

# Improving Confidentiality of Watermark Image through Image Filtering Techniques

MSc Internship  
Cybersecurity

Abhishek Vikas Parab

Student ID: x18156070

School of Computing  
National College of Ireland

Supervisor: Imran Khan

National College of Ireland  
Project Submission Sheet  
School of Computing



<b>Student Name:</b>	Abhishek Vikas Parab
<b>Student ID:</b>	x18156070
<b>Programme:</b>	Cybersecurity
<b>Year:</b>	2019
<b>Module:</b>	MSc Internship
<b>Supervisor:</b>	Imran Khan
<b>Submission Due Date:</b>	12/08/2019
<b>Project Title:</b>	Improving Confidentiality of Watermark Image through Image Filtering Techniques
<b>Word Count:</b>	4175
<b>Page Count:</b>	17

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

**ALL** internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

<b>Signature:</b>	
<b>Date:</b>	10th August 2019

**PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:**

Attach a completed copy of this sheet to each project (including multiple copies).	<input type="checkbox"/>
<b>Attach a Moodle submission receipt of the online project submission</b> , to each project (including multiple copies).	<input type="checkbox"/>
<b>You must ensure that you retain a HARD COPY of the project</b> , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

<b>Office Use Only</b>	
Signature:	
Date:	
Penalty Applied (if applicable):	

# Improving Confidentiality of Watermark Image through Image Filtering Techniques

Abhishek Vikas Parab  
x18156070

## Abstract

Image watermarking are generally utilized for copyrighting of digital images in the online world. One cannot secure its data only by this method. Therefore a new approach of using image filtering techniques with image watermarking have been successfully implemented in this paper. This research also concludes the maximum number of filtering process that can be use on the watermark image. The quality of watermark image increases as image filtering techniques are applied, but reduces the similarity index between the original and recovered watermark. Applying Mean and Median filter have proved to efficient in improving quality and making watermark image more robust in nature.

huhojp

## 1 Introduction

In today's digital world, computer felony of digital contents being captured and modified while sending and receiving online, has been increased to exponential level. Thus for any individual or an organization, it is crucial to secured their digital content from getting tampered while transferring. Digital watermarking is one such method in which the digital content is stored with the owner's information in it ( Voyatzis et al. (1998)), thus denoting its authenticity of the content.

Visual cryptography is such a method of digital watermarking that can be used to achieve the image invisible watermarking. It is a method of concealing data in the still images Lavania et al. (2012). Visual cryptography can be divided by the domain it is being used - spatial or frequency. Spatial domain consist of Least Significant Bit (LSB) and spread spectrum. Frequency domain consists of Discrete Wavelet Transform (DWT), Fourier and Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Single Value Decomposition (SVD) and other Voyatzis et al. (1998). The earlier literature has shown that frequency domain being more robust as compared with spatial domain Lavania et al. (2012).

Visual cryptography (VC) may solve the infringement of digital images on the online world, though it is not completely secure when its comes while transferring the digital image. As when watermark is introduced on the main image, it damages the main image which is known as "visible noise" in the image Johnson and Jajodia (1998). This can be easily detected by the hacker who is performing Man-in-the-Middle attack (MIM) between the two sharing parties by using tools like steganalysis and scan the Peak signal-to-noise or Mean Squared Error of that image to know whether the original image is

tampered or not. Also it will be a problem if the image is being accessed by the person who is not authorized.

PSNR ( Peak signal-to-noise ratio) is relationship between the highest signal(power) and the distorting noise that impact the display of an image Instruments (2019). While MSE is computed by averaging the squared intensity differences of distorted and reference image pixels, along with the related quantity of PSNR Wang et al. (2004). Steganalysis is the process of detecting distortion or "noise" in the image Johnson and Jajodia (1998).

The section 2 in this paper depicts the methods of VC which is currently used. It displays what it had achieved and what security its lacks. The later sections focuses on methodology, designing process and implementing image filtering techniques on digital watermark to improve its quality and the overall result of it.

## **2 Related Work**

In this section, the literature review is provided from various research papers taken from NCI library, IEEE website and Google Scholar. This section gives a brief of work that has been conducted in the field of image watermarking. It also shows what are main security attributes are to be considered and later sub-section describes previous works and the comparison between them.

### **2.1 Background and Relation**

The main focus of this section is on the security properties that should be maintained by visual cryptography process.

