorted numerically, it is just the middle value. For an even number of entries, there is more than one possible median for an even number of entries.

4.4.3 How to apply median filter

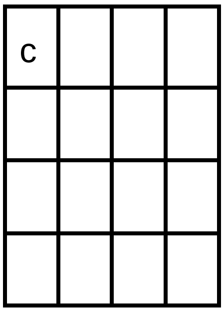
To improve the extracted watermark correlation. Non linear filter (median filter) is applied.



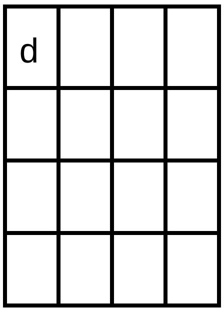
LL band



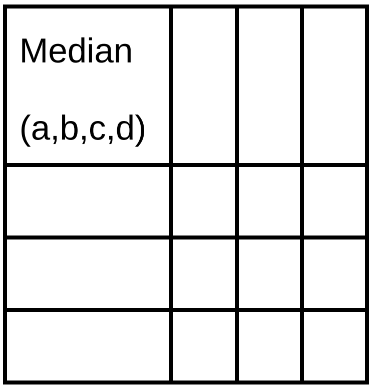
LH band



HL band



HH band



HH band

W(i,j)=median(a,b,c,d);

The median filter is applied on first element of LL, LH, HL and HH band

The result of median function is stored in another zero matrix. This is repeated throughout elements the matrix.

The matrix contains the watermark that have good correlation.

The extracted watermark is extracted from all sub bands. The median filter is applied on four extracted watermarked image. Because attack in image cause distortion in watermark But attack does not affect all sub bands. But attack depends on the type of attack.

So any sub band may affect. The median filter is applied on all extracted watermarked image. The all elements are picked from first element of all matrix. Median filter is applied on these elements throughout the image.

4.4.4 Improvement in robustness of Watermark

To enhance the robustness of watermark it is implemented all level of 3 level of DWT. To reduce the diagonal effect of caused by SVD. Median filter is applied to reduce the alpha and increase in robustness of watermark.

Figure 4.3 Extracted Watermark using median filter

Chapter 5

5.1 Results

Watermark is extracted at various alpha parameters

Figure 5.1 Host Image

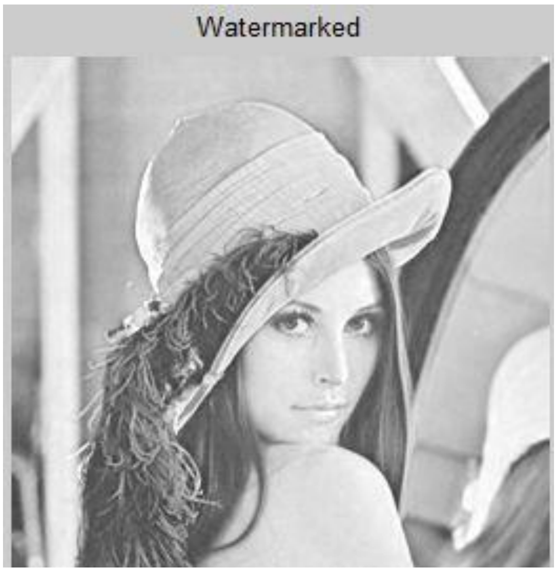


Figure 5.2 Host Image Watermarked Image alpha 0.2

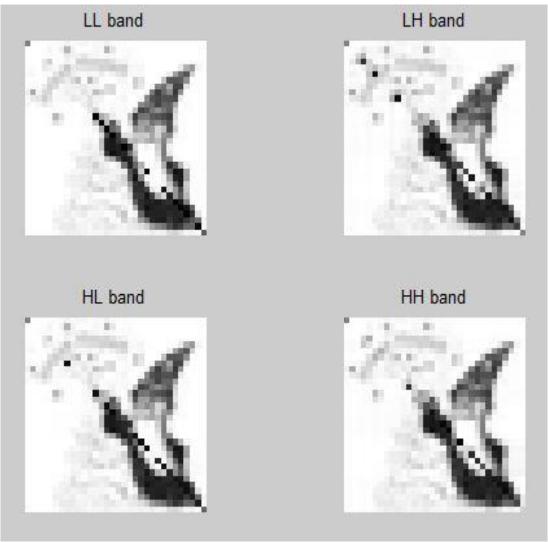


Figure 5.3 Host Image Extracted Watermarked from all subands at alpha 0.2

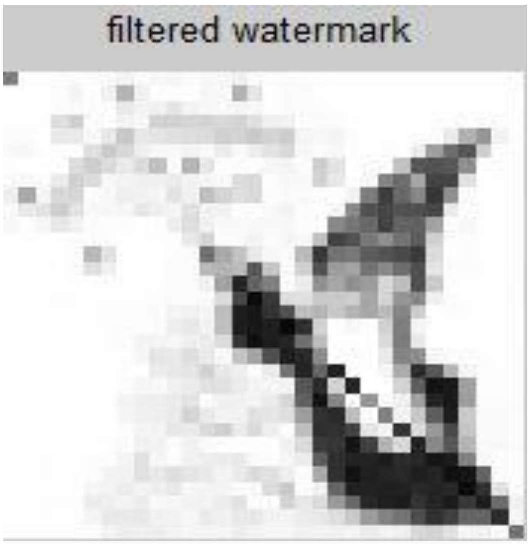


Figure 5.4 Host Image

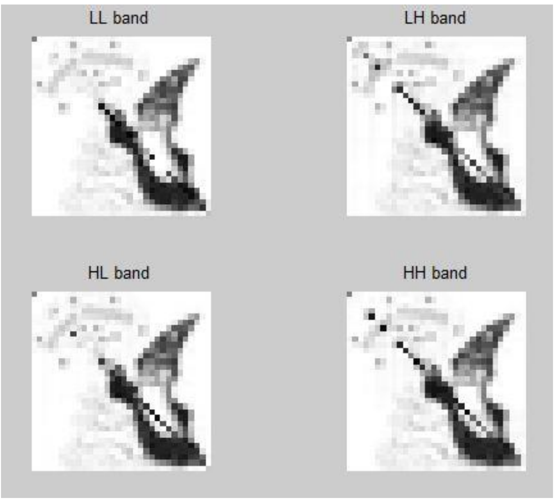


Figure 5.5 Watermarked Image alpha 0.4

Figure 5.6 Extracted Watermarked from all subands at alpha 0.04

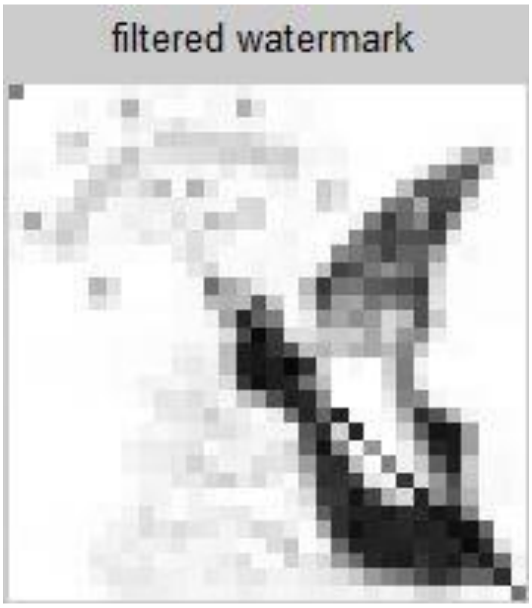


Figure 5.7 Extracted Watermark

Figure 5.8 Watermarked Image alpha 0.08

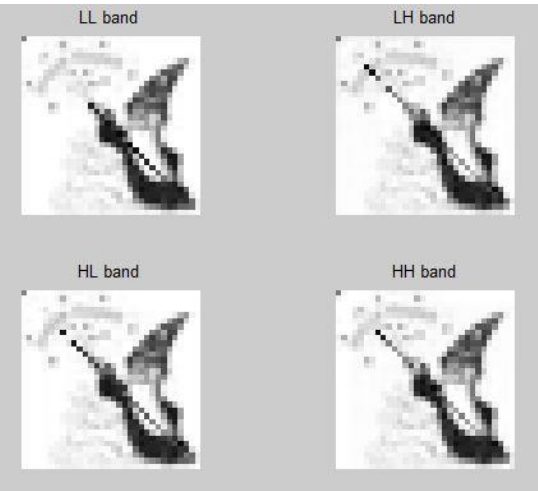


Figure 5.9 Host Image Extracted Watermarked from all subands at alpha 0.8

Figure 5.10 Host Image

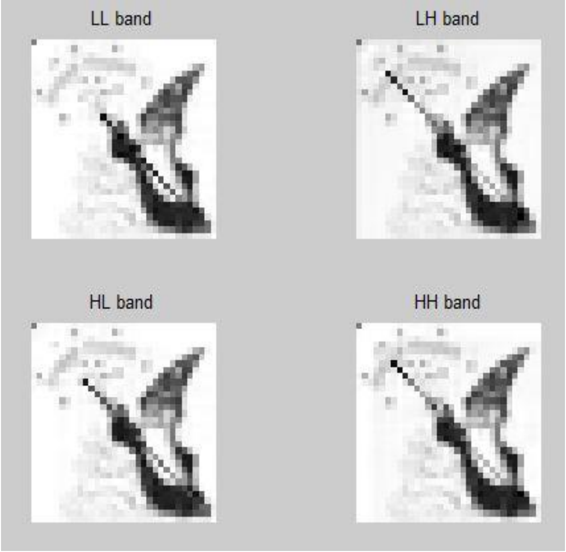


Figure 5.11 Host Image Watermarked Image alpha 0.9

Figure 5.12 Host Image Extracted Watermarked from all subands at alpha 0.9

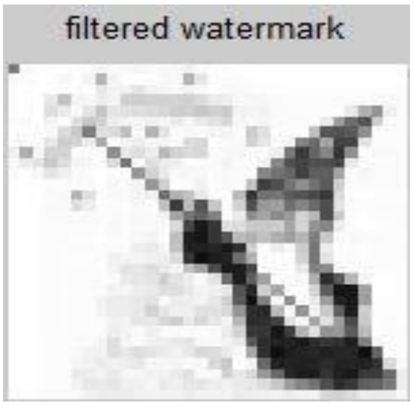


Figure 5.13 Host Image

Tempered watermarked image

Histogram equalization

Histogram equalization, a concept of contrast adjustment is utilized by making use of image's histogram. This method normally increases the global contrast in respect of variety of images, particularly so when the usable data of the image is represented by close contrast values. It must be noted that through this adjustment, the intensities can be better distributed on the histogram. This facilitates for areas with lower local contrast to gain a higher contrast.

Figure 5.14 Host image

Figure 5.15 Histogram equalisation

Histogram equalization , therefore ,causes major temper in watermarked image. At various values of alpha parameter, the watermark so extracted is given below. The watermark, so extracted is compared with real watermark image.

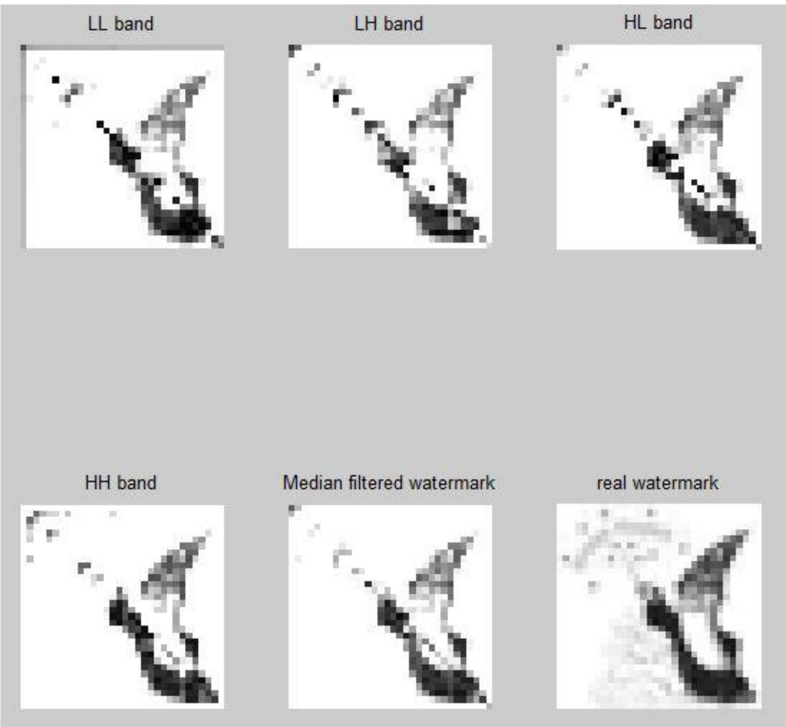


Figure 5.16 Histogram equalised watermark extracted from various subbands at alpha 0.01

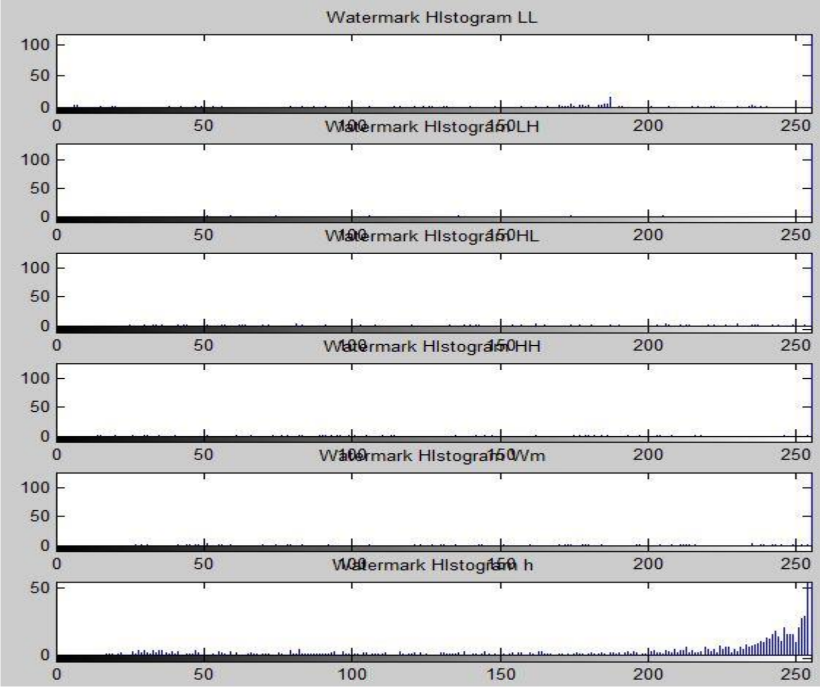


Figure 5.17 Histogram of extracted watermark from various subbands and real watermark

