

## Image Security through Visible and Invisible Watermarking Techniques

**Narendra. M. Jathe**

*Department of Computer Science, Arts Commerce and Science College  
Kiran Nagar Amravati, India*

*Received 21 September 2019; Accepted 10 October 2019*

**Abstract:** Today's world is digital world. Nowadays, in every field there is enormous use of digital contents. Information handled on internet and multimedia network system is in digital form. The copying of digital content without quality loss is not so difficult. Due to this, there are more chances of copying of such digital information. So, there is great need of prohibiting such illegal copyright of digital media. Digital watermarking (DWM) is the powerful solution to this problem. Digital watermarking is nothing but the technology in which there is embedding of various information in digital content which we have to protect from illegal copying. This embedded information to protect the data is embedded as watermark. Beyond the copyright protection, Digital watermarking is having some other applications as fingerprinting, owner identification etc. Digital water-marks are of different types as robust, fragile, visible and invisible. Application is depending upon these watermarks classifications. There are some requirements of digital watermarks as integrity, robustness and complexity. In digital watermarking, a watermark is embedded into a cover image in such a way that the resulting watermarked signal is robust to certain distortion caused by either standard data processing in a friendly environment or malicious attacks in an unfriendly environment. This paper presents a digital image watermarking based on two dimensional discrete wavelet transform (DWT2), two dimensional discrete cosines transform (DCT2) and two dimensional fast Fourier transform (FFT2). Signal to noise ratio (SNR) and similarity ratio (SR) are computed to measure image quality for each transform.

**Keywords:** Digital watermarking, DWT2, DCT2, FFT2, SNR, SR

### I. INTRODUCTION

We are living in the era of information where billions of bits of data is created in every fraction of a second and with the advent of internet, creation and delivery of digital data (images, video and audio files, digital repositories and libraries, web publishing) has grown many fold. Since copying a digital data is very easy and fast too so, issues like, protection of rights of the content and proving ownership, arises. Digital watermarking came as a technique and a tool to overcome shortcomings of current copyright laws for digital data. The specialty of watermark is that it remains intact to the cover work even if it is copied. So to prove ownership or copyrights of data watermark is extracted and tested. It is very difficult for counterfeiters to remove or alter watermark. As such the real owner can always have his data safe and secure. Our aim was to study different watermarking techniques and implement the one which is most resistant to all types of attack, scalar or geometric. Counterfeiters try to degrade the quality of watermarked image by attacking an image (generally attacks are median and Gaussian filter, scaling, compression and rotation of watermarked image). By attacking watermarked image it become very difficult to recover watermark back from the watermarked image and even if it extracted one may no longer use it to prove the ownership and copyrights. So our main idea was to find such regions, also known as patches, in an image which are very stable and resistant to attacks.

This paper gives full insight of digital watermarking, its history, requirements, application and possible attacks. The first subheading tells how, with information revolution, the need to have some technique to prevent piracy and illegal copying of data arises. This need give rise to a new technique, known as Digital Watermarking. While proposing any algorithm some parameters are needed to keep in mind on which the proposed algorithm must be consistent. These parameters are discussed in following section. Following sections are dedicated to watermarking application and attacks. A lot of work is going on for making watermarking techniques immune towards attack to retain the originality of watermark and assuring successful extraction of watermark with low error probabilities so to sort out disputes, if any, over copyrights or ownership.

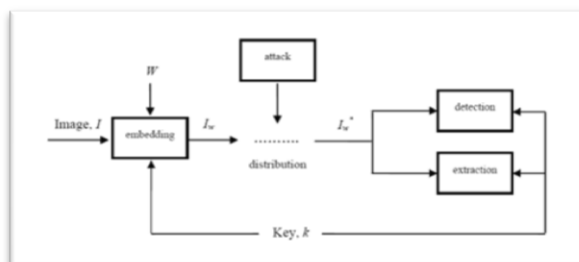
### II. OVERVIEW

Hold an Rs 100 note up or your offer letter up to light. What you will see is a picture of Mahatma Gandhi or company's logo respectively. This is what is known as a watermark mainly used to prove the ownership (in case of offer letter, watermark prove that the document is of facial document of company meant

for official work) or authenticity (in case of Rs 100, watermark rule out the forgery and authenticate the piece of paper of its worth).The watermark on the Rs100 (Figure1), just like most paper watermarks today, has two properties. First, the watermark is hidden from view during normal use, only becoming visible as a result of a special viewing process (in this case, holding the bill up to the light). Second, the watermark carries information about the object in which it is hidden (in this case, the watermark indicates the authenticity of the bill) [1].