#### **2.1.1 Robustness**

The property implies that extraction of watermark should be possible even though the VC technique made available to the public Naaz (2017).

#### **2.1.2 Imperceptibility**

In this property, the watermarked image should not have significant difference that is visible to user eye, else the VC is useless. The watermarked image might have slight differences which is acceptable but a not a major one as the attacker might be able to guess the difference if he has intercepted the communication.

#### **2.1.3 Capacity**

There is a measurement for the capacity of data that can be inserted into the watermark image. This is known as data payload. It involves the quantity of bits will be encoded in the image Naaz (2017), thus should be enough for digital watermarking process.

### **2.2 Domains and techniques involved in Digital Image Watermarking**

In Spatial domain of watermarking technique, the data is added in different pixel values of the carrier signal Kaur and Kaur (2013). There are 4 major techniques in this. The

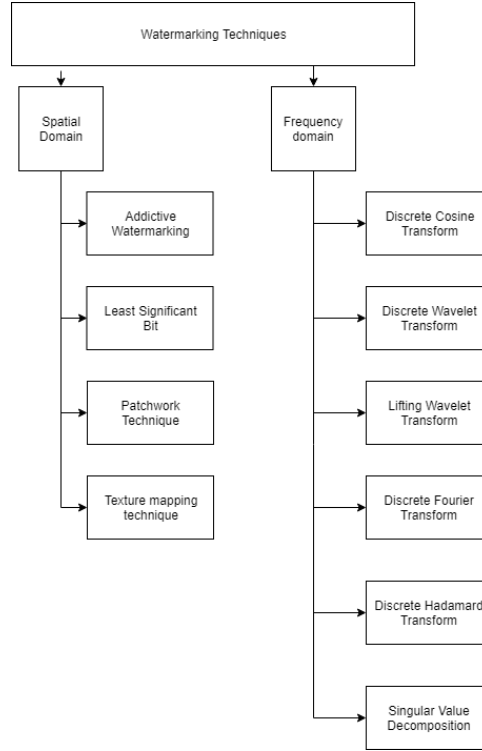


Figure 1: Types of Image watermarking techniques

first additive watermarking is the simplest of all. In additive watermarking, the pseudo random noise will be added to the intensity of image pixels Kaur and Kaur (2013). This kind of watermarking is easy to crack and gets detected in steganalysis. In Chopra et al. (2012), the authors have used Least Significant Bit (LSB) technique to implement watermark. In this, data has been added to the least significant bit of the pixels of the base image. The base image is of 8bit pixels in it. The information that has to be watermarked is replaced with the LSB of the base image. This technique is although simple, but it lacks the major security property of image watermarking of robustness. As, this technique is known to everyone, the information can be easily extracted from the watermarked image. The watermarking is vanquished by the lossy compression Mistry (2010). Also, the PSNR value of the watermarked image is low.

In patchwork technique, the information is added to the base image by making the illuminated pixel more illuminating and dark pixels more darker Yeo and Kim (2003). The drawback of this technique is it can not hold large amount of data. In texture image watermarking technique, the watermark is added to the texture part of the image Naaz (2017). the major drawback of this method only applicable to the images having expansive amount of textured image Naaz (2017). Therefore, all of the spatial domain techniques are pointless to used in real life because of their serious drawbacks.

On the contrary, the techniques in frequency domain are quite better in the aspect of robustness and resistant to various image attacks. In frequency domain watermarking, with the help of Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) or Discrete Fourier transform (DFT) the image is transformed in frequency and then data is added to the transform coefficients Mistry (2010).

	<b>Spatial Techniques</b>	<b>Frequency Techniques</b>
Robustness	Only used in digital-to-digital environments. Low Immunity	Powerful against noise attacks
Capacity and Display payload	Huge capacity	Less than Spatial
Imperceptibility	May introduce visual noise	Due to noise addition, watermark may be visible
Security	Not useful in real watermarking applications	Embedding of pseudo random sequence may be insignificant or not possible, only if an ideal technique exist.
Secret Key	Uses secret key	Uses secret key
Implementation	Easy	Moderate

Table 1: Comparison between Spatial and Frequency Techniques

## 2.3 Frequency domain used for Visual Cryptography

In Chu (2003), the author has proposed an alternative method of DCT instead of traditional method. In this the base image is sub sampled into small images which returns the DCT coefficients of those sub images Chu (2003). Coefficients of those sub images examined in pairs to find the right pair to impose the watermark. If the coefficient pair has very large contrast in their amplitudes then are skipped and not used. Watermark is inserted in those coefficients of sub images where the amplitude is distinctively similar. After imposing of watermark, it is passed through the Inverse Discrete Cosine Transform (IDCT) which results in the watermarked image. In the process of recovering the watermark, the image is processed under DCT and then compared with the sub sampled coefficients to retrieve the watermark from the image. Thus, this process of image watermarking does not need to collate the watermarked image with the original base image to recuperate the watermark.