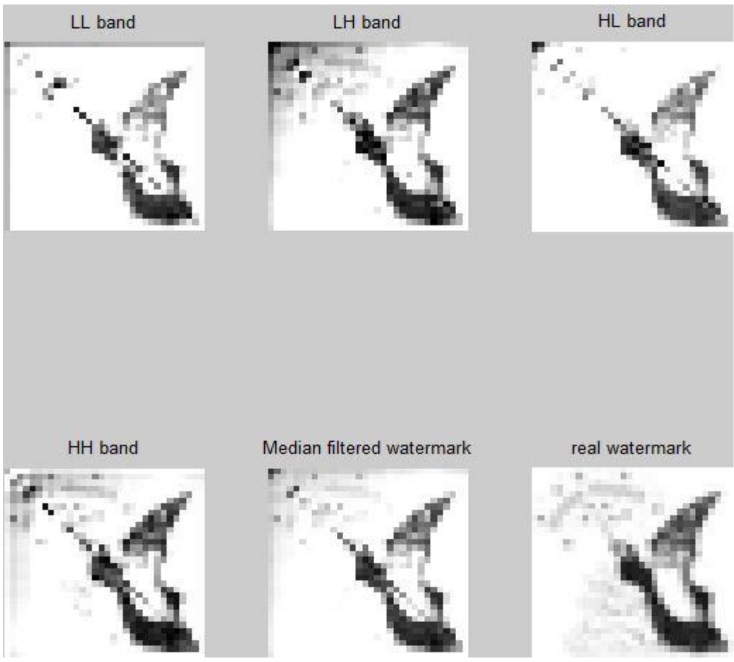


Figure 5.18 Watermark extracted from various subbands at alpha 0.06

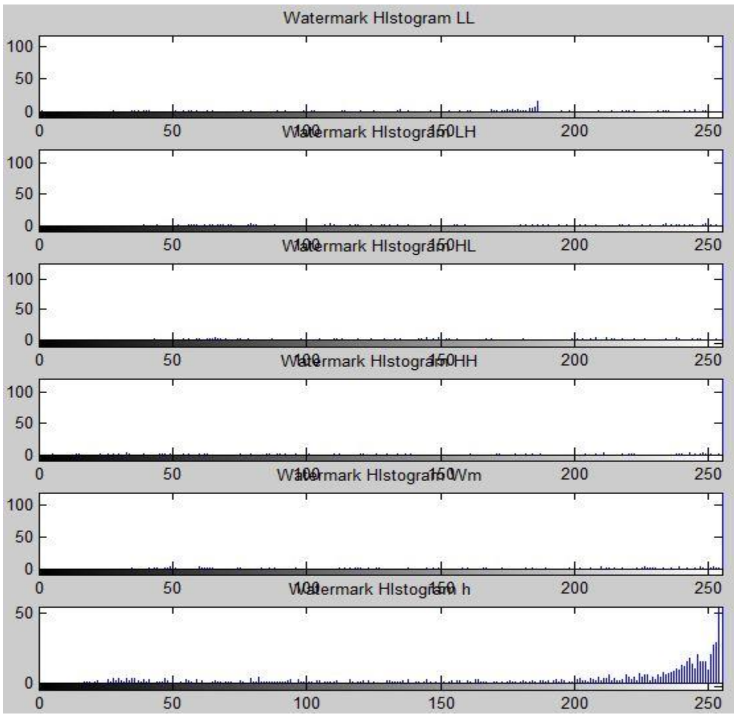


Figure 5.19 Histogram of watermark extracted from various subbands at alpha 0.06

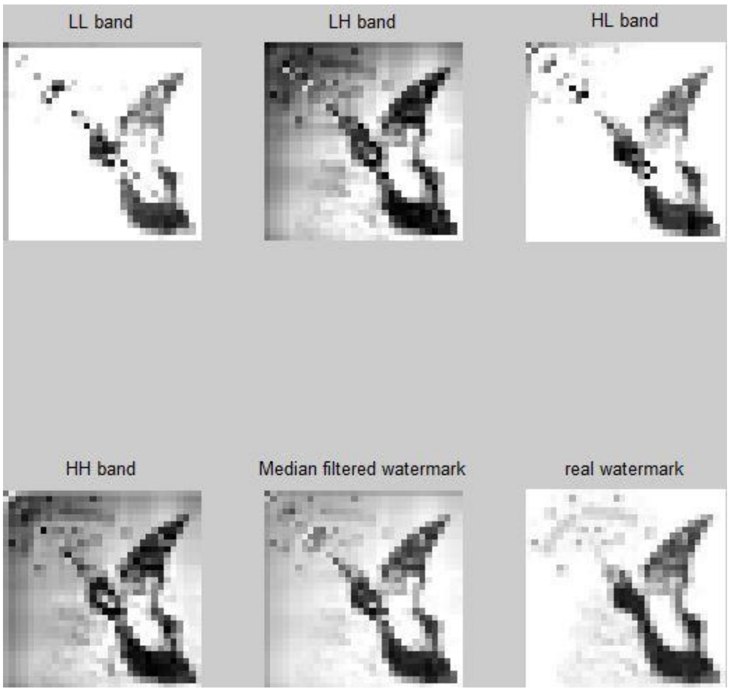


Figure 5.20 Watermark extracted from various subbands at alpha 0.11

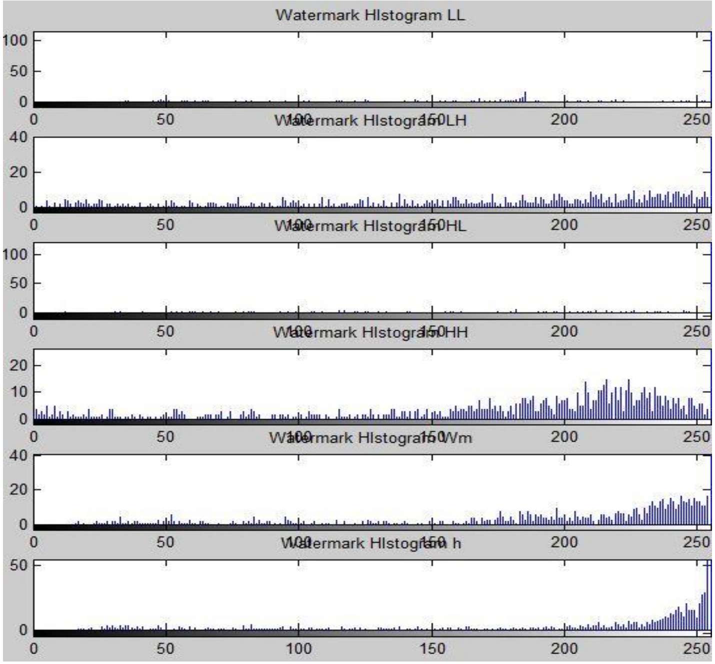


Figure 5.21 Histogram of watermark extracted from various subbands at alpha 0.06

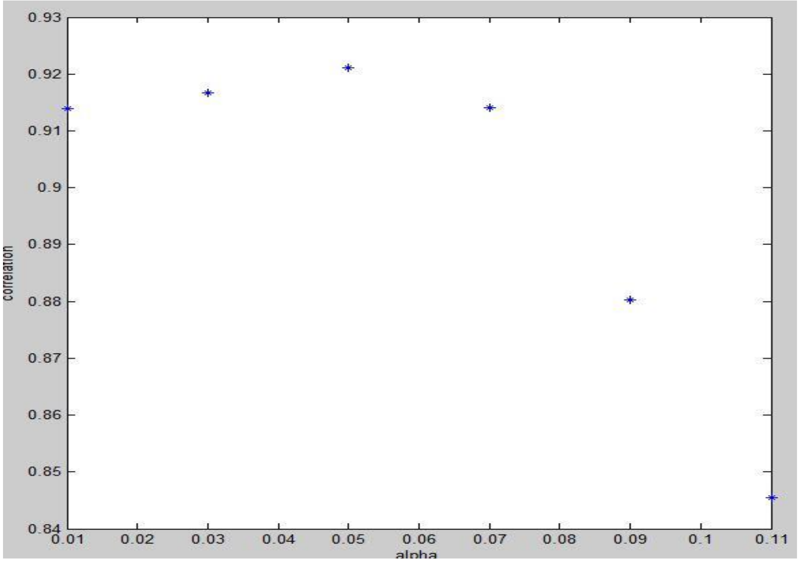


Figure 5.22 Correlation of proposed extracted watermark

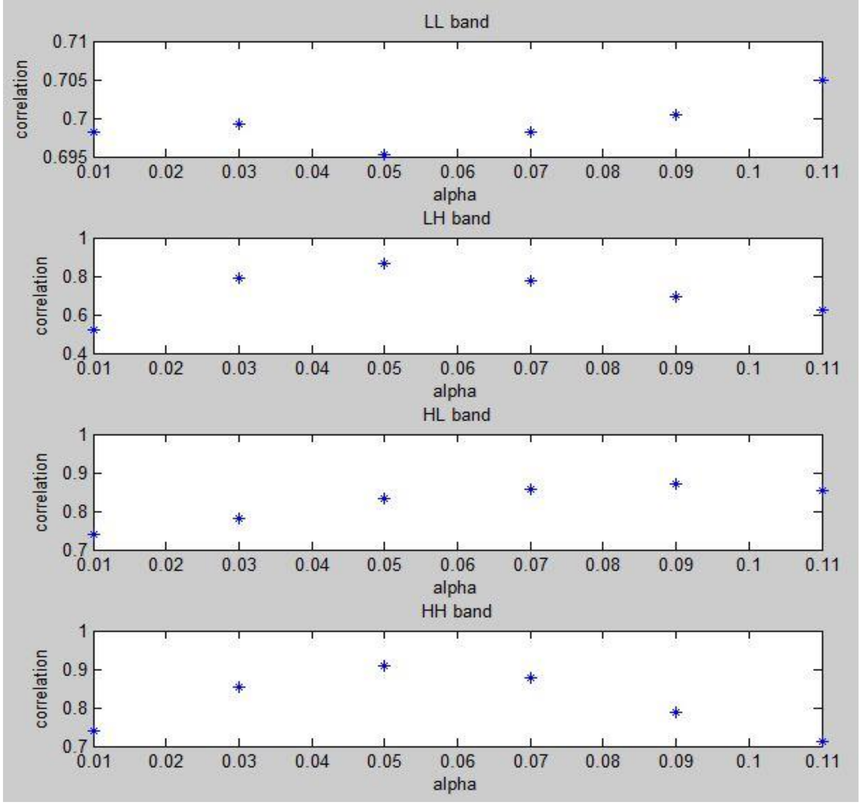


Figure 5.23 Correlation of extracted watermark

Average function

In statistics and image processing, to smooth a data set is to create an approximating function that attempts to capture important patterns in the data, while leaving out noise or other fine-scale structures/rapid phenomena. In smoothing, the data points of a signal are modified so individual points (presumably because of noise) are reduced, and points that are lower than the adjacent points are increased leading to a smoother signal.

Figure 5.24 Host image

Figure 5.25 Tampered by average function

This affects the watermark majorly in LH band and HL band.

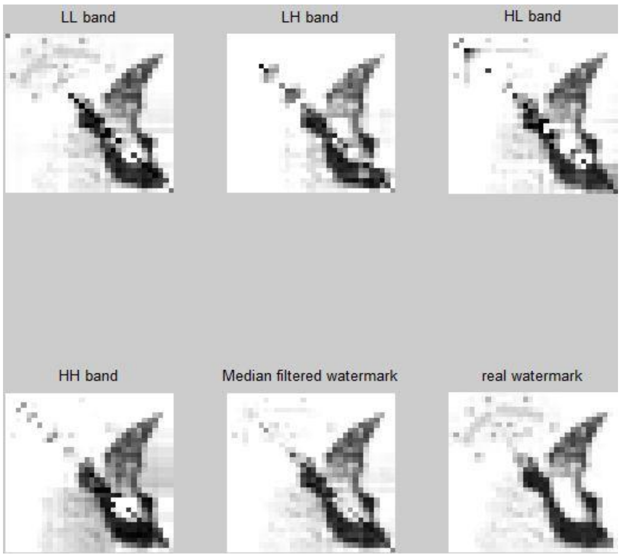


Figure 5.26 Watermark extracted from various subbands at alpha 0.1

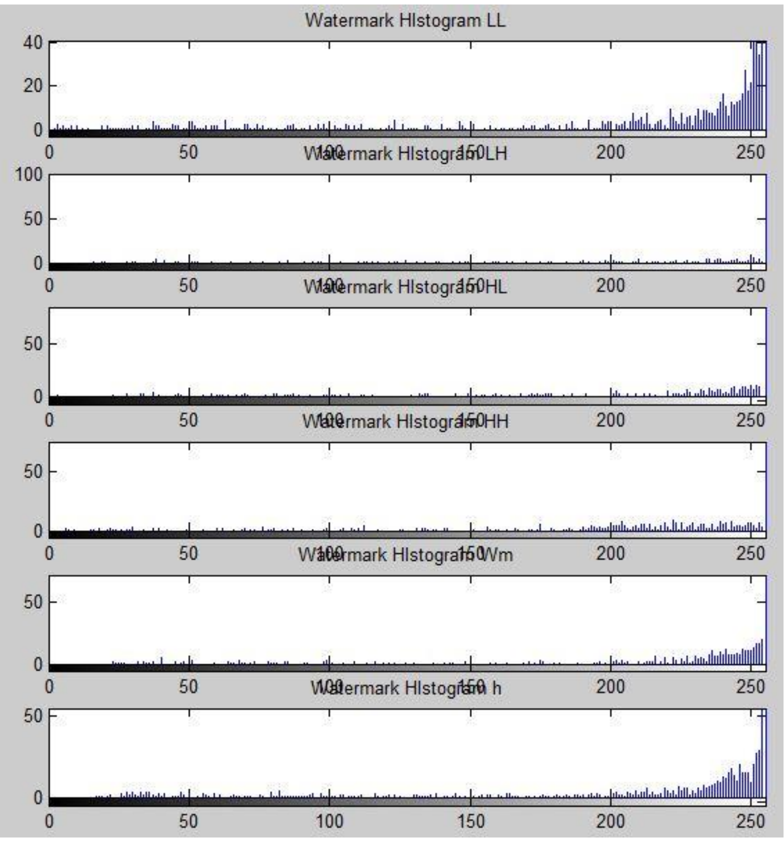


Figure 5.27 Histogram of watermark extracted from various subbands at alpha 0.01

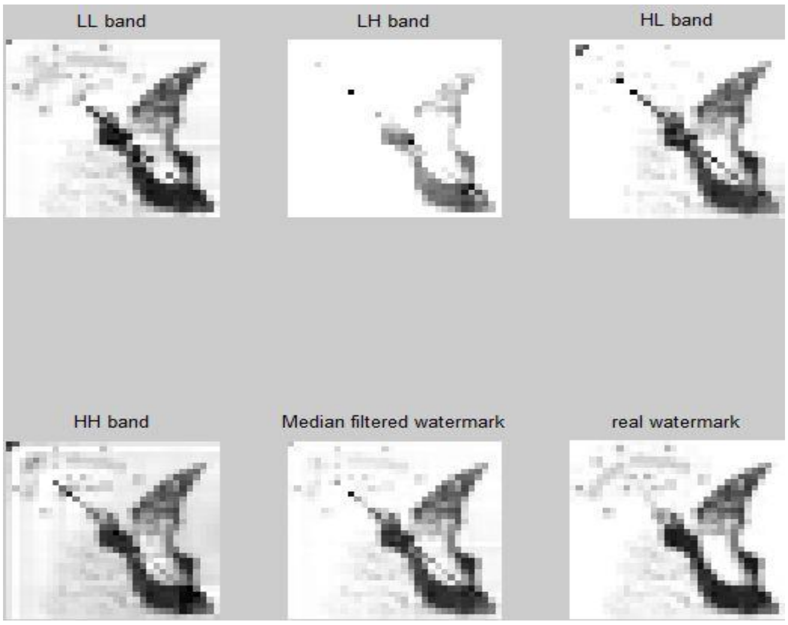


Figure 5.28 Watermark extracted from various subbands at alpha 0.6

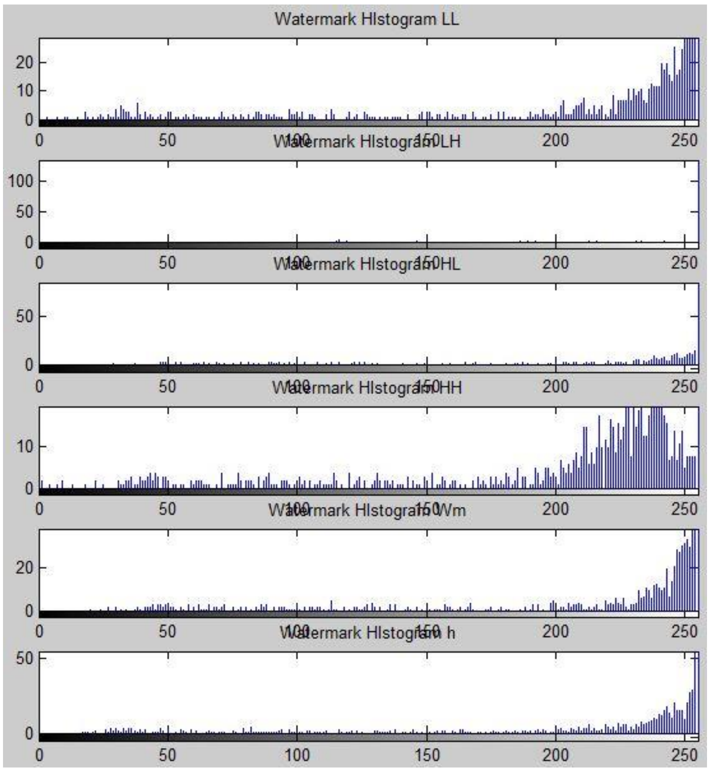


Figure 5.29 Histogram equalized watermark extracted from various subbands at alpha 0.06

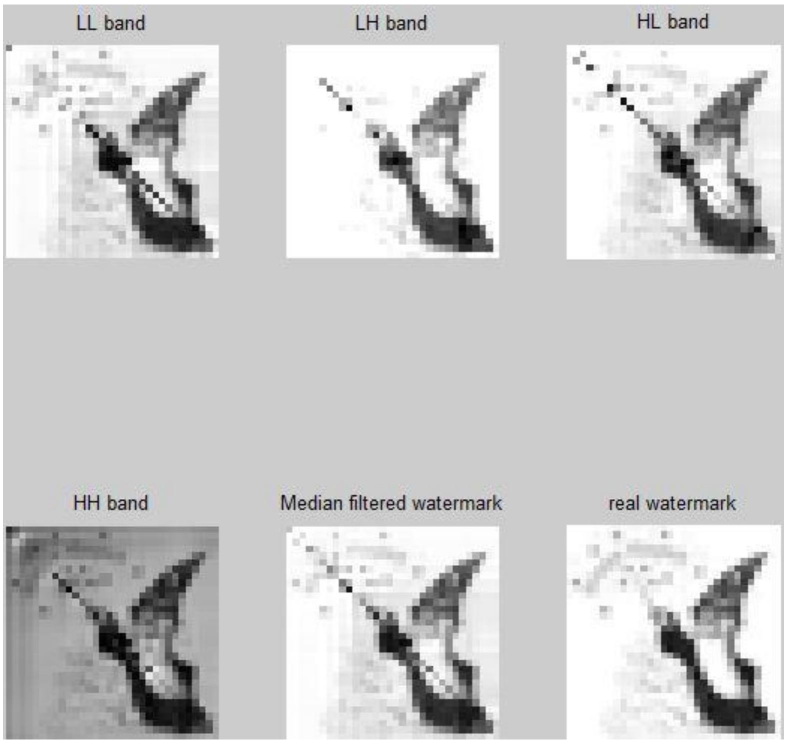


Figure 5.30 Watermark extracted from various subbands at alpha 0.11

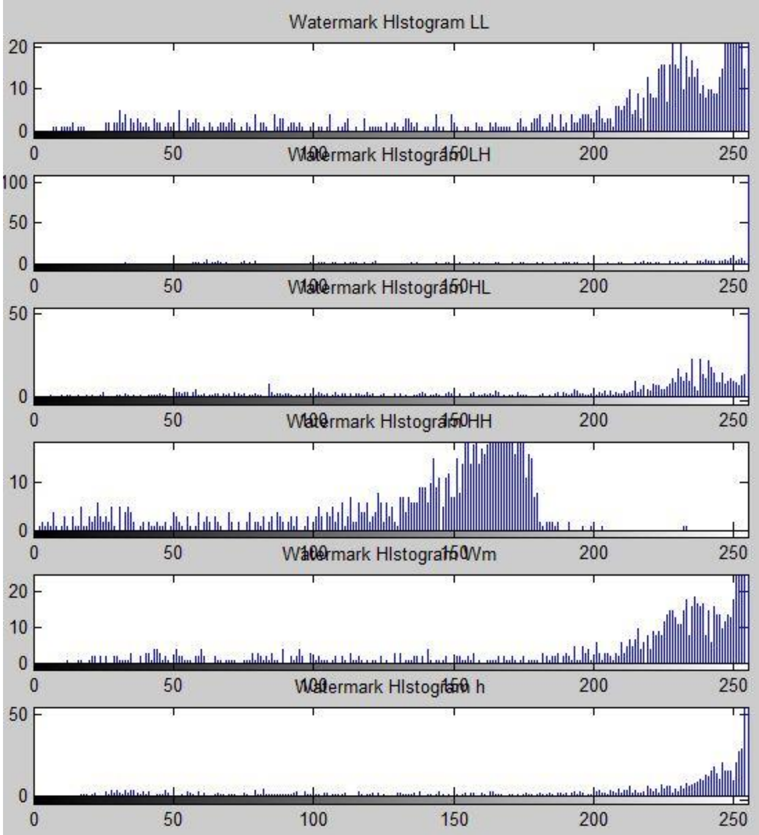


Figure 5.31 Histogram equalized watermark extracted from various subbands at alpha 0.11

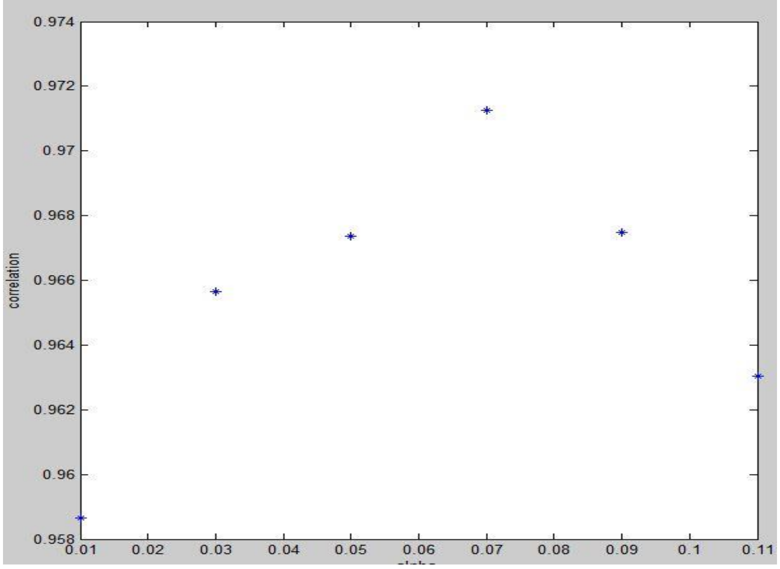


Figure 5.32 Correlation of proposed extracted watermark

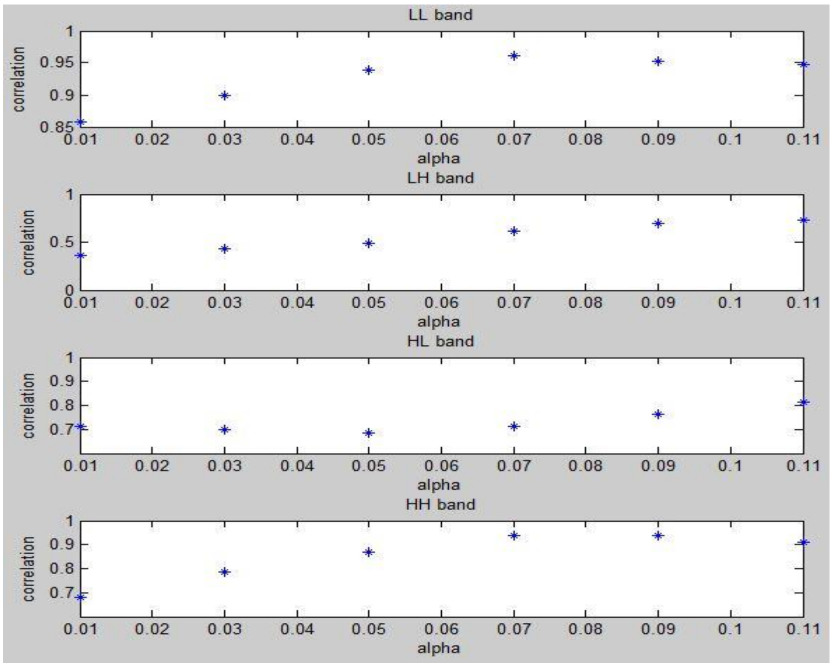


Figure 5.33 Correlation of extracted watermark

Crop

With intent to improve framing the outer part of the image is removed. This is referred to as Cropping. It also accentuates the subject matter as also changing the aspect ratio. Based on the nature of application, Cropping may be applied to artwork, film footage or physical photography or achieved digitally using image editing software. It finds wide application in broadcasting, photographic, graphic design and printing industries.