**Figure 1: Image showing an INR 100 note having watermark at its left side which is considerably visible when note hold under light**



**Figure 2: watermarking system**

Thus, watermarking is defined as, “the process of possibly irreversibly embedding information into a digital signal. The signal may be audio, pictures or video”.

The components of a watermark embedding/detection/extraction system are shown in Figure 2. The embedded data can be detected in, or extracted from, a multimedia element in an application.

### Objectives

An effective authentication scheme should have the following desirable features:

- To be able to determine whether an image has been altered or not.
- To be able to locate any alteration made on the image.
- To be able to integrate authentication data with host image rather than as a separate data file.
- The embedded authentication data be invisible under normal viewing conditions.
- To allow the watermarked image be stored in lossy- compression format [3]

### III. LITREATURE REVIEW

Within the field of watermarking, image watermarking particularly has attracted lot of attention in the research community. Most of the research work is dedicated to image watermarking as compared to audio and video. There may be 3 reasons for it. Firstly, because of ready availability of the test images, secondly because it carries enough redundant information to provide an opportunity to embed watermarks easily, and lastly, it may be assumed that any successful image-watermarking algorithm may be upgraded for the video also. Images are represented/ stored in spatial domain as well as in transform domain. The transform domain image is represented in terms of its frequencies; whereas, in spatial domain it is represented by pixels. In simple terms, transform domain means the image is segmented into multiple frequency bands. To transfer an image to its frequency representation, we can use several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways. Watermarks can be embedded within images by modifying these values, i.e. the transform domain coefficients. In case of spatial domain, simple watermarks could be embedded in the images by modifying the pixel values or the Least Significant Bit (LSB) values. However, more robust watermarks could be embedded in the transform domain of images by modifying the transform domain coefficients. In 1997 Cox et al. presented a paper “Secure Spread Spectrum Watermarking for Multimedia” [19], one of the most cited paper (cited 2985 times till April’ 2008 as per Google Scholar search), and after that most of the research work is based on this work. Even though spatial domain based techniques cannot sustain most of the common attacks like compression, high pass or low pass filtering etc., researchers present spatial domain based schemes.

Now-a-days, researchers are focusing on mixing of spatial and transformed domains (i.e. combinations of DFT, DWT and DCT) concepts and also applying more and more mathematical and statistical model, and other interdisciplinary approaches in watermarking: for example use of chaotic theory, fractal image coding etc. In this section we are presenting the brief of few recent watermarking algorithms.

In [10], authors presented a reversible watermarking scheme for the 2D-vector data (point coordinates), which are used in geographical information related applications. This reversible watermarking scheme exploits the high correlation among points in the same polygon in a map and achieves the reversibility of the whole scheme by an 8-point integer DCT, which ensures that the original 2D-vector data can be watermarked during the watermark embedding process and then perfectly restored during the watermark extraction process. In this scheme, author used an efficient highest frequency coefficient modification technique in the integer DCT domain to modulate the watermark bit “0” or “1”, which can be determined during extraction without using any additional information. To alleviate the visual distortion in the watermarked map caused by the coefficient modification, they proposed an improved reversible watermarking scheme based on the original coefficient modification technique. Combined with this improved scheme, the embedding capacity could be greatly increased while the watermarking distortion is reduced as compared to the original coefficient modification scheme presented in [13]. In [15], authors presented zero-knowledge watermark detectors. Current detectors are based on a linear correlation between the asset features and a given secret sequence. This detection function is susceptible of being attacked by sensitivity attacks for which zero knowledge does not provide protection. In this work, a new zero-knowledge watermark detector robust to sensitivity attacks is presented, using the generalized Gaussian Maximum Likelihood (ML) detector as the basis. The inherent robustness that this detector presents against sensitivity attacks, together with the security provided by the zero-knowledge protocol that conceals the keys that could be used to remove the watermark or to produce forged assets, results in a robust and secure protocol. Additionally, two new zero-knowledge proofs for modulus and square root calculation are presented. They serve as building blocks for the zero-knowledge implementation of the Generalized Gaussian ML detector, and also open new possibilities in the design of high level protocols.