In Lai and Tsai (2010), authors have proposed of using Discrete Wavelet Transform (DWT)- Single Value Decomposition (SVD) for image watermarking. Four sub-bands of the cover image is created using the one-level HAAR DWT and SVD is applied on Low-High (LH) and High-Low (HL) sub-bands. The watermark is divided in two chunks and the above two sub band LH and HL are alter with it. Finally, again SVD is perform on it to get the watermarked image. In the extraction process, the reverse method is used with the combining of the watermark that is extracted from each sub-bands. This proposed methods proves to be more imperceptible and robust under many image processing attacks.

According to the paper Kaushik (2012), a sophisticated method of image watermarking is being used. The author present the use of DFT with Arnold scrambling of the watermark before adding to it. In DFT the image is converted into frequency in the spatial image domain. Though DFT is capable of analysis of image in frequency domain, it lacks the capability of doing so in space-time domain Naaz (2017). For the proposed

method, the image is divided into sub-bands of  $256 \times 256$ . DFT is performed after the divided images are modified to  $8 \times 8$  matrix. Arnold scrambling is used with the watermark to generate two pseudo-random numbers from it. This number is added with the  $8 \times 8$  matrix of the cover image and DFT is performed to produce watermark image. The recovery process is similar to embedding process, after the watermarked image is converted into  $8 \times 8$  matrix, the watermark's amplitude spectrum is weighed up with the pseudo-random sequence. This results in the production of watermark matrix which can be extracted by using Arnold scrambling on that matrix. This method is time consuming and not feasible for real life example.

Tun and Thein (2013), proposed a method of using Lifting Wavelet Transform (LWT) with DCT transform. In LWT, the interdependence in the image pixel values helps in withdrawing the redundancy. In this paper, cover image is converted into four sub-bands - LL, LH, HL, HH using LWT transform. DCT is performed on the High-High (HH) sub-band of the cover image. Pseudo-random number is generated from watermark image which is then imposed on the HH sub-band image of the cover image. Inverse DCT (IDCT) and Inverse LWT (ILWT) transform is processed on the image to get the watermarked image. The decisions on the coefficients in LWT is difficult (Naaz (2017)) which makes it hard to implement.

In (Parvathavarthini and Shanthakumari (2014)), the watermark image and the cover image will be transformed with 2D - Hadamard. The scaling factor of the cover image will determine how much watermark can be forced on it. Inverse DHT (IDHT) transform is performed to obtain the final image. This experiment has better PSNR result but it is time consuming and the most complex of this domain methods. The section of the literature review describes the image filtering methods that can be imposed on the watermarked image to improve its quality.

In Imran Khan and Jeoti (2010), authors have demonstrated the use of Direct Current (DC) components for the manipulation in DCT domain. Generally, in DCT domain Alternating current (AC) components are handled for the watermarking of the image. The paper shows a different approach and it is as follows: quantization of JPEG image is performed and from  $8 \times 8$  blocks of pixels the DC components are gathered. Binary conversion is executed on these matrix. Least Significant Bits (LSB) are picked for embedding watermark Imran Khan and Jeoti (2010). Chaotic Seed Based Scrambler (SBR) is used to find random position of DC components in bit-plane are chosen to insert watermark. The blocks are replaced in the above random places and thus producing a watermark image. This is one of the blind watermarking techniques where, the original image is not required to withdraw watermark from the output image. This method is sensitive to many image processing attacks and also, its PSNR values are lower than the other traditional techniques.

## 2.4 Image watermarking with image filtering techniques

This section depicts various image filtering techniques which are available and can help to improve the visual cryptography imposed on the image. Only VC is not sufficient when it comes to watermarked image being transferred online as VC disrupts the quality and thus can be detected in steganalysis. Image filtering is a method of improving the quality of the original image without altering or degrading it.