Figure 5.34 Host image

Figure 5.35 Tampered by cropping

The cropping cause distortion in watermark. It is visible in watermark's right bottom of corner. The water mark is distorted in

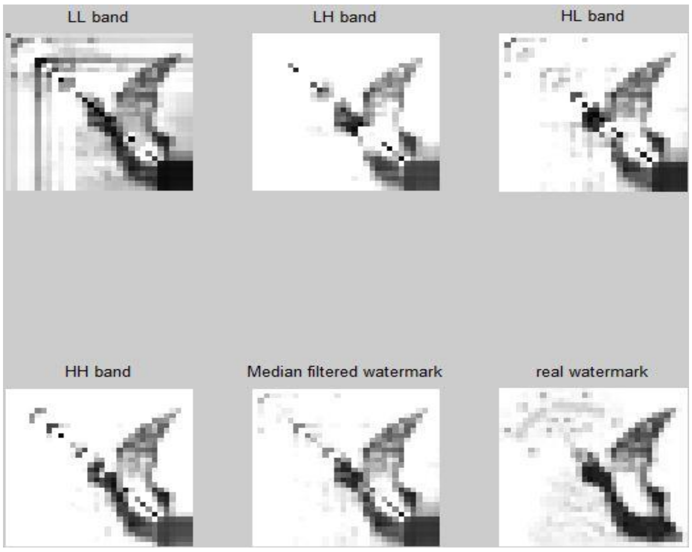


Figure 5.36 Tampered by crop function at alpha 0.01

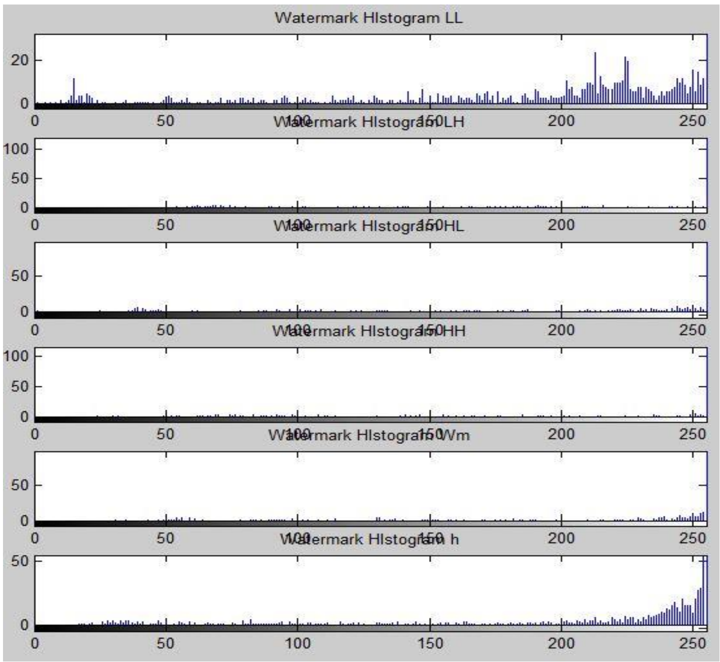


Figure 5.37 Watermark extracted from various subbands at alpha 0.11

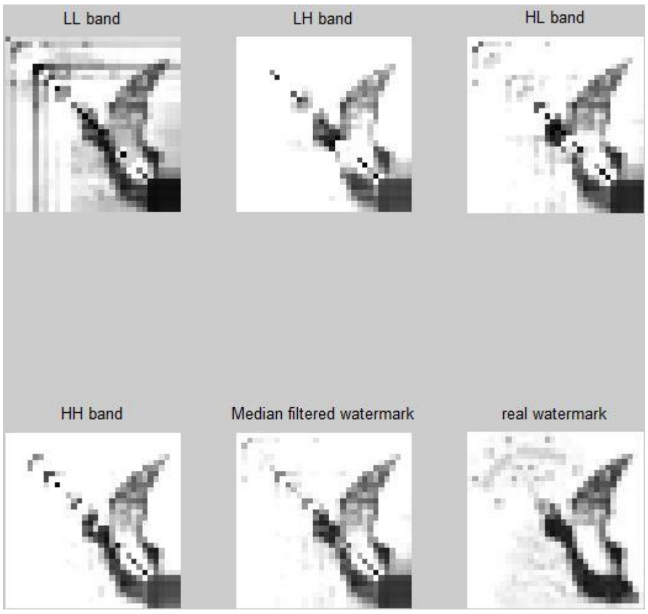


Figure 5.38 Tampered by crop function alpha at 0.06

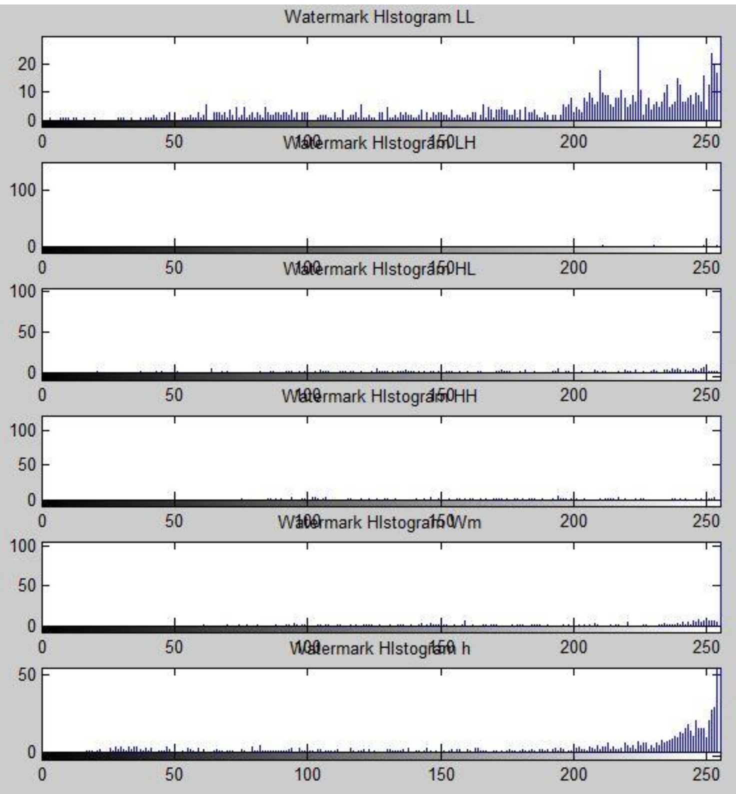


Figure 5.39 Histogram of watermark extracted from various subbands at alpha 0.11

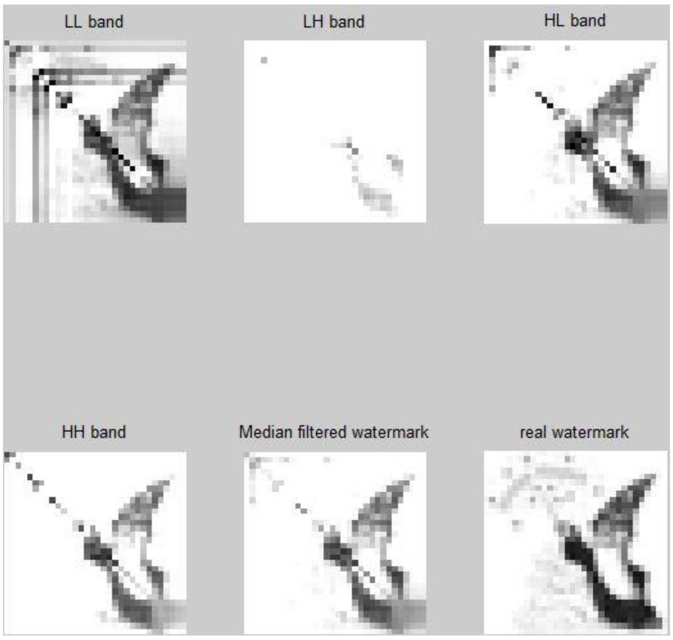


Figure 5.40 Tampered by crop function alpha at 0.11

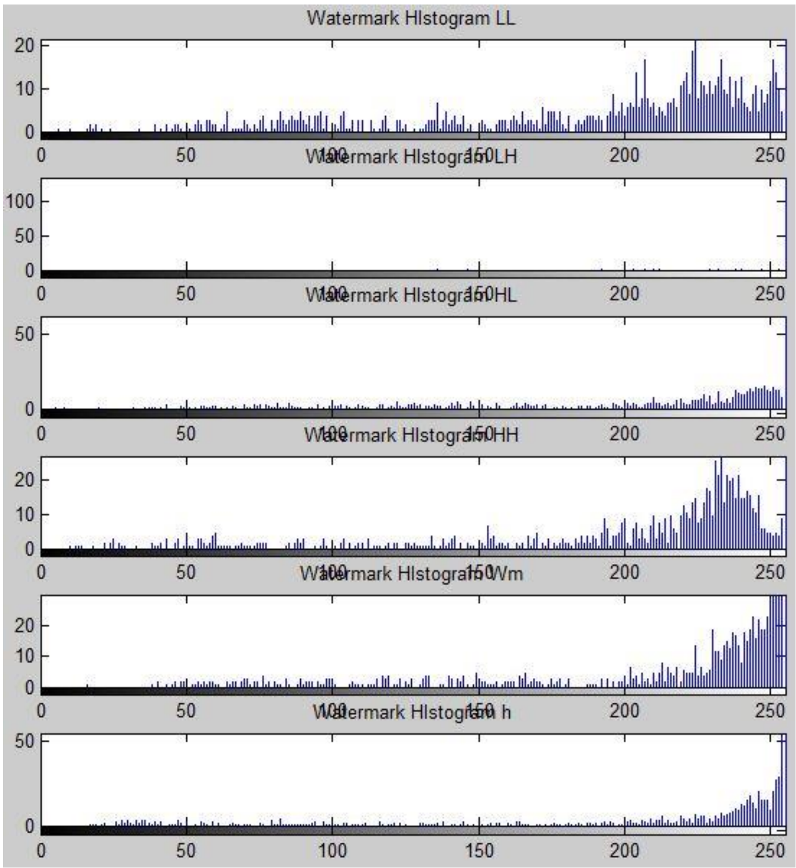


Figure 5.41 Histogram of watermark extracted from various subbands at alpha 0.11

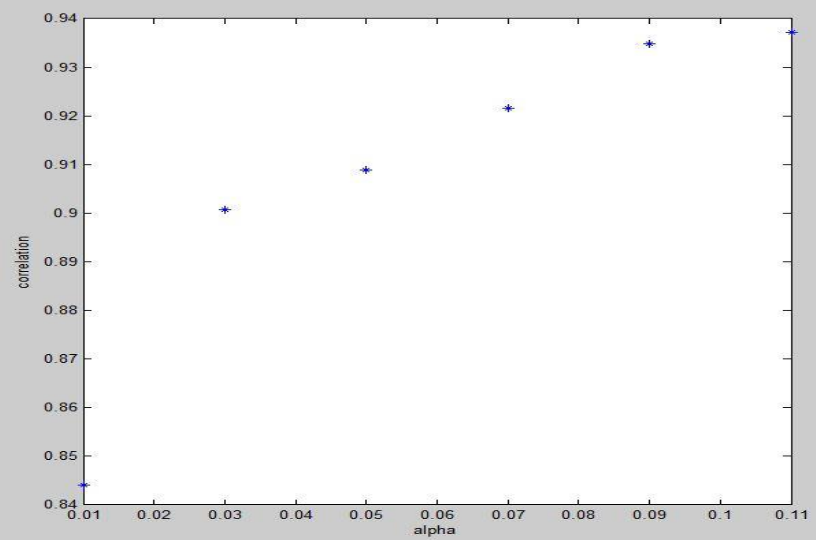
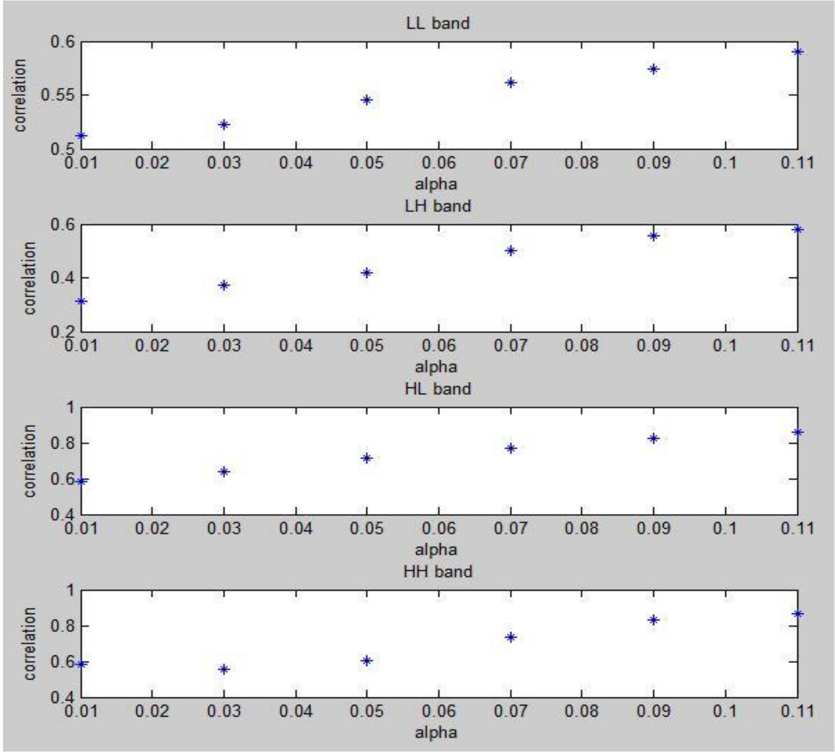


Figure 5.50 Correlation of proposed extracted watermark



<u>**Figure 5.51 Correlation of extracted watermark**</u>

Rescale

The process of scaling of image, often used in in computer graphics involves resizing of digital image. Scaling, it must be understood is essentially a non-trivial process which invariably involves, amongst other things, a trade-off between efficiency, smoothness and sharpness. In case of graphics like bitmap graphics, with the increase or reduction in the size of the image, the pixels that forms the image become increasingly visible, making the image appear "soft" if pixels are averaged, or jagged if not.

Figure 5.52 Host image

Figure 5.53 Tampered by rescaling

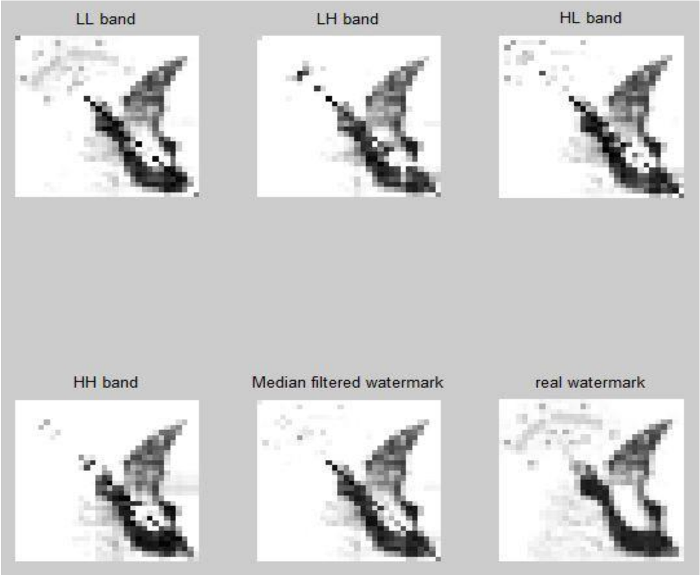


Figure 5.54 Tampered by rescaling alpha at 0.01

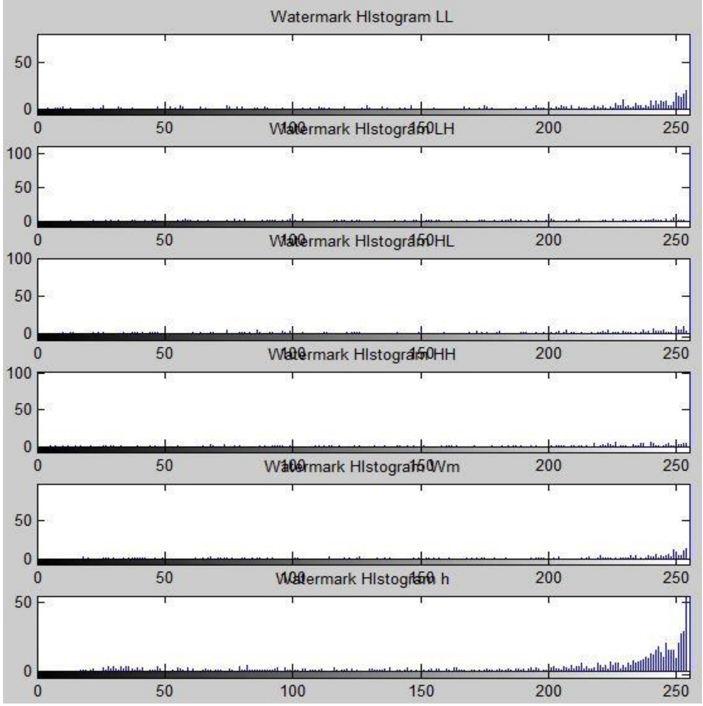


Figure 5.55 Histogram of watermark extracted from various subbands at alpha 0.01

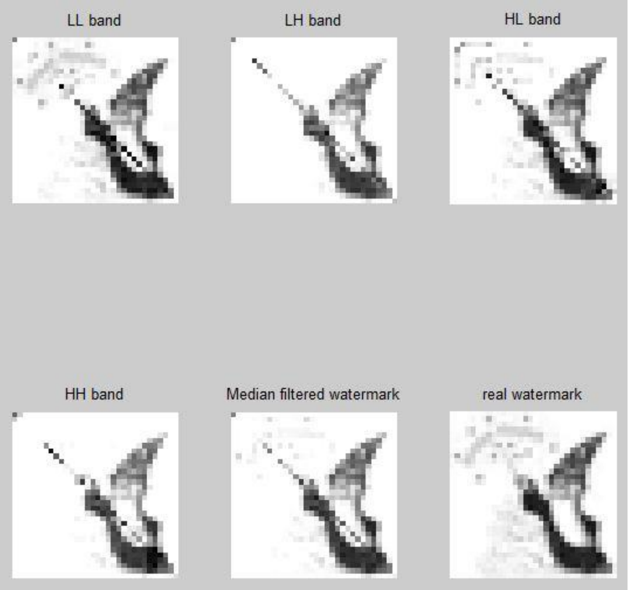


Figure 5.56 Tampered by rescaling alpha at 0.06

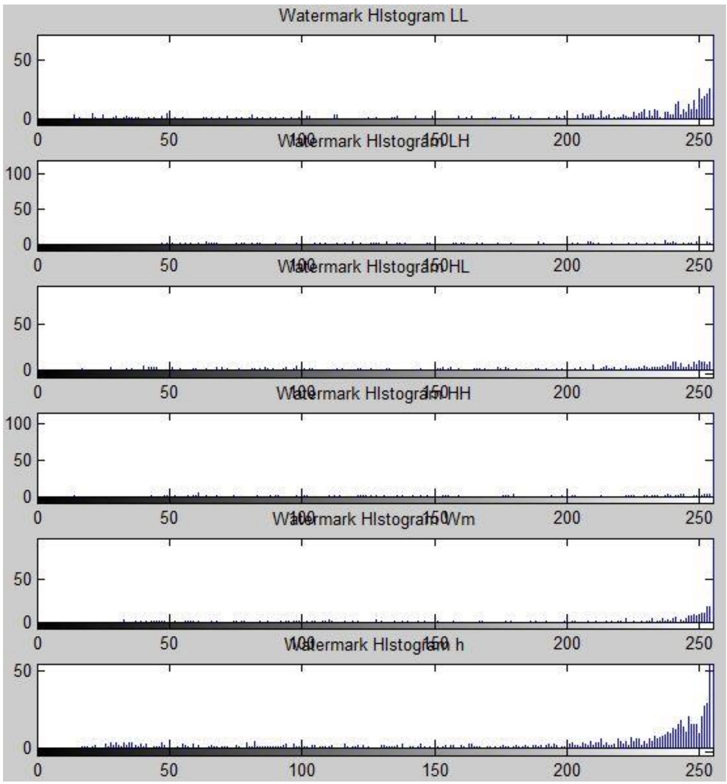


Figure 5.57 Histogram of watermark extracted from various subbands at alpha 0.06

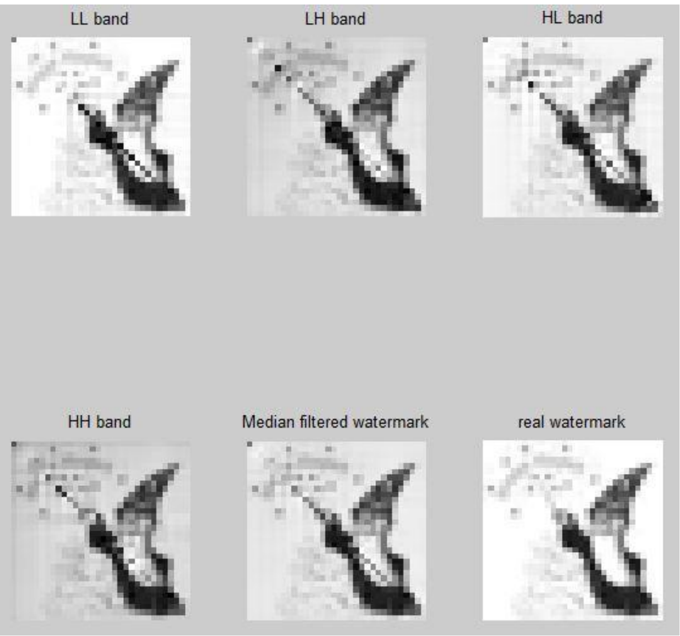


Figure 5.58 Tampered by rescaling alpha at 0.11

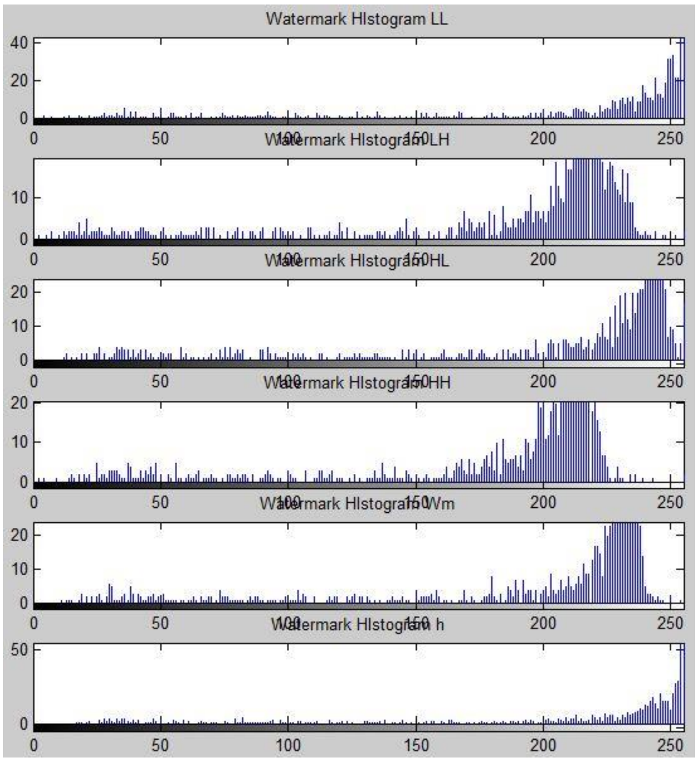


Figure 5.59 Histogram of watermark extracted from various subbands at alpha 0.11

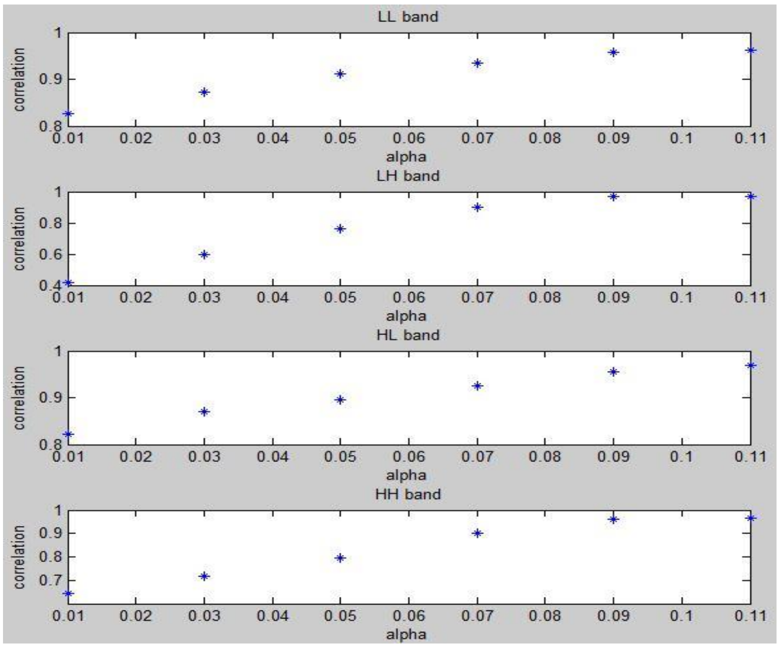


Figure 5.60 Correlation of proposed extracted watermark

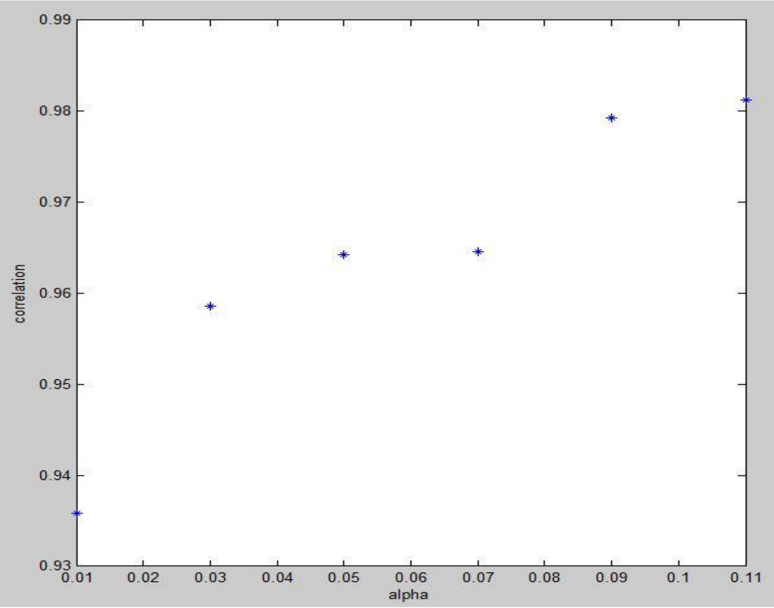


Figure 5.61 Correlation of proposed extracted watermark

Gaussian Noise

Image noise is essentially a random variation in terms of brightness or the colour information as regards the image .It is not present in the object, and is usually an aspect of electronic noise. The sensor and circuitry of a scanner or digital camera produces the Gaussian Noise. It is also known to originate in film grain. It may also originate in the unavoidable shot noise of an ideal photon detector. It is an unwanted spin-off of image capture which adds counterfeit and information that is extraneous .Principal sources of Gaussian noise in digital images emerge during acquisition e.g. sensor noise caused by poor illumination and/or high temperature, and/or transmission e.g. electronic circuit noise.