If digital watermarking is to adequately protect content in systems which provide resolution and quality scalability, then the watermarking algorithms must provide both resolution and quality scalability. Although there exists a tradeoff between resolution and quality scalability, it has been demonstrated that it is possible to achieve both types by taking advantage of human visual system characteristics to increase quality scalability without compromising resolution scalability. Watermarking algorithms considering this problem have been proposed; however, they tend to focus on a single type of scalability, resolution or quality. In their work, authors focused on providing a spread spectrum watermarking algorithm which had both resolution and quality scalability demonstrated through experimental testing using the JPEG2000 compression algorithm. To alleviate this trade off, they began with a non-adaptive resolution scalable algorithm and exploited the contrast sensitivity and texture masking characteristics of the HVS to construct an HVS adaptive algorithm that has good quality scalability. Their algorithm is specifically designed to concentrate on textured regions only, avoiding the visible distortions, which may occur when strength increases are applied to edges. Furthermore, this texture algorithm is applied in the wavelet domain but uses only a single resolution for each coefficient to be watermarked.

In the field of color images watermarking, many methods are accomplished by marking the image luminance, or by processing each color channel separately. Therefore, in paper [25], authors proposed a new DCT domain watermarking expressly devised for RGB color images based on the diversity technique in communication system. The watermark is hidden within the data in the same sequence by modifying a subset of the block. DCT coefficients of each color channel. Detection is based on combination method which takes into account the information conveyed by three color channels. Even if a particular channel is severely faded, they are still able to recover a reliable estimated of transmitted watermark through other propagation channel. Experimental results, as well as theoretical analysis, are presented to demonstrate the validity of the new approach with respect to algorithm operating on image luminance only.

#### IV. METHODOLOGY

The methodology for this paper is to encode the given digital images with different cover images. Here, the water marking is implemented with the help of DWT and DCT techniques. The process is carried out with the help of encoder and decoder technique.

##### **Encoder**

The first part of the watermarking process is, of course, the encoder. The first step is to decompose the image into ten frequency bands using three resolutions of Haar wavelets.

The steps of the our proposed watermarking methodology is described as follows:

1. Select image I and Apply DWT on the Cover image
2. Select a key k that generates the QR(Quick Response) code as a secret key.
3. QR code and Watermark is encrypted by using simple XOR operation

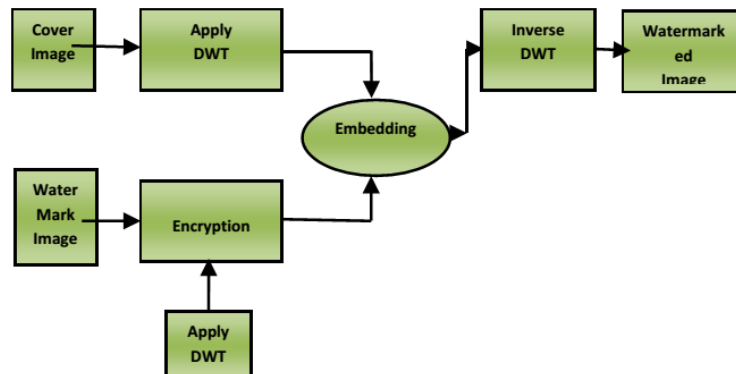
$$E(I,j) = W(I,j) \oplus QR(I,j)$$

4. Encrypted Watermark is embedded into the cover image by applying simple condition

$$IF (E(I,j) \neq 0)$$

$$\text{Then Red}(I(I,j)) = \text{Red}(I(I,j)) + 1$$

Then Green  $(I(I,j))=Red(I(I,j))+1$   
 Then Blue  $(I(I,j))=Red(I(I,j))+1$   
 5. Then apply Inverse DWT on the embedded watermarked image  
 $WI(I,j) = IDWT(I(I,j))$



This technique will decompose the cover image of the two dimensional DWT into four frequency bands through the first pass as (LL1), (LH1), (HL1) and (HH1) frequency coefficients. The frequency bands where it has the lowest resolution of the 1<sup>st</sup> pass (LL1) can be also decomposed into a 2<sup>nd</sup> level (pass). Secondly, we are to apply the Gaussian Noise and can insert the watermark signature into the rest of the available frequency bands which include the high frequency coefficients without dealing with (LL) regions from all over the passes (levels). We must add the signal of the bands where the large frequency components to the signal of the Gaussian Noise and modifying them without moderating the original signal which resides in the (LL) band; thereafter, the watermarked image would be performed appropriately.