In Poljicak et al. (2011), proposed a method of Unsharp filter can be used with watermarked image. In the image, the high frequency components are increased through

this filter. The high-frequency will be removed from image with the help of negative laplacian and then will be forced upon the original image. In the end, a blind deconvolution method which uses one point of soften image to enhance it will be applied to get the resulted image. This experiment has simple implementation, although output is not as good as expected.

According to Lavania et al. (2012), he proposed two filters that can be used to improve the quality of the image. Center to Boundary (CB) filter uses Newton-Raphson's formula to inspect the distance of the filter from the center to boundary and repeated till all the pixels of the image is scanned. Another filter, Boundary to Boundary (BB) filter, uses the same Newton-Raphson's formula to calculate the distance between the upper left Boundary to lower right Boundary pixels Lavania et al. (2012) until all pixel distance are calculated. As both the process are similar and are also easy to implement. The major drawback of these filters is the time constrain which they take process a single image. The next section displays the technologies and methods used for this research and how these technologies and methods benefited it.

### 3 Methodology

As it has been known, visual cryptography as a single mechanism is robust against the various types of image processing attacks and steganalysis. Due to the noise introduce after the watermark has been introduce in it, it will not be secure while transmitting. It may be detected if there is Man-in-the-Middle (MAM) attacks. Therefore, in this paper we proposed a method of image filtering that will be used over watermarked image. For this experiment, DWT-DCT method of watermarking is used from ( Al-Haj (2007)). This method proves to be more effective in terms of robustness and time processing. Also, for image filtering, three filters have been used - Mean, Median and Box filter for the research. The following section gives a brief introduction of DWT and DCT transformation and also of filters that will be used over it.

#### 3.1 DWT Transform

In unpredicted and discontinuity of signals, wavelets has been greatly acknowledged. In 2-D images, when DWT is applies it converts the images into four non-overlapping sub-bands LL1 LH2, HL1, HH2 ( Al-Haj (2007)). Rough-scale DWT coefficient is presented by the LL1 sub-bands and other sub-bands represents the fine scale of it. LL1 sub-band is divided additionally more to obtained N scale of rough-scale of coefficients N. After achieving N scale of coarse, a multiresolution of 'sub-bands LLN and LHx, HLx, and HHx combined as  $3N+1$  sub-bands, where x resides from 1 to N ( Al-Haj (2007)).

DWT is worthy when it comes to find out the region where watermark can be embedded in the original image due to its spatio-frequency localization characteristic. This feature also helps when a DWT coefficient is changed, only neighboring coefficients gets affected, which is great as entire image's coefficients is not disturbed. Most of image watermarking techniques which is done with DWT transform is done in the LL sub-bands as more image energy is focused here. This also deteriorate the image quality but increases the robustness effectively. Therefore, the best regions to implement watermark is the sub-bands like LHx and HLx which gives tolerable robustness and imperceptibility be gained( Al-Haj (2007)).



### 3.2 DCT Transform

In this, the conversion of time domain signal into frequency domain signal is performed (Naaz (2017)). For the modified output image,  $y$ , with the equation below and the input image,  $x$ , is transformed. Also,  $y(u,v)$  represents the DCT coefficients and  $x(m,n)$  is the  $N \times M$  pixels of the source image.

$$y[u, v] = \sqrt{\frac{2}{M}} \sqrt{\frac{2}{N}} \alpha_u \alpha_v \sum_{m=0}^{M-1} x(m, n) \cos \frac{(2m+1)u\Pi}{2M} \cos \frac{(2n+1)v\Pi}{2N} \quad (1)$$

where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{2}}, & u=1 \\ 1, & u=1,2,\dots,N-1 \end{cases} \quad (2)$$

$$\alpha_v = \begin{cases} \frac{1}{\sqrt{2}}, & v=1 \\ 1, & v=1,2,\dots,N-1 \end{cases} \quad (3)$$

Image reconstruction is performed by applying inverse DCT that is shown in the Eq.(4) below:

$$x(m, n) = \sqrt{\frac{2}{M}} \sqrt{\frac{2}{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \alpha_u \alpha_v y(u, v) \cos \frac{(2m+1)u\Pi}{2M} \cos \frac{(2n+1)v\Pi}{2N} \quad (4)$$

When DCT is applied to an image, it produces three frequency sub-bands i.e., low, mid and high frequency sub-bands (Al-Haj (2007)). Most of the information of the image is stored in the low and high frequency sub-bands. Therefore, the best practical way to insert watermark is into middle sub-band as the image quality will not be disturbed.