Figure 5.62 Host image

Figure 5.63 Tampered by Gaussian noise

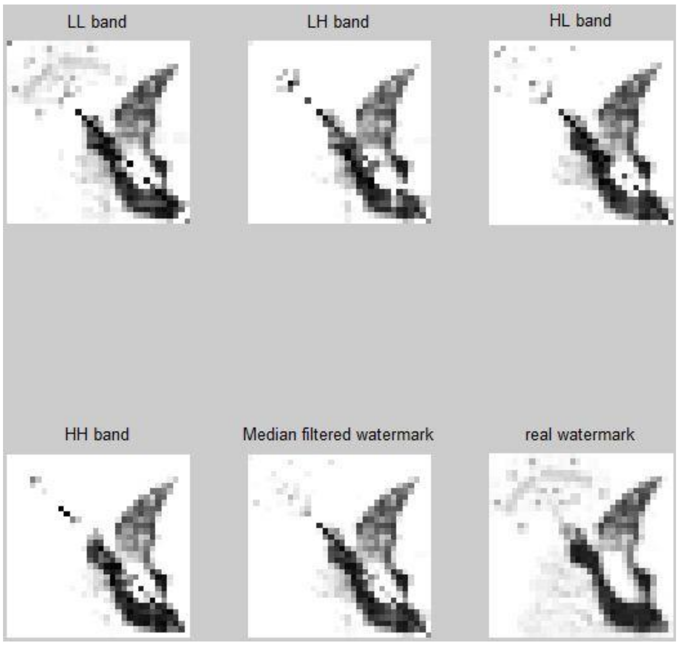


Figure 5.64 Tampered by Gaussian noise at alpha 0.01

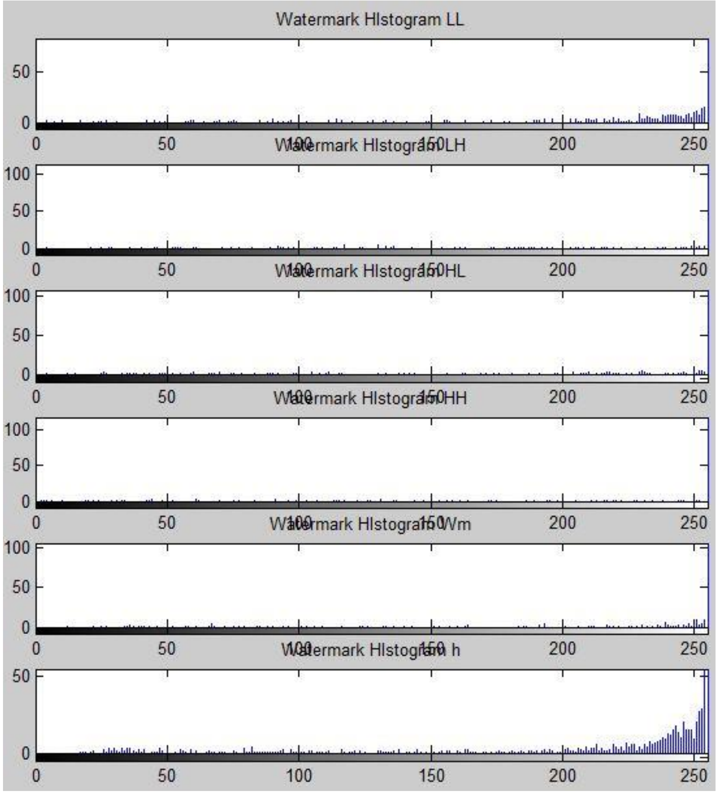


Figure 5.65 Histogram of watermark extracted from various subbands at alpha 0.01

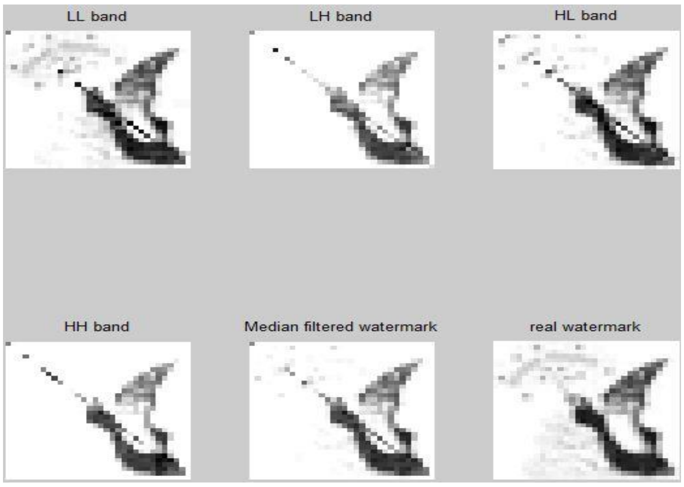


Figure 5.66 Tampered by Gaussian noise at alpha 0.06

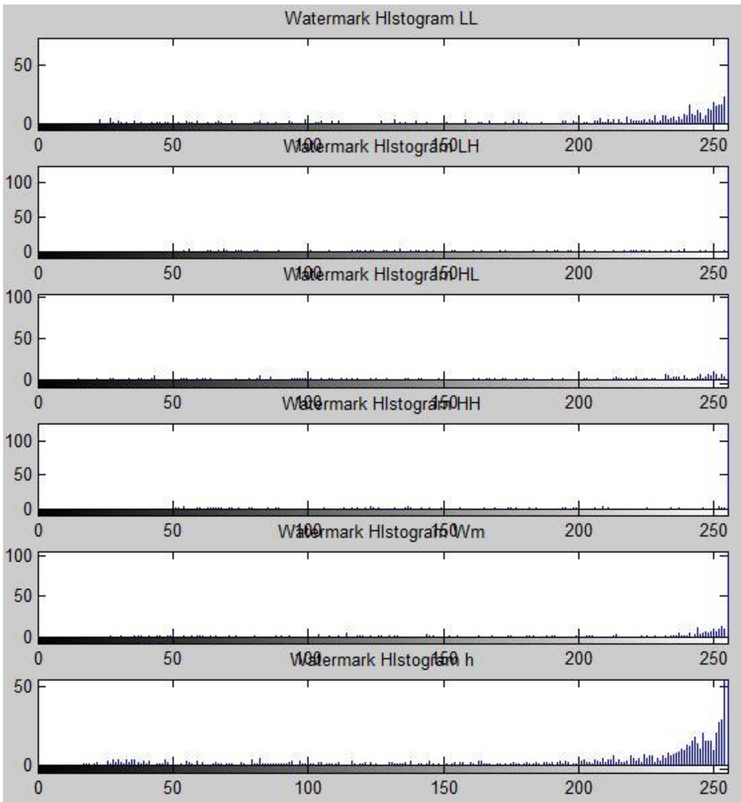


Figure 5.67 Histogram of watermark extracted from various subbands at alpha 0.06

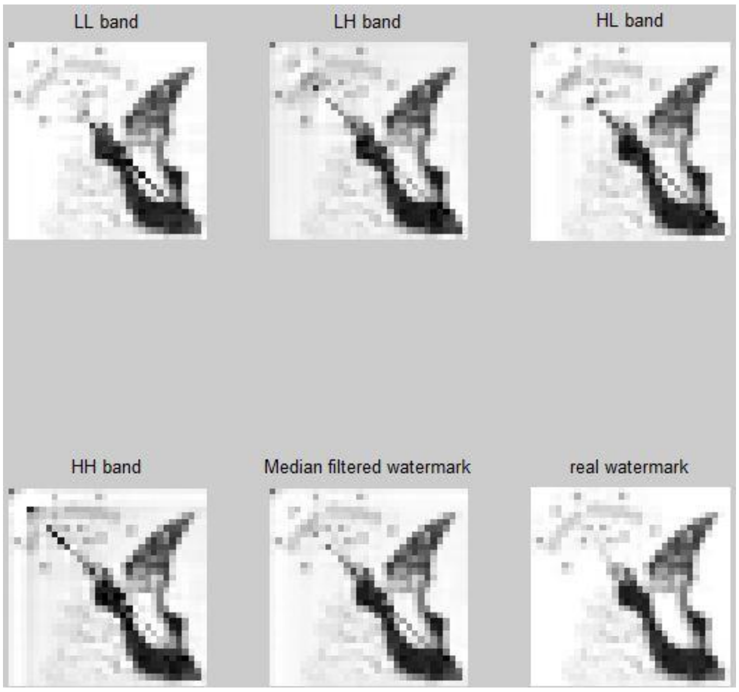


Figure 5.68 Tampered by Gaussian noise at alpha 0.11

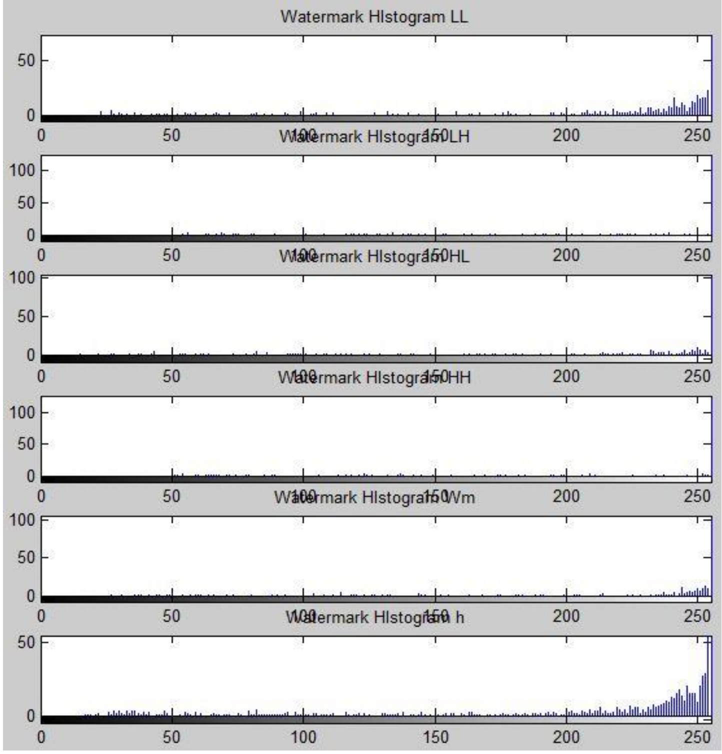


Figure 5.69 Histogram of watermark extracted from various subbands at alpha 0.11

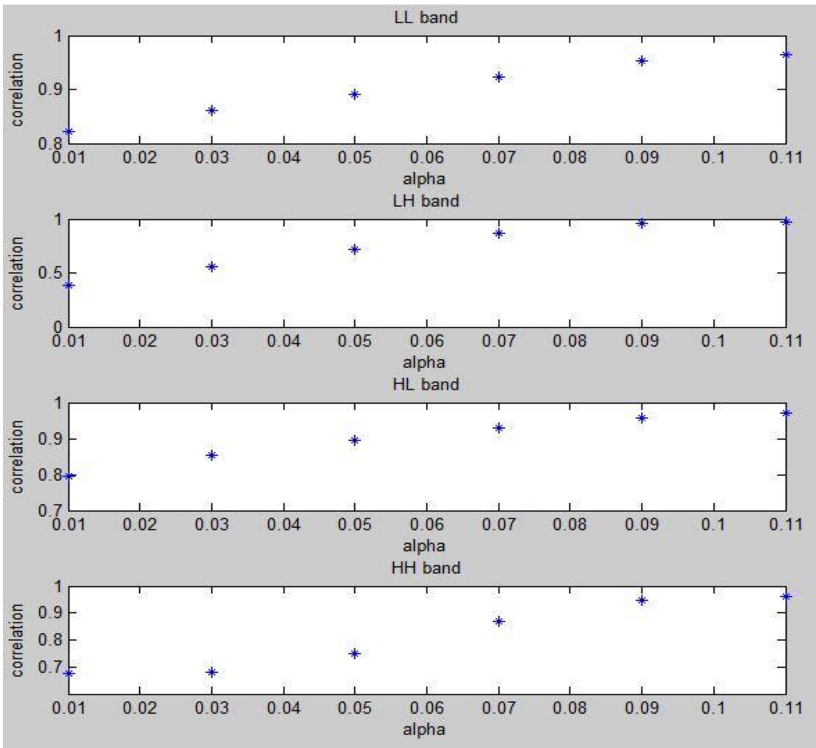


Figure 5.70 Correlation of proposed extracted watermark

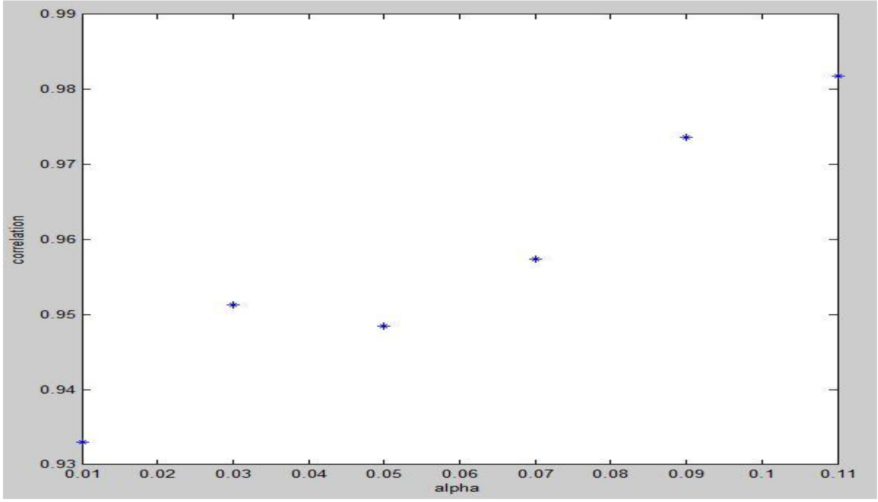


Figure 5.71 Correlation of proposed extracted watermark

Motion Blur

An image created by the camera does not indicate a single instance of time. As a consequence of constraints of technology and inherent requirement of an artistic endeavor, an image invariably represents a scene over a period of time. The time of exposure most often is so short that it tends to give an impression that the image is captured is of instantaneous moment.