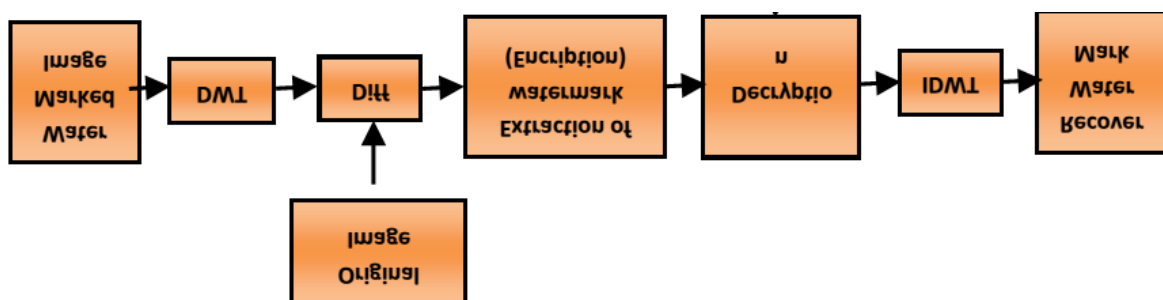
**Decoder**

At the other end of the communication channel, a decoder is used to extract the watermarked information from the received image. Upon reception of the supposedly watermarked image, the algorithm first isolates the signature included in this image by comparing the DWT coefficients of the image with those of the original (non-watermarked) one. The following operation consists of taking the identified key to put in contrast with the found signature by computing the cross-correlation at the first resolution level (*i.e.* highest frequency coefficients). The watermark is called detected if there is a peak in the cross-correlation corresponding to a positive identification. If there is no central peak, the decoder adds the second resolution level to the computation aiming at finding a peak. Once again, if there is a peak, the watermark is called detected and if not, we go to the third resolution... and so on until we reach the ninth resolution limit.

After encryption and embedding of watermark in cover image we have to recover the watermark and decryption shown in the block diagram and execution of the algorithm is shown in the figures. Extraction of Watermark. Select the watermarked image  $WI(I,j)$  and apply the DWT on the watermarked image.

$WD(I,j) = DWT(WI(I,j))$

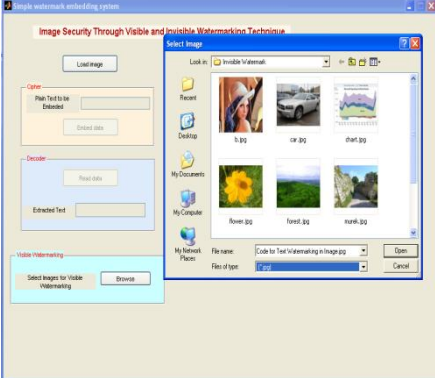

1. Select the original cover image  $I(I,j)$  and then apply the DWT on the Cover image.
2. Compare the transformed original image and watermarked image and get encrypted watermark  $E(I,j)$ .
3. apply the decryption algorithm on the  $E(I,j)$   
 $W(I,j)=QR(I,j) \text{ X-NOR } E(i,j)$



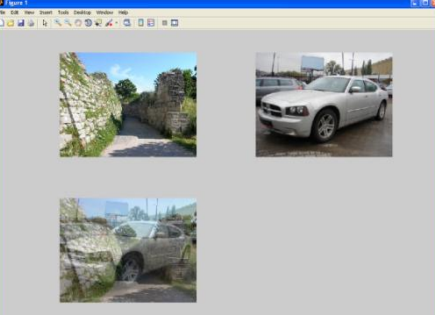
**IV. EXPERIMENTAL ANALYSIS AND RESULTS**

Experiments have been done on the proposed method with its two methodologies such as invisible and visible watermarking. The DWT and DCT technique is used for the experiments. Which is explain in the next context. The practical implementation of proposed algorithm with the help of MATLAB is shown.

**A. Invisible Watermarking**

<p>The first button of the GUI i.e. Load Image is used to select the cover image. The second button get automatically enabled after the selection of cover image.</p>	
<p>The text box inside the Cipher operation feed with the plain text to be embedded in the cover image. After pressing the Embed data button, the plain text will be hidden in the cover image. And it will generate the output.bmp file as shown in this figure.</p>	
<p>During the Decoder operation, when pressing the Read Data button, the plain text will be extracted from the cover image. If we select the output.bmp file from the Load Image button, we can also extract the plain text correctly which is shown in this figure.</p>	

**B. Visible Watermarking**

<p>In the visible watermarking, two different images has been selected for the operation. The intermixing of both the images can be done here. It is the visible watermarking and is shown in this figure.</p>	
--	--

The above figure shows two different image intermixed with the help of MATLAB implementation.