### 3.3 Image Filters

For this research, three filters will be used to enhance the quality of watermarked image.

#### 3.3.1 Mean filter

It is a linear filter, which basically calculating the average value of the neighbouring pixels changes the output image. Smoothing the image and removing the noise from it is the advantage of this filter.<sup>1</sup>

#### 3.3.2 Median filter

This filter uses a window that slides to each pixels of the image to collect its value. If it is  $3 \times 3$  filter, then 9 values will be collected. So after adding one with nine and then dividing it by 2 will give the median filter number. The pixel value at that number will be consider as median and all the values of other pixels will be change accordingly. This filter is good for smoothing of the image and best when it has to remove salt and paper noise from it<sup>2</sup>.

---

<sup>1</sup> Tutsplus <https://code.tutsplus.com/tutorials/image-filtering-in-python--cms-29202>

<sup>2</sup> Tutsplus <https://code.tutsplus.com/tutorials/image-filtering-in-python--cms-29202>

### 3.3.3 Box filter

This is type of low pass filter. It averages out the kernel matrix of the images. This kernel size can be defined as we want but usually depends on the size of the image <sup>3</sup>. The next section describes how these above methods will be implemented in the research and the flow of this.

## 4 Design Specification

### 4.1 Performing DWT-DCT to obtain watermark image

The following flowchart describes the procedure of obtaining watermark image. There are five major mathematical calculation in this section - applying two level DWT, DCT, IDCT, two level IDWT and key generation for the watermark.

1-level DWT is performed to obtain 4 sections of the image known as four sub-bands. When again DWT is performed, it is applied on the HH1 or HL1 sub-band of the previous output to get sub section only in this specific band. DCT is performed on the this selected sub-band from previous output of two-level DWT.

Inverse DWT and DCT are performed to get watermarked image. Key of watermark will be used to extract the watermark from the watermarked image.

### 4.2 Applying Mean, Median and Box filter

These filters are applied to enhance the quality of watermarked image. First mean filter is applied, which is followed by median filter and then finally by the box filter. These three filter will help to remove the noise that was introduced in the watermarked image, when watermark was added in it. The outcome will be an enhanced watermarked image.

### 4.3 Recovering watermark

The key that was used with watermark will be used to recover the watermark from the watermarked image. The procedure is in reverse order of that used in insertion of watermark.

---

<sup>3</sup> Packtpub <https://hub.packtpub.com/image-filtering-techniques-opencv/>