Figure 5.72 Host image

Figure 5.73 Tampered by motion blur

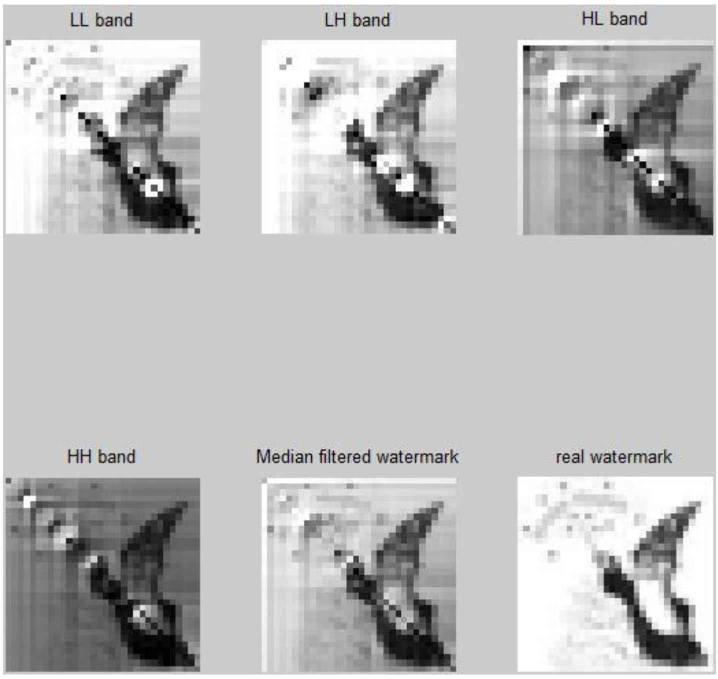


Figure 5.74 Tampered by motion blur at alpha 0.11

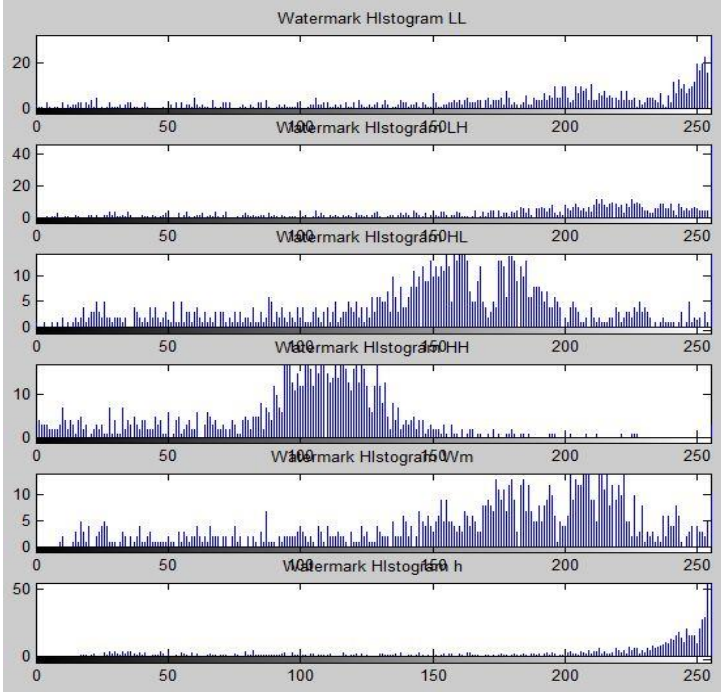


Figure 5.75 Histogram of watermark extracted from various subbands at alpha 0.11

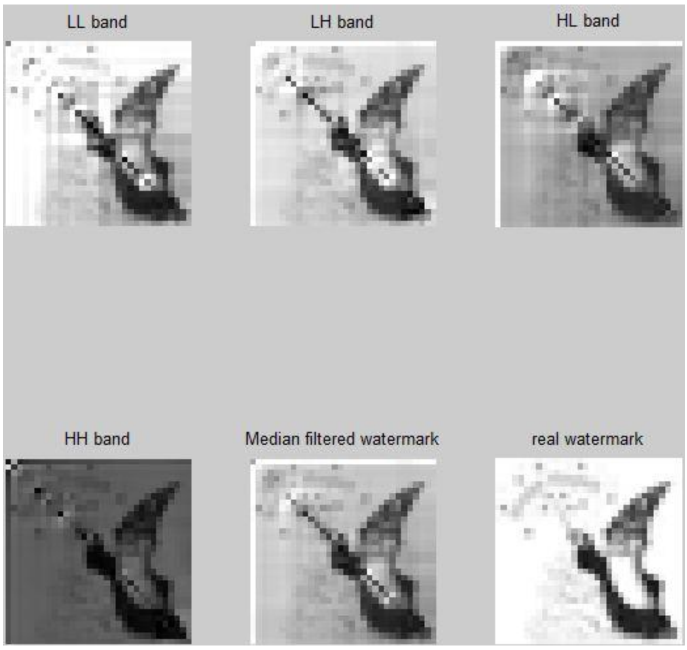


Figure 5.76 Tampered by motion blur at alpha 0.11

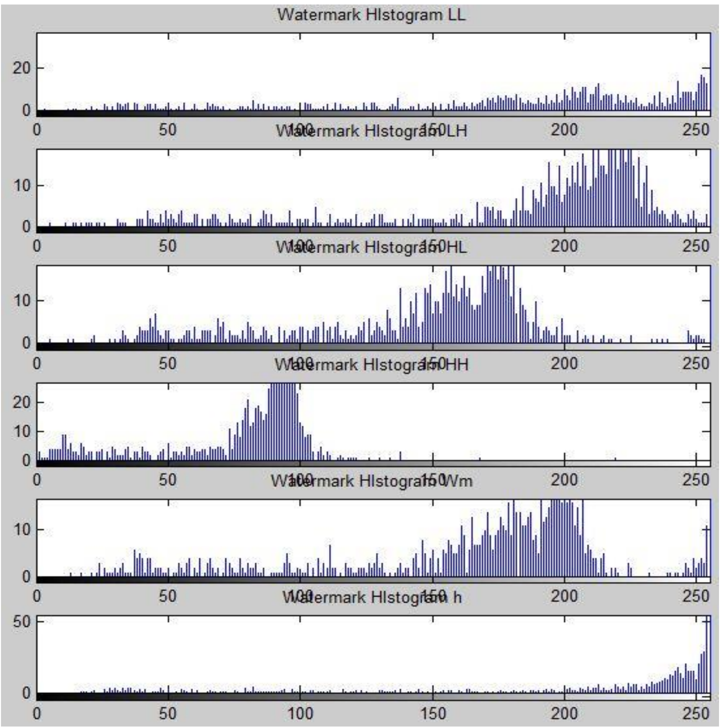


Figure 5.77 Histogram of watermark extracted from various subbands at alpha 0.11

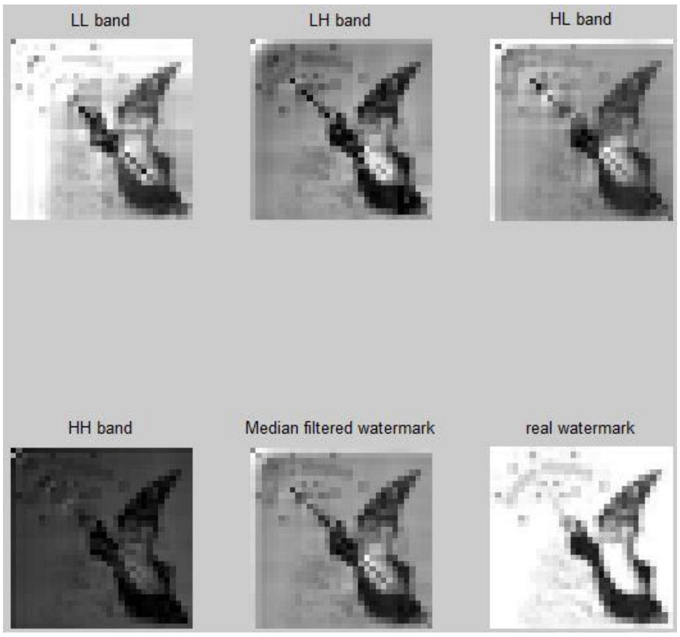


Figure 5.78 Tampered by motion blur at alpha 0.11

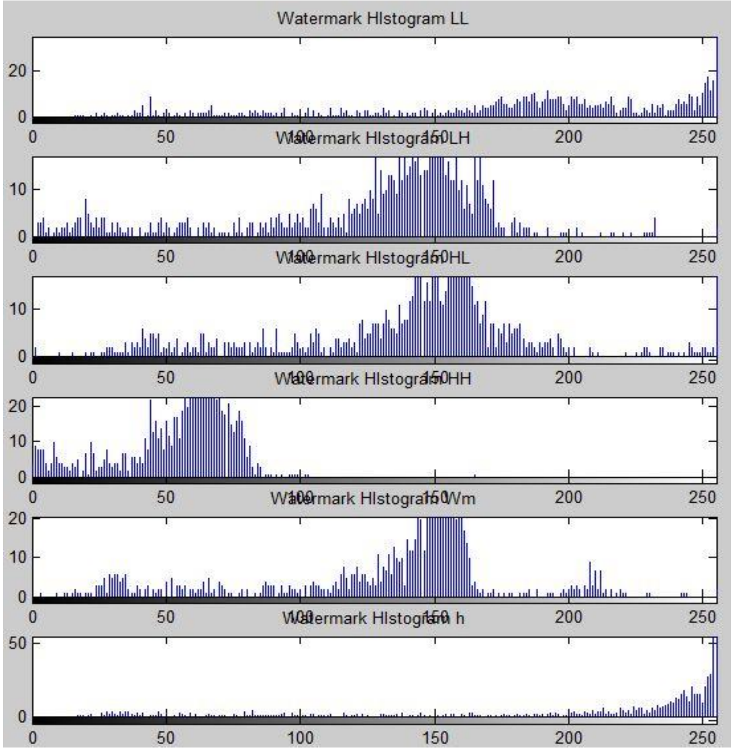


Figure 5.79 Histogram of watermark extracted from various subbands at alpha 0.11

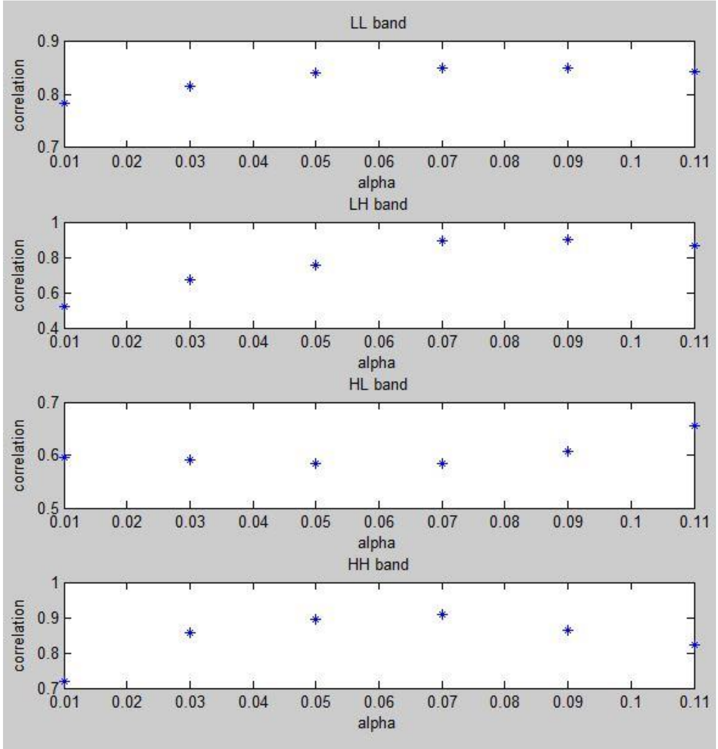


Figure 5.80 Correlation of extracted watermark

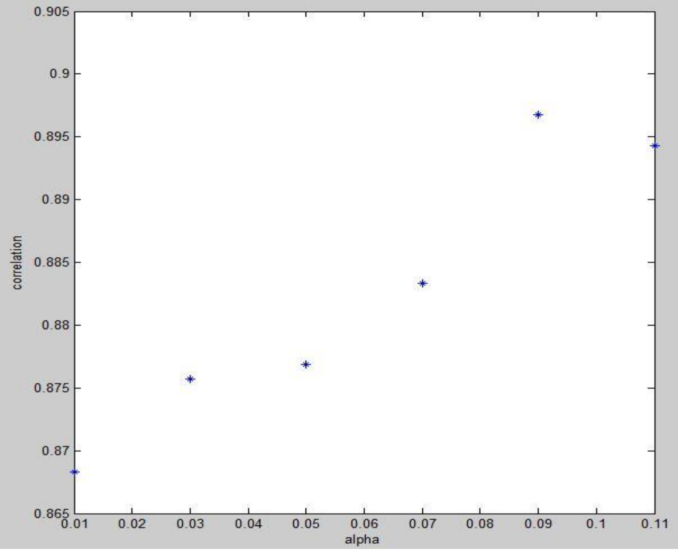


Figure 5.81 Correlation of proposed extracted watermark

Rotation

Rotation Matrix is used to undertake rotation of Euclidean space

$$R = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

For instance, the rotation matrix rotates points in x -y Cartesian plane in a counter clockwise direction through an angle θ about the origin. For performing rotation using the matrix the position of each of the points must be clearly depicted by a coloumn matrix V. the coloumn matrix V contains a coordinates of pixels. The multiplication of R & V gives the rotated vector RV.