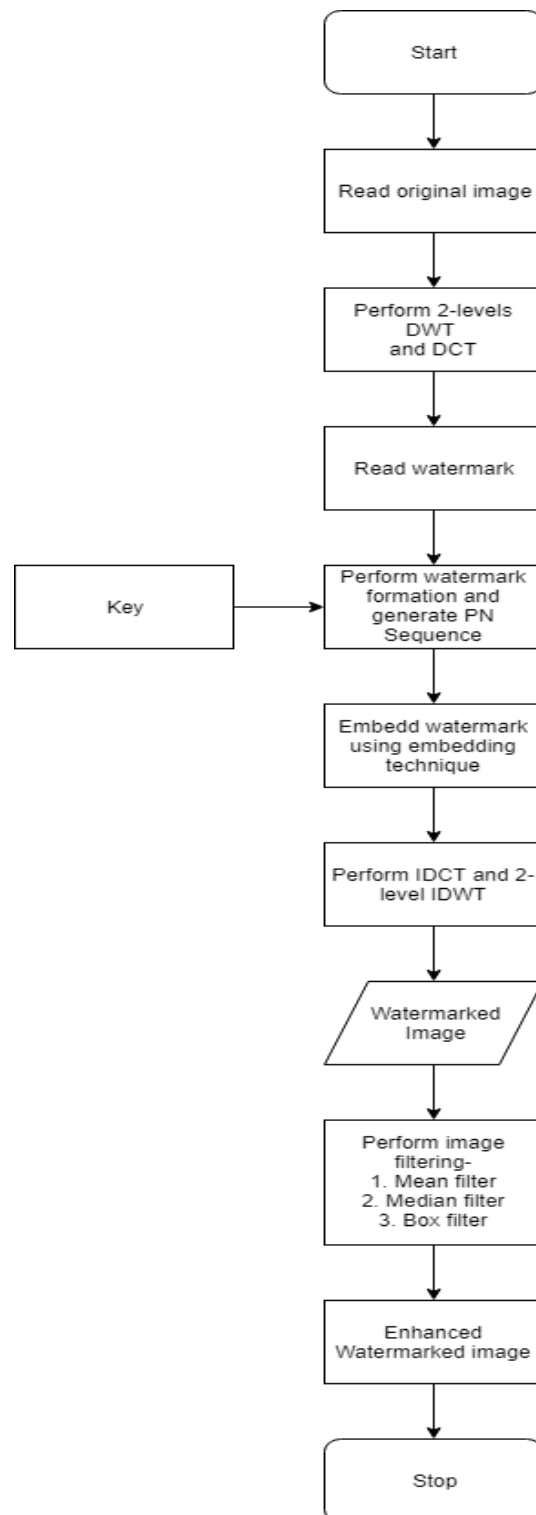


Figure 2: Flowchart for watermarking of an image using Visual Cryptography

## 5 Implementation

For this experiment, python programming language is used. As the language is similar C, C++ it is easy to understand. The purposed of this experiment is to improve the quality of watermarked image through image enhancement techniques so that the confidentiality of the watermark remains intact and has better PSNR, MSE values. The following is the detail process of implementing the research method.

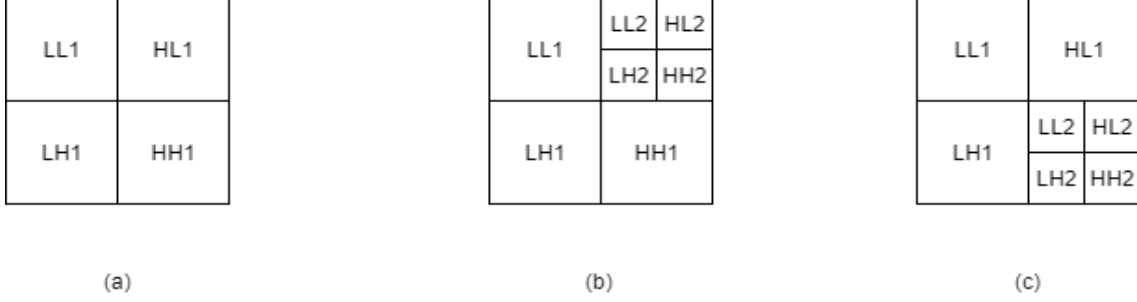


Figure 3: (a) DWT applied on the cover image; (b) DWT applied on HL1; (c) DWT applied on HH1

### 5.1 Algorithm for Embedding Watermark and Applying Mean, Median and Box Filter

- Step 1:** Four non-overlapping sub-bands are created using DWT on the cover image - LL1, LH1, HL1, HH2.
- Step 2:** DWT is performed again on the HL1 to get four sub-bands and HL2 of it is selected or it can be performed on HH1 sub-band and HH2 is selected as displayed in the fig. 5.
- Step 3:** Perform division on selected HH2 (or HL2) and convert into 4×4 sub-bands.
- Step 4:** Perform DCT on each of the chosen bands.
- Step 5:** Convert the grey-scale watermarked image into the quantity of ones and zeros.
- Step 6:** Initiate two uncorrelated pseudo-random sequences. One will be used to insert watermark bit 0 (PN\_0) and the other will be utilized to insert watermark bit 1 (PN\_1). The total number of mid-bands components of DCT-transformed DWT sub-bands Al-Haj (2007) should be equal to the number of bits in the pseudo-random sequence.
- Step 7:** In the DCT transformed of selected block insert the pseudo-random sequence with the help of gain factor.
- Embedding is only process in the mid-block section of DCT coefficients. The embedding is as follows, if the matrix of the mid-band coefficient of DCT transformed is considered as Y:

$$Y = Y + \alpha \times PN_0 \quad (5)$$

otherwise,

watermark bit 1 is used then,

$$Y = Y \dot{+} \alpha \times PN\_1 \quad (6)$$

**Step 8:** Apply IDCT to the each of the modified blocks to embed the watermark as related above.

**Step 9:** On the modified blocks and also the DCT blocks, apply IDCT on it to construct the watermark image fig.(4).



Figure 4: Watermark applied on Lena Image

**Step 10:** Apply Median filter on the watermarked image. For this the image is divided into  $3 \times 3$  kernel.

**Step 11:** Then all the pixels values are read and stored. To find the median, total number of kernel blocks plus 1, divided by 2 will give the median.