Figure 5.82 Host image

Figure 5.83 Tampered by rotation

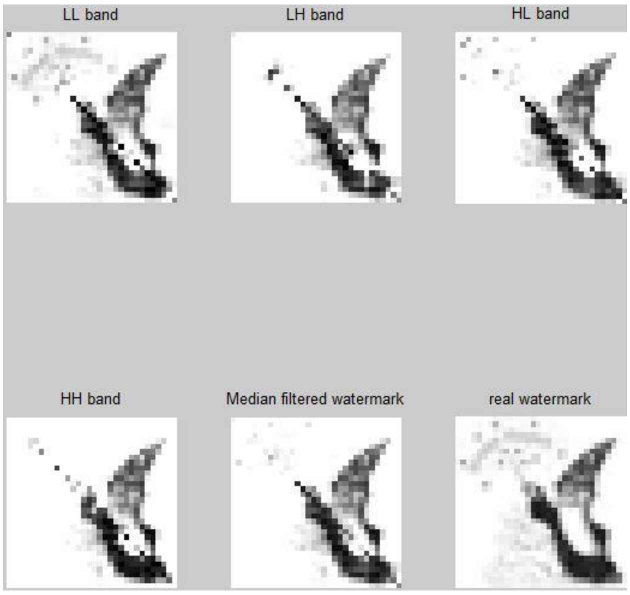


Figure 5.84 Tampered by rotation at alpha 0.01

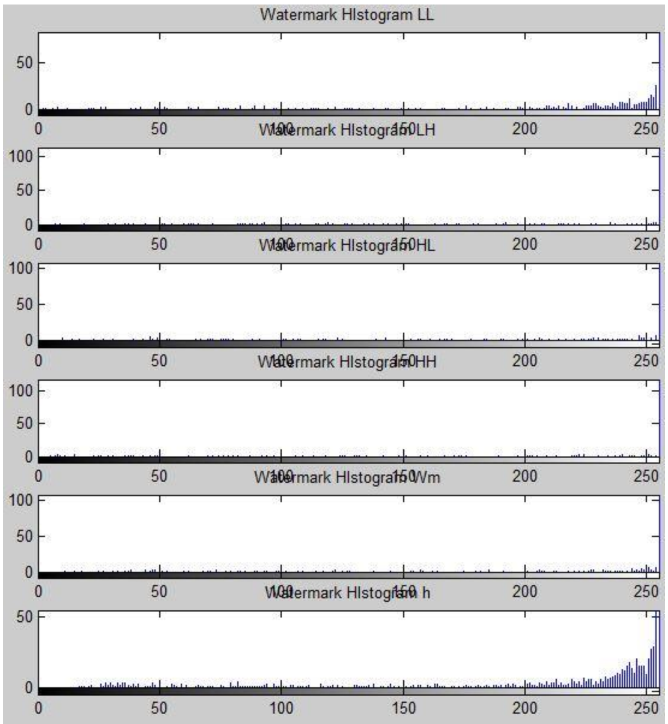


Figure 5.85 Histogram of watermark extracted from various subbands at alpha 0.01

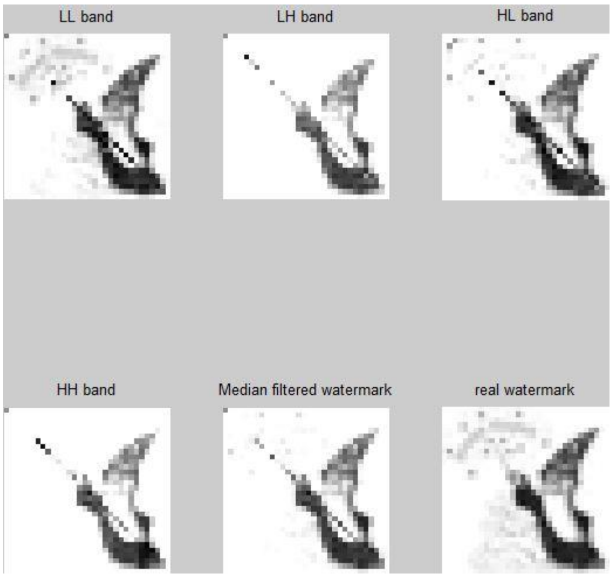


Figure 5.86 Tampered by rotation at alpha 0.06

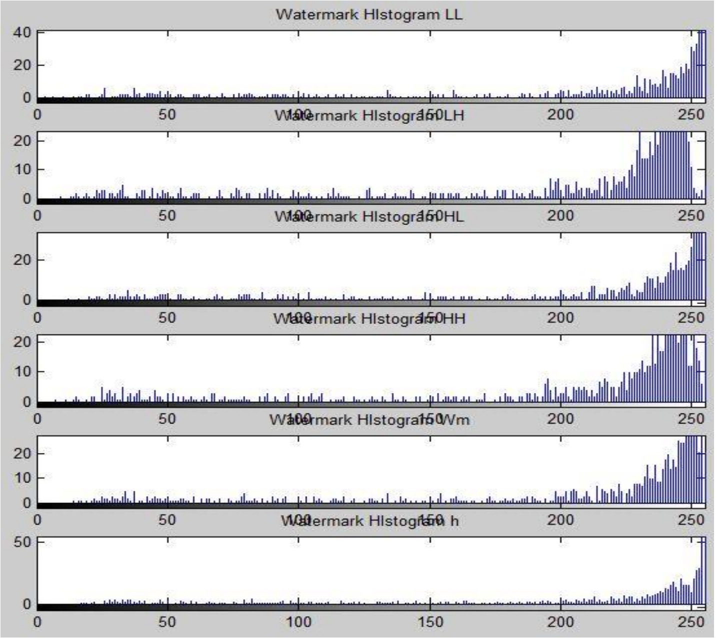


Figure 5.87 Histogram of watermark extracted from various subbands at alpha 0.06

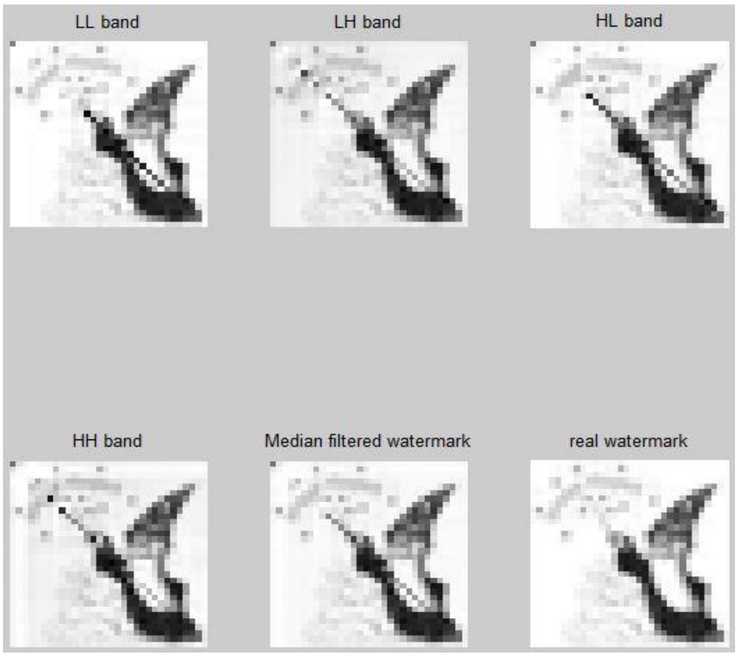


Figure 5.88 Tampered by rotation at alpha   0.11

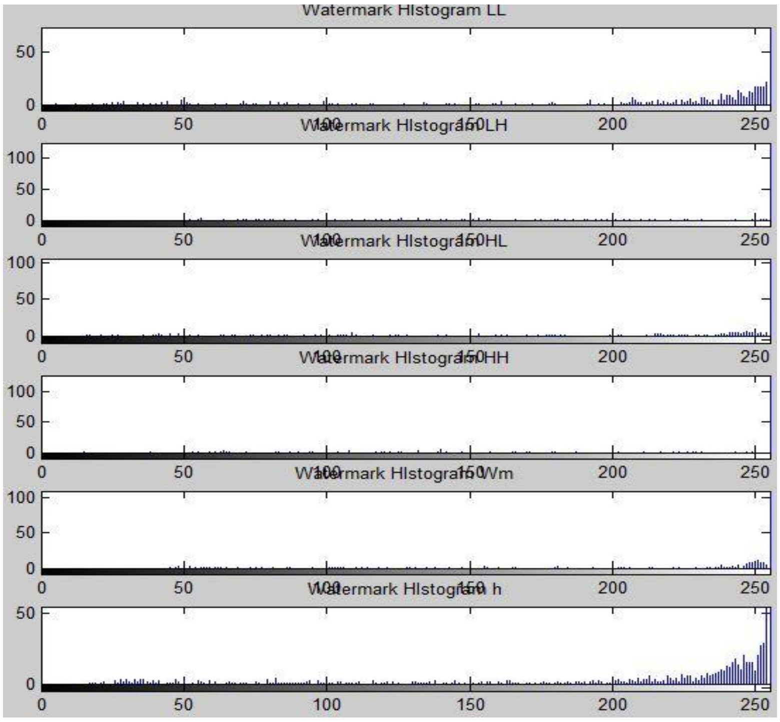


Figure 5.89 Histogram of watermark extracted from various subbands at alpha 0.11

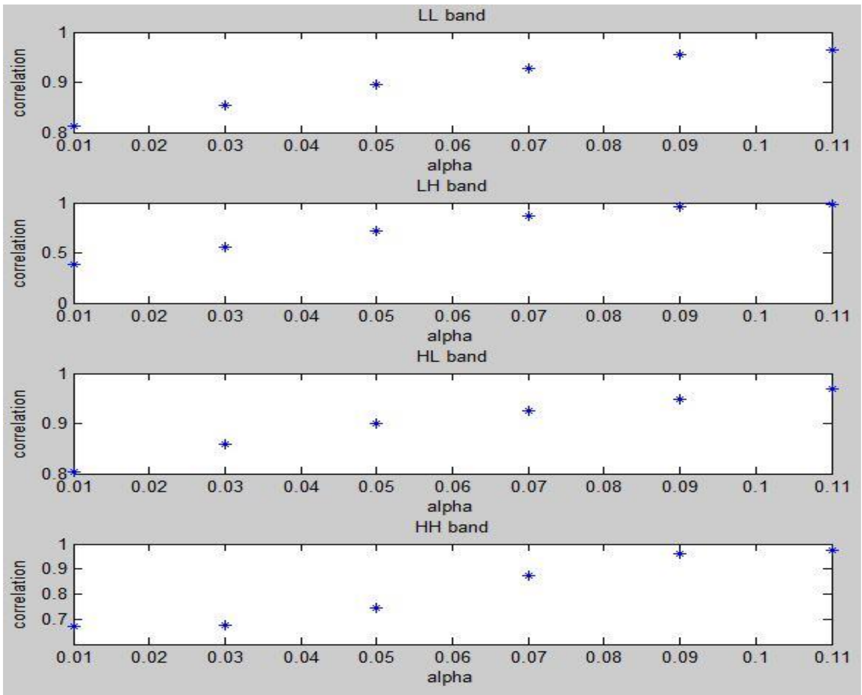


Figure 5.90 Correlation of extracted watermark

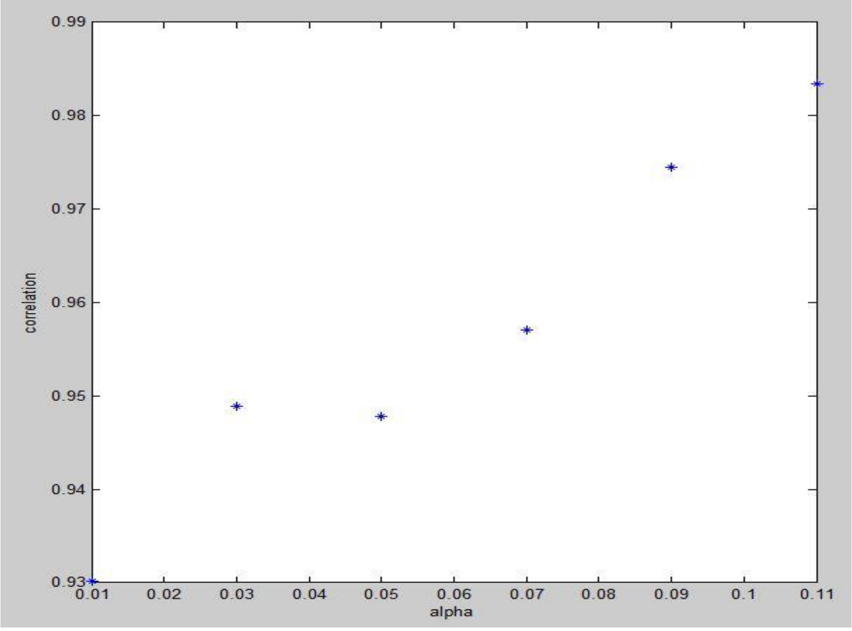


Figure 5.91 Correlation of proposed extracted watermark

Pixel Mosaic

Figure 5.92 Host image

Figure 5.93 Tampered by Pixel Mosaic

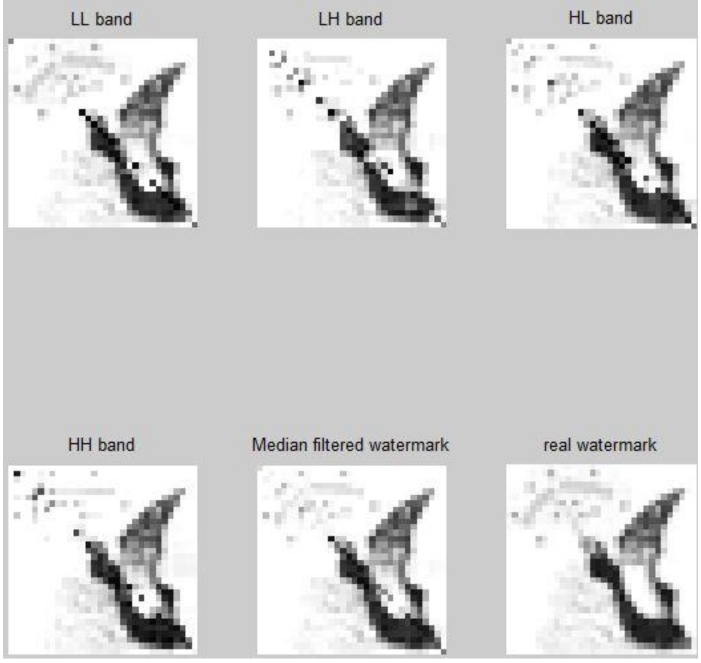


Figure 5.94 Tampered by Pixel mosaic at alpha 0.01

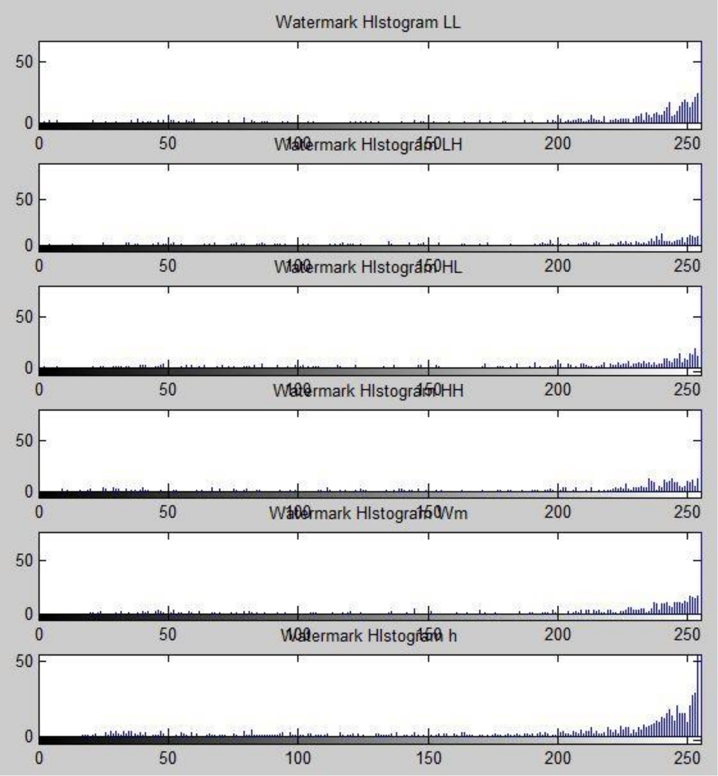


Figure 5.95 Histogram of watermark extracted from various subbands at alpha 0.11

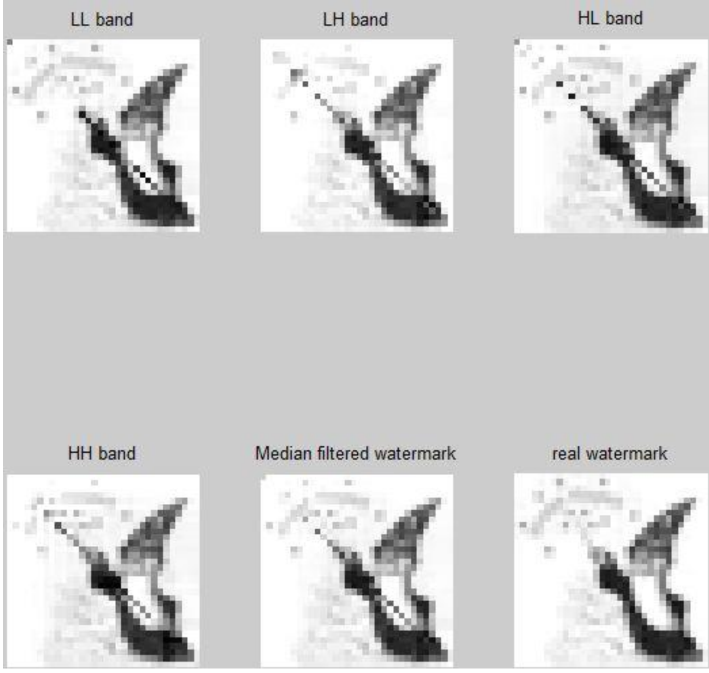


Figure 5.96 Tampered by Pixel mosaic at alpha 0.06

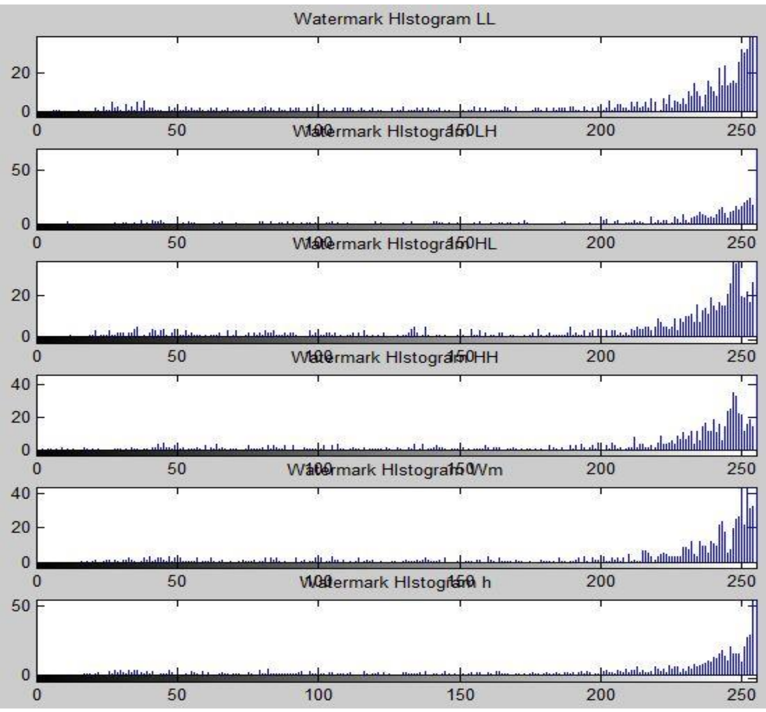


Figure 5.97 Histogram of watermark extracted from various subbands at alpha 0.11

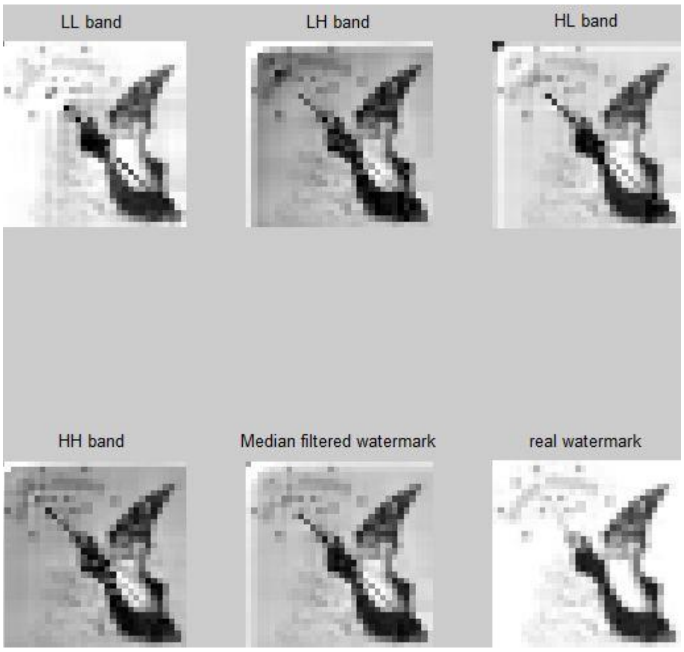


Figure 5.98 Tampered by Pixel mosaic at alpha 0.11

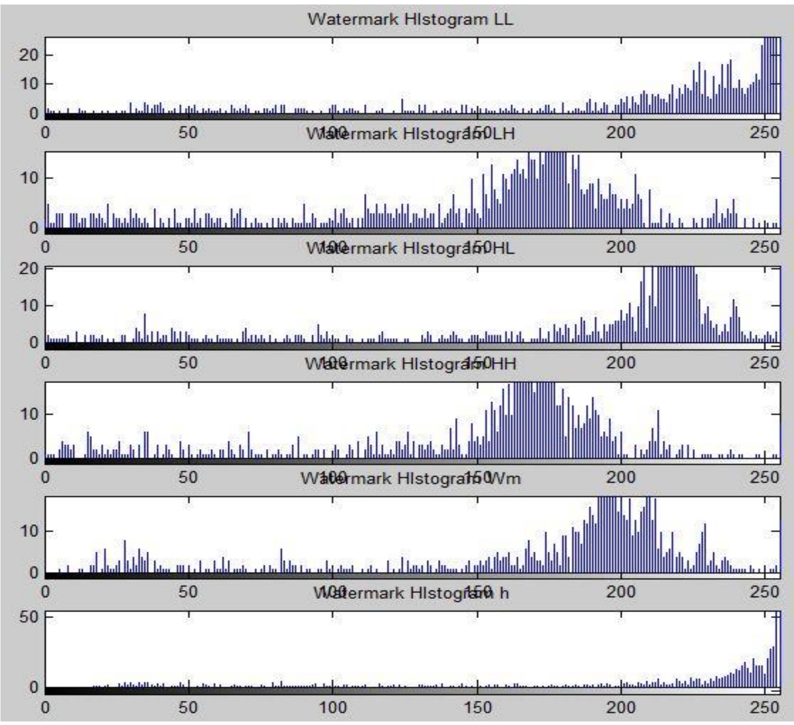


Figure 5.99 Histogram of watermark extracted from various subbands at alpha 0.11

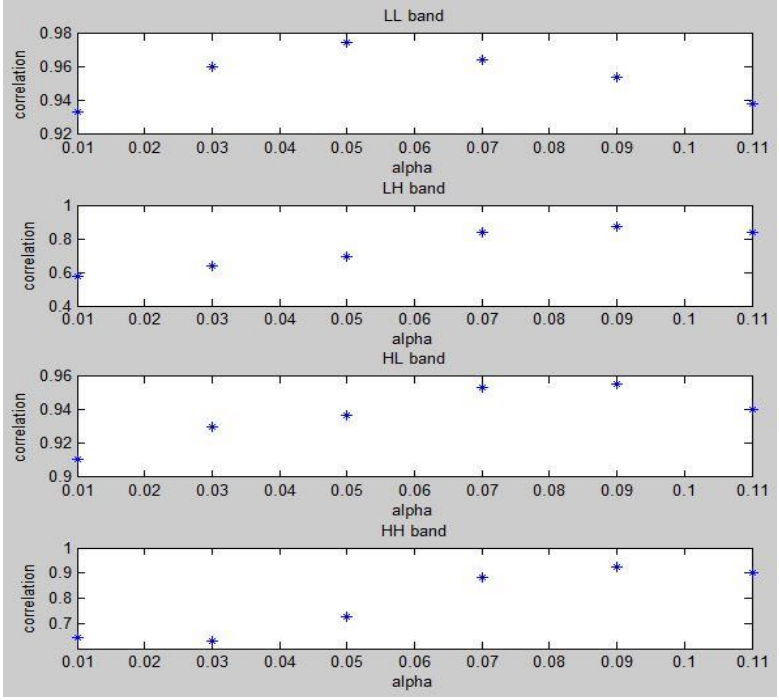


Figure 5.100 Correlation of extracted watermark

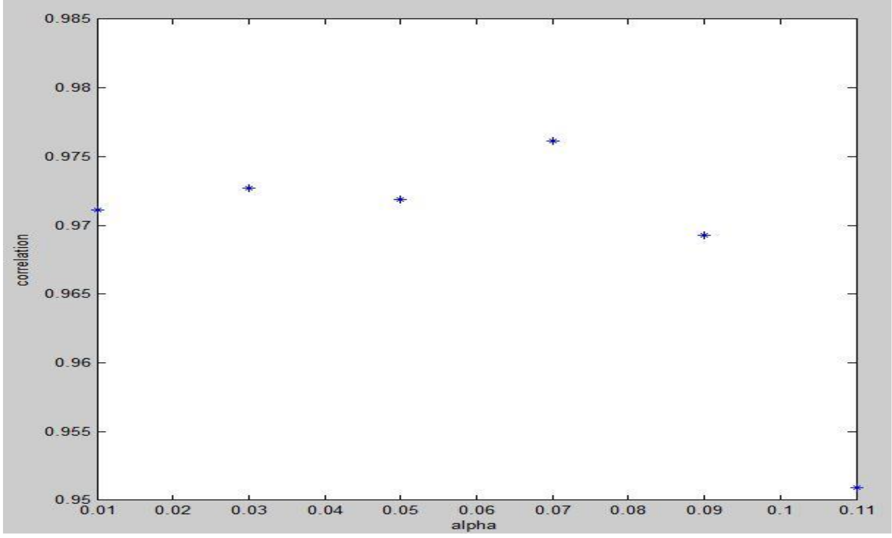


Figure 5.101 Correlation of proposed extracted watermark

Contrast adjustment

To enable an object to be distinguishable, the contrast adjustment is resorted to. It is the difference in luminance and/or color referred to as contrast that makes an object (or its representation in an image or display) distinguishable. In visual perception of the real world, The contrast, in visual perception of the real world is given by the difference in the color and brightness of the object and other objects within the same field of view. Since the human visual system is more sensitive to contrast than the absolute luminance, we can perceive the world similarly regardless of the noticeable changes in illumination over the day or from place to place.

Figure 5.102 Host image

Figure 5.103 Tampered by Contrast adjustment

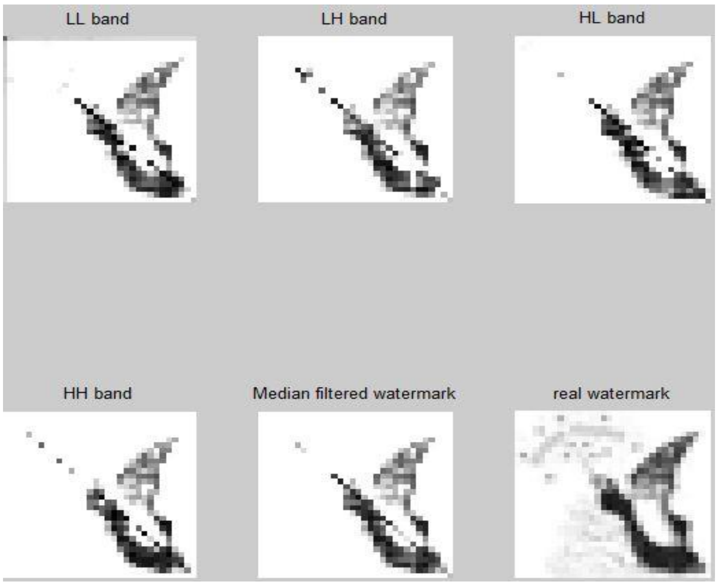


Figure 5.104 Tampered by Contrast adjustment at alpha 0.01

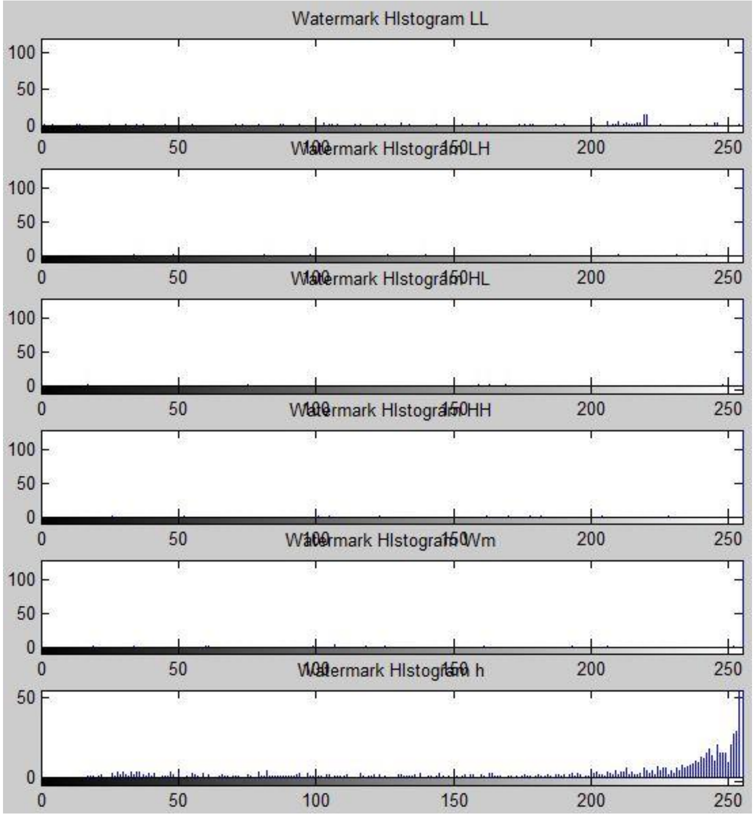


Figure 5.105 Histogram of watermark extracted from various subbands at alpha 0.01

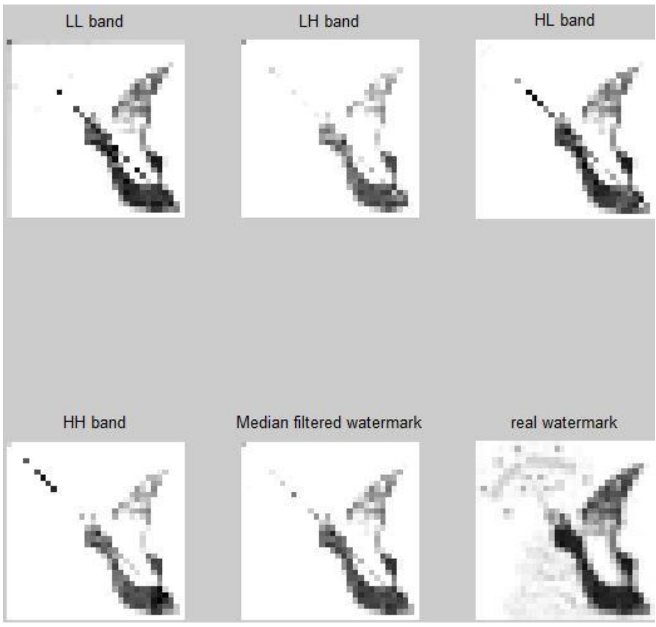


Figure 5.106 Tampered by Contrast adjustment at alpha 0.06

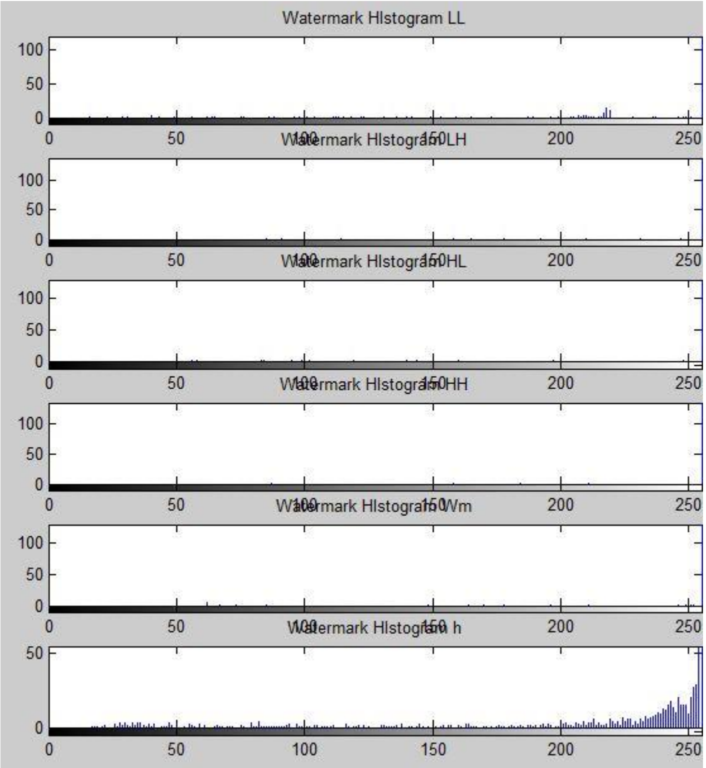


Figure 5.107 Histogram of watermark extracted from various subbands at alpha 0.06

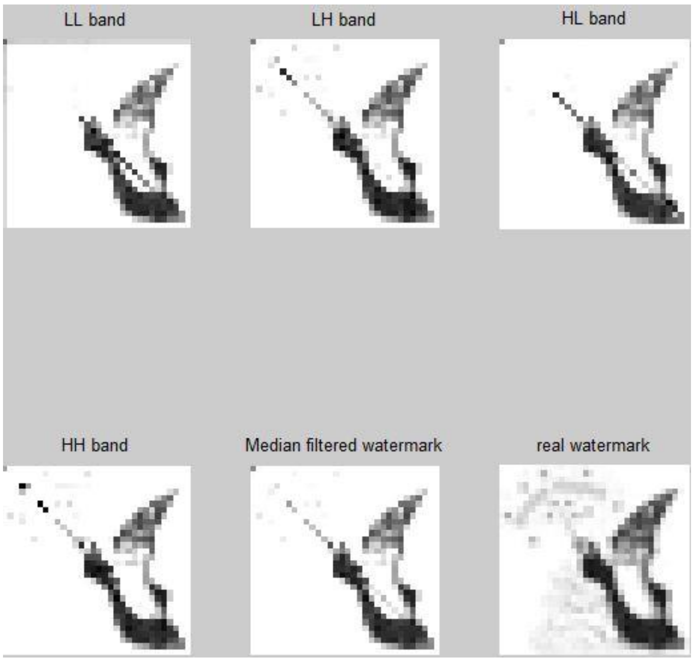


Figure 5.108 Tampered by Contrast adjustment at alpha 0.11

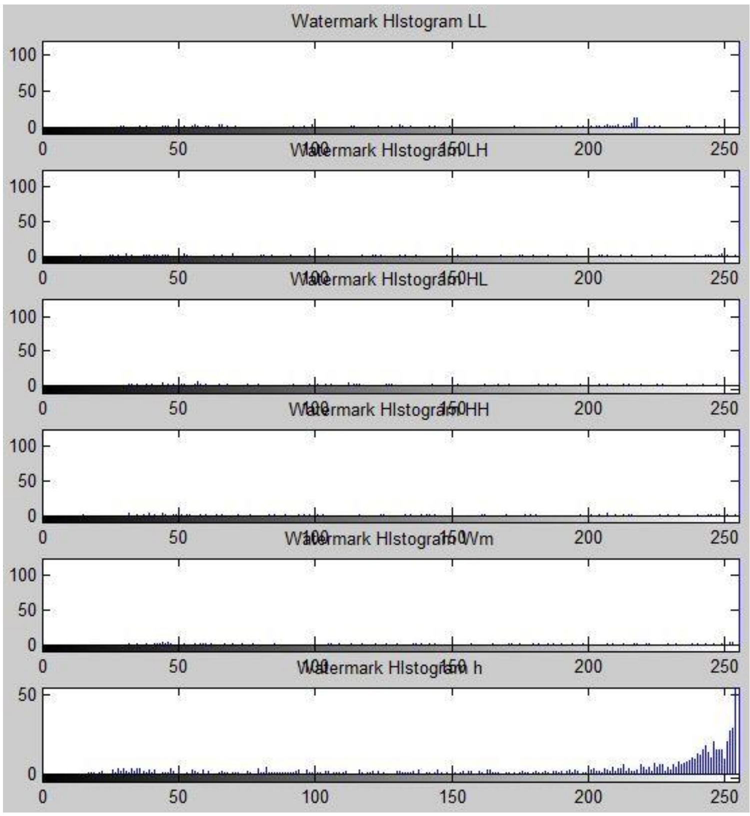


Figure 5.109 Histogram of watermark extracted from various subbands at alpha 0.11

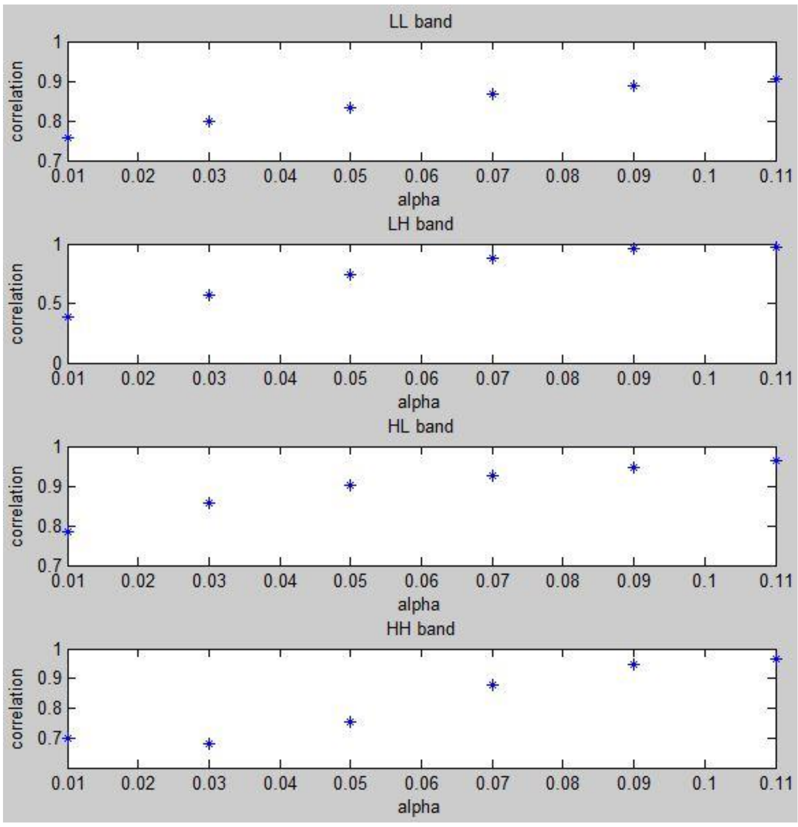


Figure 5.110 Correlation of extracted watermark

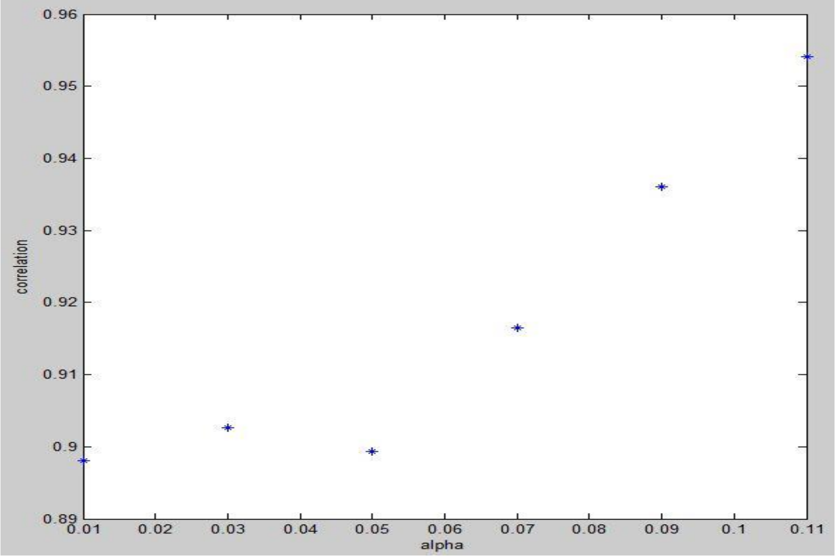


Figure 5.111 Correlation of proposed extracted watermark

Multiple attacks

Figure 5.112 Host image

Figure 5.113 Tampered by Multiple attacks

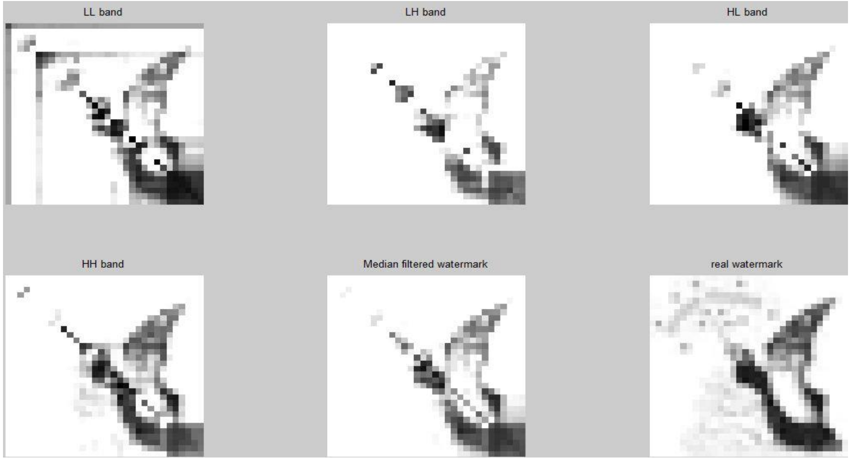


Figure 5.114 Tampered by multiple attacks at alpha 0.01

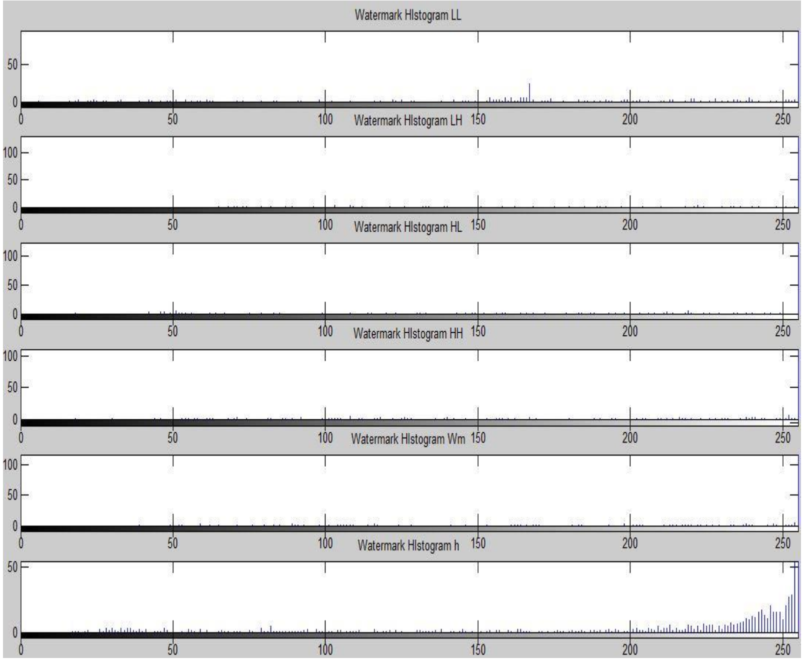


Figure 5.115 Histogram of watermark extracted from various subbands at alpha 0.01

Figure 5.116 Tampered by multiple attacks at alpha 0.06 at alpha 0.01

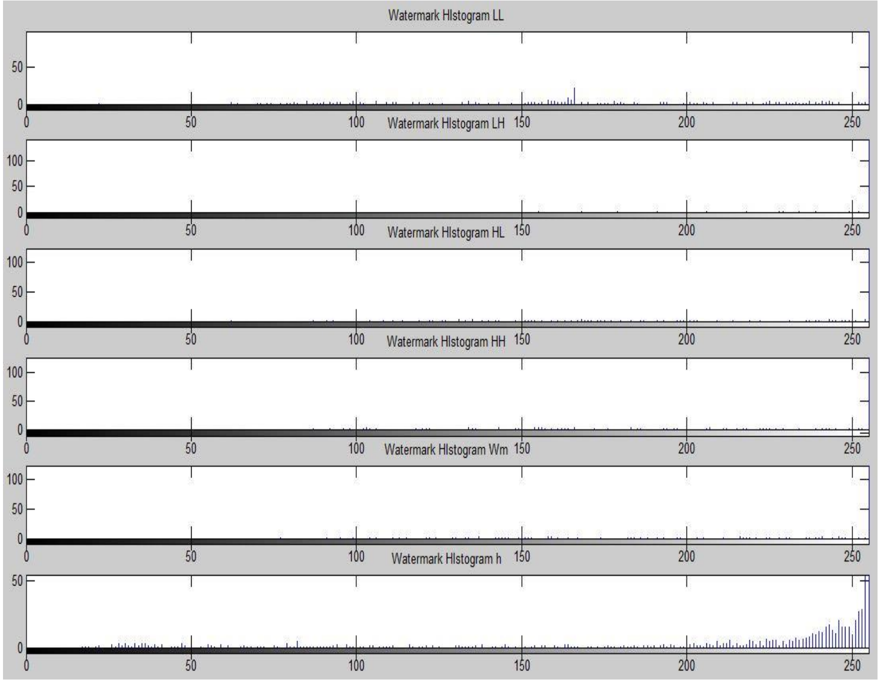


Figure 5.117 Histogram of watermark extracted from various subbands at alpha 0.06

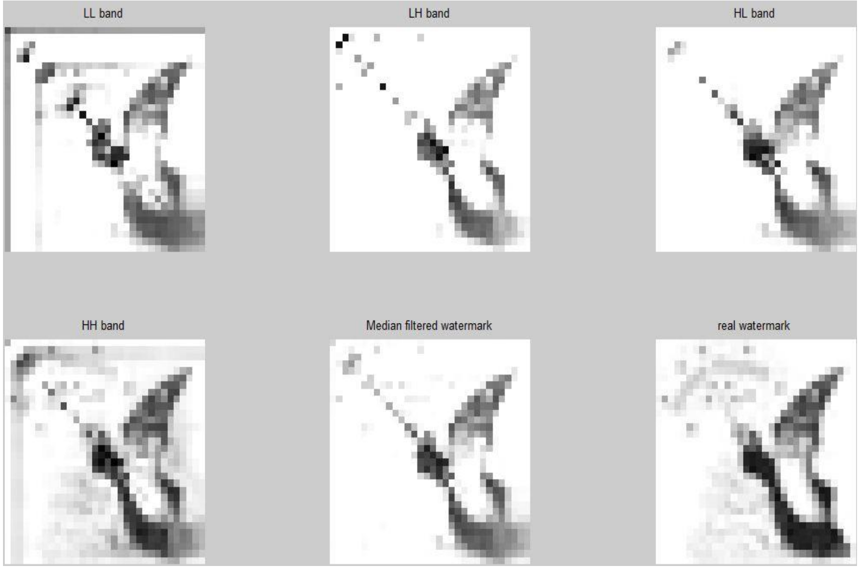


Figure 5.118 Tampered by multiple attacks at alpha 0.11 at alpha 0.01

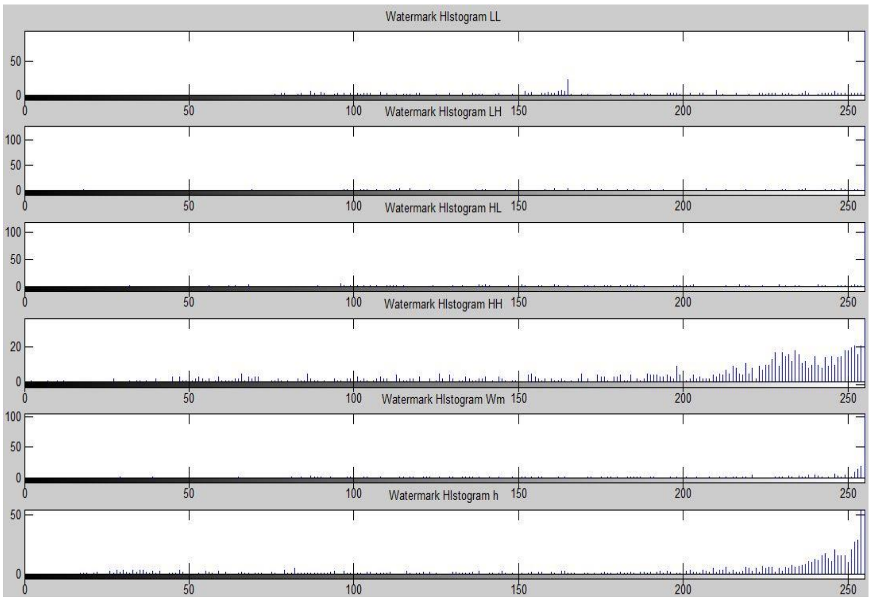


Figure 5.119 Histogram of watermark extracted from various subbands at alpha 0.11

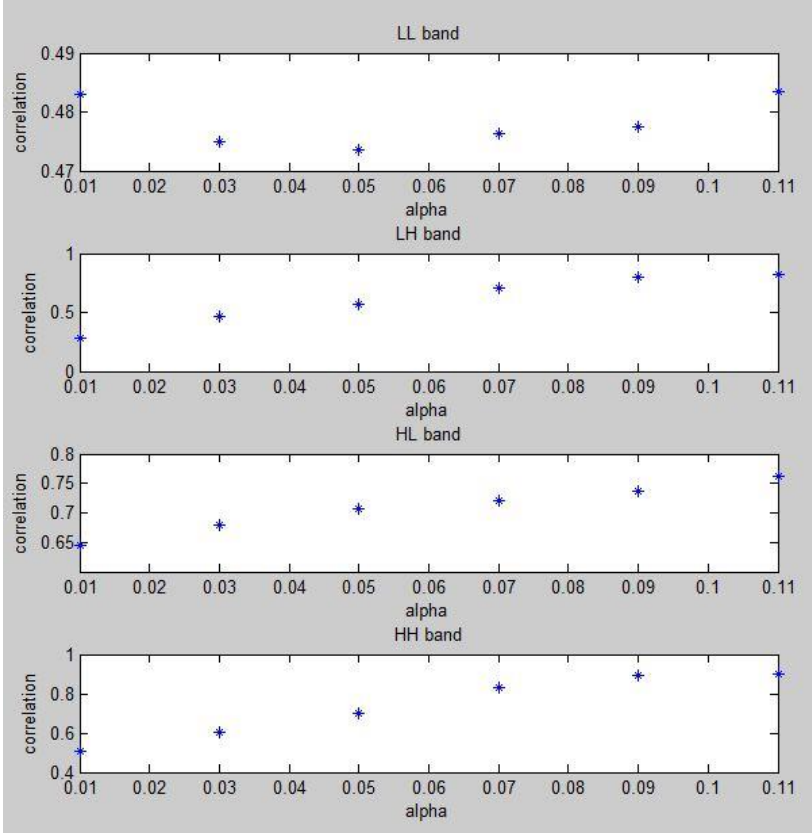
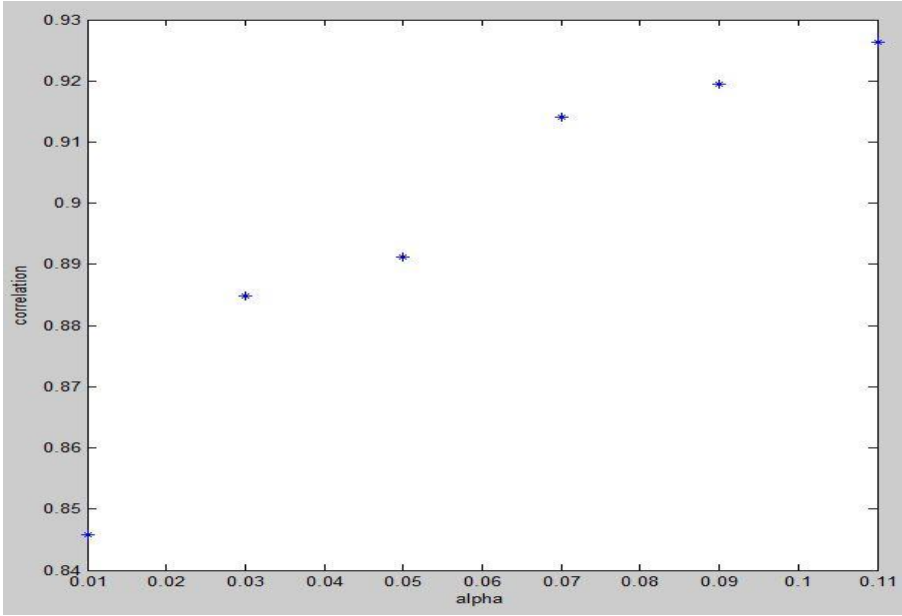


Figure 5.120 Correlation of extracted watermark



<u>Figure 5.121 Correlation of proposed extracted watermark</u>

Chapter 6

6.1 Performance evaluation of watermarking algorithms

Performance evaluation is very important part in the any algorithmic designing watermarking. The main task of this is to evaluate the quality matrices of algorithm or method to find out, how much he is effective? Some of the quality matrices an image watermarking method or algorithm.