**Step 12:** The pixel value to this number will be selected and that will be applied to all the blocks of the kernel pixels. Thus producing median filter watermarked image.

**Step 13:** On the previous output image apply mean filter. In this, the image will be again divided into  $3 \times 3$  blocks.

**Step 14:** The sum of each pixel will be taken and be subtracted by 9. This will give the mean value of the pixels.

**Step 15:** The resulted value will be replaced with the center pixel and all the other pixel values will be changed according to the mean value of the neighboring pixels. And finally a mean filter applied image will be generated.

**Step 16:** Box filtered is applied on the above output image. This will result in up-scaled robust watermarked image fig. (5).



Figure 5: Image enhancement applied on watermark Lena Image

For the recovery of the watermark, the host image is not required to withdraw watermark which makes this algorithm as blind algorithm. The method for recovering the watermark is similar to the implementing the watermark.

For this experiment to be held, python language was used to write and execute the the algorithm and evaluate the outcomes. The following two cover images and watermark image were used for this experiment.

Copyright

Figure 6: Watermark



(a) Lena.png



(b) Teddy.png

Figure 7: Cover image samples

The next section describes how the evaluation of the results of the recovered watermark and how image enhancement has affected it.

## 6 Evaluation

This section shows how image enhancement techniques have affected the watermark in the image and how it can be used. For the evaluation purpose MSE, PSNR and SSIM is used. Higher the value of PSNR, better the image quality. MSE shows the difference between two images, whereas SSIM shows the similarity between the two images.

### 6.1 No filters applied

Simply after the image was processed through the image watermarking process. The watermark was recovered from the image and then compared with the original watermark to learn how much it has been recovered and how was the quality (PSNR). As it can be

MSE: 1344.08, SSIM: 0.89 , PSNR: 16.85



Figure 8: Comparison between original watermark and watermark recovered from DWT and DCT Technique

seen that, the MSE and PSNR value is good. Also, SSIM index is 0.89 ,which makes the similarity between the two images identical.

### 6.2 Applied mean filter

In this case study, watermark image was processed with mean filter only. The watermark was then extracted from that output. The PSNR and MSE values of this recovered image is better than the previous without filtering.

MSE: 35874.91, SSIM: 0.16 , PSNR: 2.58



Figure 9: Comparison between original watermark and watermark recovered from mean filter

### 6.3 Median filter applied on mean filter watermarked image

For this experiment, the previous experiment with median filter was applied to it. The watermark image was processed by mean filter and then by median filter applied on it. The watermark was required thus after this step for comparison.

MSE: 47837.92, SSIM: 0.03 , PSNR: 1.33



Figure 10: Comparison between original watermark and watermark recovered from mean and median filter

For the above output, it can be concluded that after median filter quality of the image has increased, though the SSIM value is low but still it is visibly similar.

When the third filter was applied on the above watermark image, it was impossible to recover the watermark. Thus, it proved that only two filters can be applied or else the watermark can not be extracted. Those two filters are - mean filter and median filter.



The following table summarizes the quality of watermark image when compared with original watermark. Also, it shows different combination of techniques used on lena.png.

Original watermark vs Watermark recovered from	MSE	SSIM	PSNR
DWT-DCT transform	1344.08	0.89	16.85
DWT-DCT mean filter	35874.91	0.16	2.58
DWT-DCT transform median filter	18808.60	0.51	5.39
DWT-DCT transform box filter	55113.30	0.01	0.72
DWT-DCT transform mean median filter	47837.92	0.03	1.33
DWT-DCT mean median box filter	55801.88	0.00	0.66
DWT-DCT transform mean box filter	55332.51	0.01	0.70
DWT-DCT transform median box filter	55837.67	0.00	0.66

Table 2: Different combination of filtering techniques and their quality

The following is the comparison between the original cover image and mean and median filter applied to watermark image of Lena.png.

MSE: 7.24, SSIM: 0.93 , PSNR: 39.53



Figure 11: Comparison between original cover image and watermark image after mean and median filter

From the above fig. (11), it can be conclude that after applying two filters - mean and median , the quality of the image increases and the similarity index (SSIM) is excellent as compared to just watermark image.

## 6.4 Discussion

In this research, it can be concluded that only two filters can be applied maximum on watermark image as till now. The value of SSIM and PSNR are inversely proportionate. IF more filter are applied on watermark image in order to enhance it , the PSNR value of the recovered watermark will be more but the SSIM value will decreased and eventually there will be no similarity between the two images. Also,the research only work when only two filters are applied, if more numbers of filters are applied, then it impossible to recover the data from the image.

## 7 Conclusion and Future Work

In this research, a better method of increasing the quality of watermark image has been implemented. This method helps the watermark image to withstand various image processing attacks and can avoid its detection in steganalysis process. This experiment also presented that only two image filtering process can be applied on watermark. As concluded in the evaluation if more than two are applied, it is unmanageable to recover the watermark. Also the the quality of the image is inversely proportional to the similarity index between the two images. In future, a new filtering process can be applied on the above method to achieve a better watermark image with capability of recovering superior quality watermark.

## References

- Al-Haj, A. (2007). Combined dwt-dct digital image watermarking, *Journal of computer science* **3**(9): 740–746.
- Chopra, D., Gupta, P., Sanjay, G. and Gupta, A. (2012). Lsb based digital image watermarking for gray scale image, *IOSR journal of Computer Engineering* **6**(1): 36–41.
- Chu, W. C. (2003). Dct-based image watermarking using subsampling, *IEEE Transactions on Multimedia* **5**(1): 34–38.
- Imran Khan, M. and Jeoti, V. (2010). A blind watermarking scheme using bitplane of dc component for jpeg compressed images, *2010 6th International Conference on Emerging Technologies (ICET)*, pp. 150–154.
- Instruments, N. (2019). Peak signal-to-noise ratio as an image quality metric. Last accessed 25 March 2019.  
**URL:** <http://www.ni.com/en-us/innovations/white-papers/11/peak-signal-to-noise-ratio-as-an-image-quality-metric.html>
- Johnson, N. F. and Jajodia, S. (1998). Steganalysis: the investigation of hidden information, *1998 IEEE Information Technology Conference, Information Environment for the Future (Cat. No.98EX228)*, pp. 113–116.
- Kaur, G. and Kaur, K. (2013). Image watermarking using lsb (least significant bit), *International Journal of Advanced Research in Computer Science and Software Engineering* **3**(4).
- Kaushik, A. K. (2012). A novel approach for digital watermarking of an image using dft, *Int JElectronComp Sci Eng* **1**(1): 35–41.
- Lai, C. and Tsai, C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition, *IEEE Transactions on Instrumentation and Measurement* **59**(11): 3060–3063.
- Lavania, K. K., Kumar, R. et al. (2012). Image enhancement using filtering techniques, *International Journal on Computer Science and Engineering* **4**(1): 14.

- Mistry, D. (2010). Comparison of digital water marking methods, *International Journal on Computer Science and Engineering* **2**(09): 2905–2909.
- Naaz, S. (2017). Spatial and frequency domain digital image watermarking techniques for copyright protection, *International Journal of Engineering Science and Technology (IJEST)* **9**: 691–699.
- Parvathavarthini, S. and Shanthakumari, R. (2014). An adaptive watermarking process in hadamard transform, *International Journal of Advanced Information Technology* **4**(2): 1.
- Poljicak, A., Mandi, L. and Kurecic, M. (2011). The influence of image enhancement filters on a watermark detection rate authors, *Acta Graphica : Journal for Printing Science and Graphic Communications* **22**.
- Tun, A. and Thein, Y. (2013). Digital image watermarking scheme based on lwt and dct, *International Journal of Engineering and Technology* **5**(2): 272.
- Voyatzis, G., Nikolaidis, N. and Pitas, I. (1998). Digital watermarking: An overview, *9th European Signal Processing Conference (EUSIPCO 1998)*, pp. 1–4.
- Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P. et al. (2004). Image quality assessment: from error visibility to structural similarity, *IEEE transactions on image processing* **13**(4): 600–612.
- Yeo, I.-K. and Kim, H. J. (2003). Generalized patchwork algorithm for image watermarking, *Multimedia Systems* **9**(3): 261–265.  
**URL:** <https://doi.org/10.1007/s00530-003-0097-0>