6.2 Mean square error (MSE)

The mean squared error (MSE) in an image watermarking is to estimate or measures the average of the squares of the “errors", between host image and watermark image

$$MSE = 1 \div MN \sum_{i}^{M} \sum_{j}^{N} \left(Wij - Hij\right)^2$$

Where M, N is pixel values in host image
Wij= Pixel value in Watermarked Image
Hij= Pixel value in Host Image

Peak signal to noise ratio (PSNR)

PSNR (Peak Signal to Noise Ratio) is used to determine the Efficiency of Watermarking with respect to the noise. The noise will degrade the quality of image. The visual quality of watermarked and

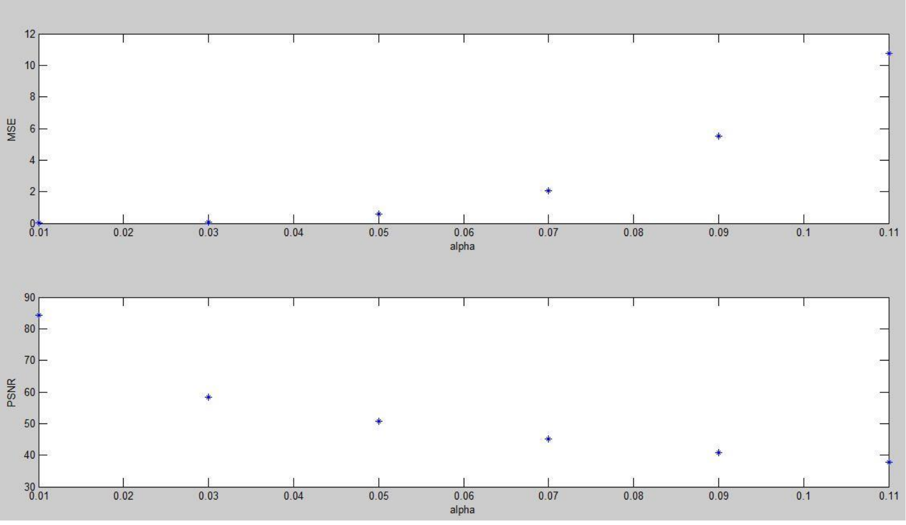


Figure 6.1 Host Image MSE of water mark extracted at alpha various alpha

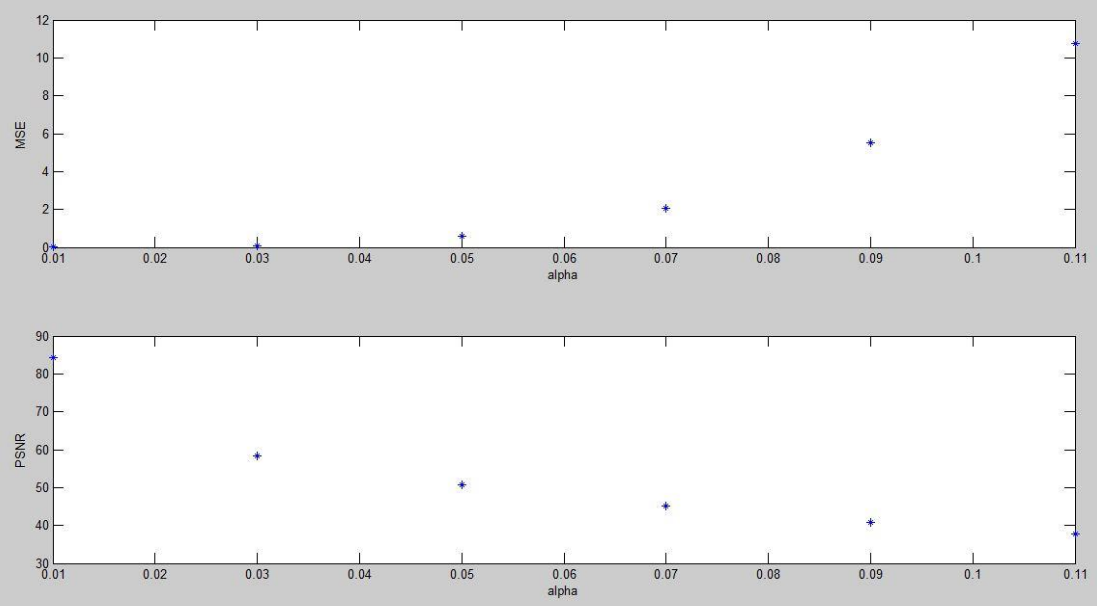


Figure 6.2 Host Image MSE of water mark extracted and filtered using median filter at alpha various alpha

6.3 Attacked images are measured using the Peak Signal to Noise Ratio.

The visual quality metrics are made use of as a measure of distortions introduced by the watermarking process. It must be noted that it is distinguishable by visual quality of the data on account of embedding of the watermark and the visual quality of the watermarked data as a result of the attacks performed on it. It must be appreciated that the visual quality of the watermarked data is required to be as high as possible. This aspect means that the degradation of the data due to the watermarking operation is hardly noticeable.

Peak Signal to Noise Ratio (PSNR), defined as:

$$\mathrm{PSNR}(dB) = 10\log_{10}\left(N_1 N_2 \frac{\max\limits_{x_1,x_2} \mathbf{I}^2{}_{x_1,x_2}}{\sum\limits_{x_1,x_2} (\mathbf{I}_{x_1,x_2} - \mathbf{I}_{\mathrm{W}x_1,x_2})^2}\right)$$

Where N1 andN2 are dimensions of the original image I and watermarked image

$x_1 = 1,\ldots,N_1,\ x_2 = 1,\ldots,N_2$

The PSNR shows that Watermarked image is perceptible or watermark is not recognized by naked eyes.

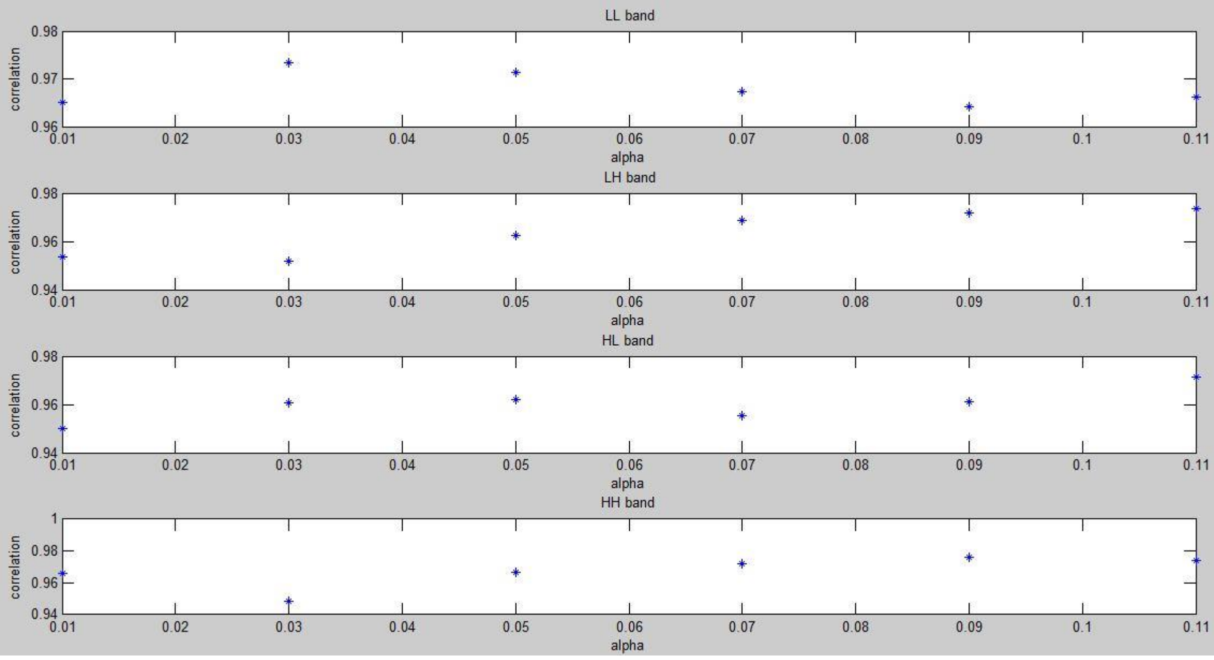


Figure 6.3 Host Image PSNR of water mark extracted at alpha various alpha

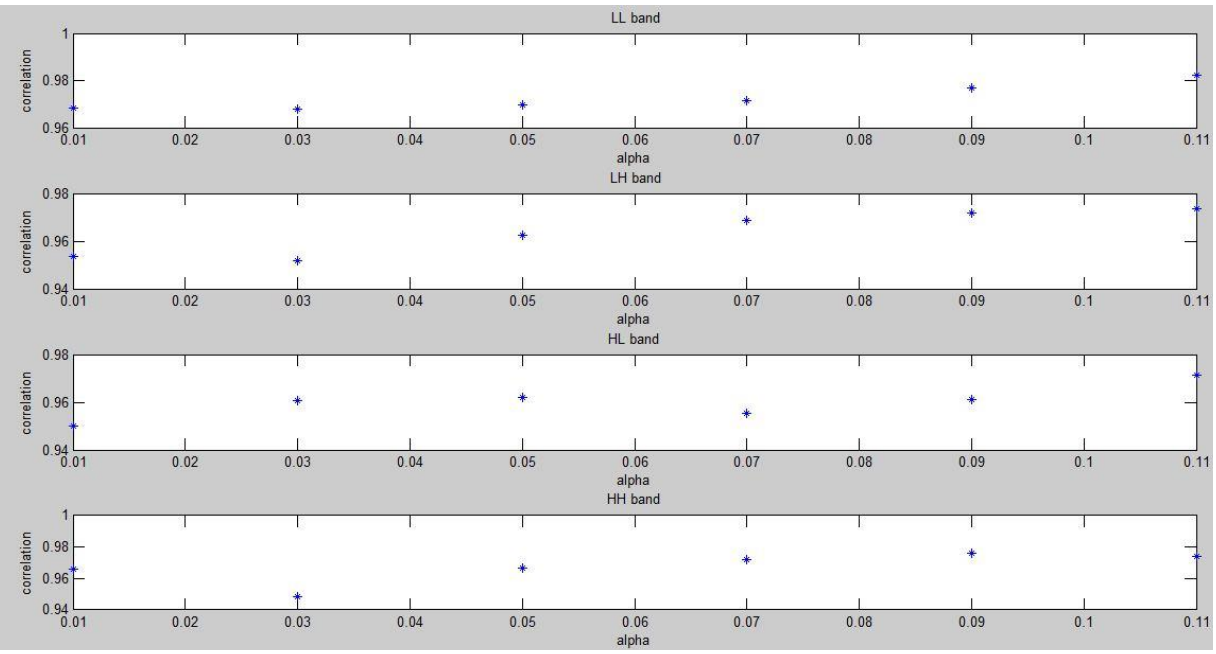


Figure 6.4 Host Image PSNR of water mark extracted and filtered using median filter at alpha various alpha

Table: 6.1

MULTIPLE ATTACK CORRELATION[[[[					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.483	0.285	0.644	0.509	0.846
0.03	0.475	0.467	0.678	0.601	0.885
0.05	0.474	0.573	0.708	0.702	0.891
0.07	0.476	0.706	0.721	0.834	0.914
0.09	0.478	0.797	0.737	0.894	0.92
0.11	0.483	0.827	0.763	0.898	0.926

Table: 6.2

HISTOGRAM EQUALIZATION CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.698	0.524	0.74	0.741	0.914
0.03	0.699	0.79	0.781	0.853	0.917
0.05	0.695	0.865	0.832	0.907	0.921
0.07	0.698	0.775	0.855	0.879	0.914
0.09	0.7	0.692	0.872	0.788	0.88
0.11	0.705	0.626	0.855	0.71	0.846

Table: 6.3

AVERAGE FUNCTION CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.858	0.361	0.714	0.681	0.959
0.03	0.9	0.435	0.701	0.788	0.966
0.05	0.938	0.493	0.685	0.869	0.967
0.07	0.961	0.614	0.712	0.94	0.971
0.09	0.952	0.692	0.764	0.938	0.967
0.11	0.947	0.733	0.814	0.912	0.963

Table: 6.4

CROP CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.512	0.314	0.581	0.58	0.844
0.03	0.522	0.372	0.638	0.553	0.901
0.05	0.545	0.419	0.714	0.604	0.909
0.07	0.561	0.503	0.769	0.733	0.922
0.09	0.574	0.557	0.823	0.829	0.935
0.11	0.591	0.579	0.862	0.863	0.937

Table: 6.5

RESIZE CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.827	0.314	0.821	0.645	0.936
0.03	0.871	0.372	0.871	0.719	0.959
0.05	0.911	0.419	0.896	0.797	0.964
0.07	0.934	0.503	0.925	0.903	0.965
0.09	0.957	0.557	0.956	0.959	0.979
0.11	0.963	0.579	0.969	0.965	0.981

Table: 6.6

GAUSSIAN NOISE CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.822	0.389	0.796	0.678	0.933
0.03	0.861	0.562	0.855	0.679	0.951
0.05	0.891	0.719	0.895	0.747	0.948
0.07	0.922	0.865	0.93	0.871	0.957
0.09	0.953	0.956	0.956	0.948	0.974
0.11	0.965	0.975	0.972	0.961	0.982

Table: 6.7

MOTION BLUR CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.784	0.519	0.594	0.718	0.868
0.03	0.816	0.671	0.59	0.856	0.876
0.05	0.841	0.759	0.584	0.896	0.877
0.07	0.85	0.892	0.584	0.908	0.883
0.09	0.852	0.902	0.607	0.864	0.897
0.11	0.844	0.866	0.655	0.822	0.894

Table: 6.8

MOTION BLUR CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.784	0.519	0.594	0.718	0.868
0.03	0.816	0.671	0.59	0.856	0.876
0.05	0.841	0.759	0.584	0.896	0.877
0.07	0.85	0.892	0.584	0.908	0.883
0.09	0.852	0.902	0.607	0.864	0.897
0.11	0.844	0.866	0.655	0.822	0.894

Table: 6.9

ROTATION CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.813	0.389	0.803	0.673	0.93
0.03	0.855	0.563	0.86	0.677	0.949
0.05	0.896	0.723	0.901	0.743	0.948
0.07	0.928	0.87	0.926	0.874	0.957
0.09	0.955	0.96	0.949	0.959	0.975
0.11	0.965	0.981	0.97	0.977	0.983

Table: 6.10

PIXEL MOSAIC CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subbands
0.01	0.934	0.574	0.911	0.645	0.971
0.03	0.96	0.641	0.93	0.629	0.973
0.05	0.975	0.691	0.937	0.727	0.972
0.07	0.964	0.835	0.954	0.881	0.976
0.09	0.954	0.871	0.955	0.924	0.969
0.11	0.938	0.837	0.94	0.901	0.951

Table: 6.11

CONTRAST ADJUSTMENT CORRELATION					
ALPHA	LL	LH	HL	HH	Filtered Watermark From All Subband
0.01	0.758	0.39	0.784	0.7	0.898
0.03	0.797	0.569	0.857	0.681	0.903
0.05	0.833	0.739	0.901	0.754	0.899
0.07	0.866	0.882	0.926	0.878	0.917
0.09	0.888	0.958	0.948	0.946	0.936
0.11	0.904	0.969	0.965	0.965	0.954

Chapter 7

7.1 Conclusion

The concept of robust watermarking is primarily based on geometric invariant domain which is constructed using DWT and SVD algorithm with median filter. Copyright protection is provided by extracted watermark. To the best knowledge this is of first kind of increment in robustness of watermark.

Two chief aspects that need to be enhanced are the visual quality of stage image and the effectiveness of content recovery. The diagonal effect caused by SVD is reduced by application median filter application. Embedding watermark in all sub bands of DWT increase in robustness of watermark.

As the watermark is implemented in four subbands. The multiple attacks reduce watermark correlation.

If the value of alpha parameter increased then PSNR of host image get reduces. The quality of watermarked get reduced. To makes good PSNR (peak signal to noise ratio) of watermarked image the alpha parameter is fixed with low value. The low value of alpha reduces watermark's robustness.

It is shown that watermark is extracted at various attacks from various band. Have low correlation. Based on this correlation It creates difficulty in automated decision.

Thus the applications of median filter make it more robust and make good correlation of watermark.

7.2 Chapter Summary

Robust watermark suited for copy right protection purpose given their contrasting effect. It is most suitable for copy right protection due to the robustness of watermark. The watermarks embed in all subbands and median filter application makes watermark more robust. The graphical analysis is shown for different value of alpha (transparency). The comparative analysis is shown in graph by correlation and PSNR values.

Chapter 8

8.1 The Need for Watermarking

The amount of digital content consumption has increased tremendously owing to economical mass storage and increasing file transfer speeds. Digital media can be copied, modified, and distributed easily. The introduction of HP Memory Spot Chip increased the importance of content integrity because C of the increased availability of digital content through conventional channel. Recently, a war zone image was doctored to increase the thickness of smoke as a means to magnify conflict situations. These factors have increased research in digital media security. Confidentiality and integrity can be provided to digital media using cryptography. The decrypted media can further be protected using stenography. One such method is digital watermarking. Digital watermarks provide protection to decrypted media so that illegal use of modification may be avoided or deducted. Digital watermarking is a field that has been seen as a potent area of research over the past decades.

The aim of this research will be :-

(a) To analyze the strength and limitation of water marking schemes is use today.

(b) To design and develop improved scheme so as to overcome the limitations

(c) To evaluate the new schemes using various scenarios of application.

Robust watermarks owing to its resistance against media manipulation are the proposed technique used to protect the copyright of the owner. Using the fundamental geometrical operation of RST, improved robust watermarking methods was made within approaches. The first approach enabled successful watermark detection by resynchronizing the watermark data. The approach was a geometric invariant domain for robust watermarking. The watermark that was extracted in the deduction process provides information that would be valuable for Media Forensics. Since, it can detect behind watermarks, this is a very practical method.

References

[1] Yang Zhao, Patrizio Campisi, Member, IEEE, and Deepa Kundur, Senior Member, IEEE “DualDomain Watermarking for Authentication and Compression of Cultural Heritage Images” ,IEEE Transactions On Image Processing, VOL. 13, NO. 3, MARCH 2004.

[2] WANG WEI, WANG Rang-ding,Dept. of ckc Ningbo University Ningbo zhejiang 315211, China “The Analysis and Detection of Double JPEG 2000Compression Based on Statistical Characterization DWT Coefficients” 2012 International Conference on Future Electrical Power and Energy Systems.

[3] Suresh N. Mali∗, Pradeep M. Patil, Rajesh M. Jalnekar “Robust and secured image-adaptive data hiding”Vishwakarma Institute of Technology, Pune, (MS), India.

[4] P Karthigaikumara, Anumolb, K Baskaranc, a* “FPGA Implementation of High Speed Low AreaDWT Based Invisible Image Watermarking Algorithm”Department of Computer Science andEngineering, Government College of Technology, Coimbatore-641 013, India.

[5] Roberto Caldellia, Francesco Filippinia, Mauro Barnib “Joint near –lossless compression and watermarking of still image for authentication and tamper localization”Department of Electronics and Telecommunications, University of Florence, Via di Santa Marta, 3, 50139 Florence, Italy.

[6] Osama S. Faragallah “Efficient video watermarking based on singular value decompositionIn the discrete wavelet transform domain” Dept. of Computer Science &Engineering,FacultyOf Electronic Engineering, Minufiya University, Menouf 32952, Egypt.

[7] M. Jethloja, A. K.Kalariya, Abhishek Chobey“Performance Analysis of Digital ImageWatermarking Using Combined DWT – DCT”International Journal of Electronics, Communication& Soft Computing Science and Engineering (IJECSCSE) Volume 1,Issue 1

[8] Baisa L. Gunjal Department of Computer Engineering, Amrutvahini College of Engineering,“An Overview Of Transform Domain Robust Digital Image Watermarking AlgorithmsJournal of Emerging Trends in Computing and Information Sciences
Volume 2 No. 1, ISSN 2079-8407

[9] Ali Al-Haj, “CombinedDWT-DCT Digital Image Watermarking” Journal of Computer Science 3(9):740-746, 2007

[10] M.Mohemad Sathik, S.S Sujatha“A Novel Dwt based Invisible Watermarking

Technique forDigital images” International Arab journal of e-Technology, Vol2, No.3, January 2012.

[11] Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, “SVD-based digital image watermarking scheme”, Pattern Recognition Letters, Volume 26, Issue 10, July 2005, pp. 1577-1586.

[12] D. V. S. Chandra, “Digital Image Watermarking Using Singular Value Decomposition,” Proceedingsof 45th IEEE Midwest Symposium on Circuits and Systems, Tulsa, OK, August 2002, pp. 264-267.

[13] R. Mehul and R. Priti, “Discrete Wavelet Transform Based Multiple Watermarking Scheme,” Proceedings of IEEE Region 10 Technical Conference on Convergent Technologies for the Asia-Pacific, Bangalore, India, October 14-17, 2003.

[14] Peter Meerwald, “Digital Image Watermarking in the Wavelet Transform Domain”, MSc thesis in University of Salzburg, 2001.

[15] Saraju P. Mohanty, “Watermarking of digital images”, MSc thesis, Indian Institue of Science, January 1999.

[16] Cox, I., Millar, M., and Bloom, J. 2002. “Digital watermarking”, Morgan-Kaufmann,San Francisco, CA, ISBN: 1-55860-714-5.

[17] December 2004, http//www.watermarkingworld.org/, “Digital Watermarking Frequenly Asked Questions”, last checked on 03 January, 2007.

[18] Ingemar J. Cox, Matt L. Miller, Jeffrey A.Bloom, “Watermarking applications and their properties”, in International Conference on Information Technology, ITCC'2000. 2000, pp. 6-10.

[19] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, “Can Invisible Watermarks Solve Rightful Ownerships?” IBM Technical Report RC 20509,IBM Research, July 1996. IBM Cyberjournal: http://www.research.ibm.

[20] B. Zhou and J. Chen, “A Geometric Distortion Resilient Image Watermarking
Algorithm Based on SVD”, Chinese Journal of Image and Graphics, Vol. 9, April 2004, pp. 506-512.

[21] Jie Liu, Xiamu Niu and Wenhai Kong, “Image Watermarking based on Singular Value Decomposition”, Proceedings of the 2006 International Conference on Intelligent formation Hiding and Multimedia Signal Processing (IIH-MSP'06), pp. 457-460.

[22] Hearn, D. and Baker, M. 1997. “Computer graphics”, Prentice Hall, Englewood Cliffs,NJ, ISBN: 0-13-530924-7.

[23] Tolga Gokozan, “Template Based Image Watermarking in the Fractional Fourier Domain”, MSc thesis, Middle East Technical University, January, 2005.

E-mail id - Singhsaudan08@gmail.com