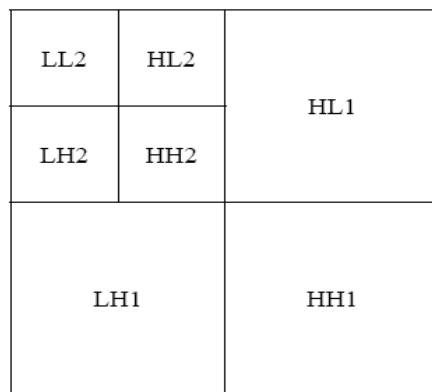
The theoretical aspect of invisible and visible watermarking is discussed in the following context.



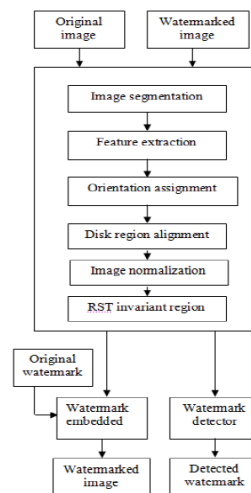
**i. DWT Domain Watermarking**

Wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part. It can distill the information from signal effectively. The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district .Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low frequency district(LL) and three high-frequency districts (LH,HL,HH). If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. The following figure represents the watermarking system in DWT.

In two-dimensional separable dyadic DWT, each level of decomposition produces four bands of data, one corresponding to the low pass band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass bands. The decomposed image shows a coarse approximation image in the lowest resolution low pass band, and three detail images in higher bands. The low pass band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached.



**Figure 3 : DWT decomposition with two levels**



**Figure 4 : Architecture of Watermarking**

The proposed watermarking system is given in the following process:

**Embedding watermarking**

The following is the proposed system methodology.

**Simulation results**

Since the magnitudes of DWT coefficients are larger in the lowest band at each level of decomposition, it is possible to use a larger scaling factor for watermark embedding. For the other 3 bands, the DWT coefficients are smaller, allowing a smaller scaling factor to be used. The resulting watermarked image does not have any degradation leading to a loss in its commercial value. In the below experiments, we measured the visual quality of watermarked and attacked images using the Signal To-Noise Ratio (SNR), SNR measures are estimates of the quality of the reconstructed image compared with an original image. The fundamental idea is to compute the value which reflects the quality of the reconstructed image. Reconstructed image with higher metric are judged as having better quality.

The visual quality of extracted visual watermarks is measured by the Similarity Factor (SF). The DWT was performed using Matlab with the wavelet filter. The chosen attacks were JPEG compression (with 3 quality factors), also we measured a compression ratio (CR) it defined by compression Ratio=image bytes/compressed bytes.

For first levels of decomposition, the proposed watermarking scheme was tested using six types of attacks. The DWT was performed using Matlab. The chosen attacks were JPEG compression (with 3 quality factors), blurring, adding Gaussian noise, filtering, histogram equalization, intensity adjustment and rotation. The scaling factor we use it with three different values 0.09, 0.5 and 0.8.

The following data calculated from run matlab code for DWT watermarking for different value of quality factor and alpha (gain).

### First Level Decomposition

Figure 5 shows the 256x256 gray scale cover image Cameraman and 128x128 visual watermark copyright.



Figure 5 a) Cover Image



b) Watermark text

The watermarked image in LL, LH, HL and HH bands are presented respectively in Figure 5a for different value of scaling factors and different quality factors, and the number below each image denotes the SNR value.

The attacked images are presented in Figure 5b together with the tools and parameters used for the attacks. The number next to the label below each image denotes the SNR value.

### ii. DCT Image watermarking

The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. The DCT has special property that most of the visually significant information of the image is concentrated in just a few coefficients of the DCT. It's referred as 'Energy compaction Property'.

As DCT is having good energy compaction property, many DCT based Digital image watermarking algorithms are developed. Common problem with DCT watermarking is block based scaling of watermark image changes scaling factors block by block and results in visual discontinuity. In this paper, we propose a visible watermarking technique that modifies the DCT coefficients of the host image using eqn. (1). We call an embedding factor we try different values for it to achieve visible watermarking we find  $\alpha = 10$  a good value and we also use  $\alpha = 0.09$  for invisible watermarking. We have also proposed a modification to make the watermark more robust.

### Insertion of Watermark

The steps for watermark insertion are discussed below:

- The original image I (to be watermarked) and the watermark image W are reading. (Both the images may be not of equal size).
- The watermark image resize if necessary to make it size the same of host image.
- The DCT coefficients for host image and watermark image are found out.
- The value of embedding factor defined to be suitable for visible watermarking.
- The DCT coefficient of the host image and watermark image is modified

### Simulation result

Figure 6 shows the 512x512 gray scale cover image Lena and 512x512 watermark copyright.



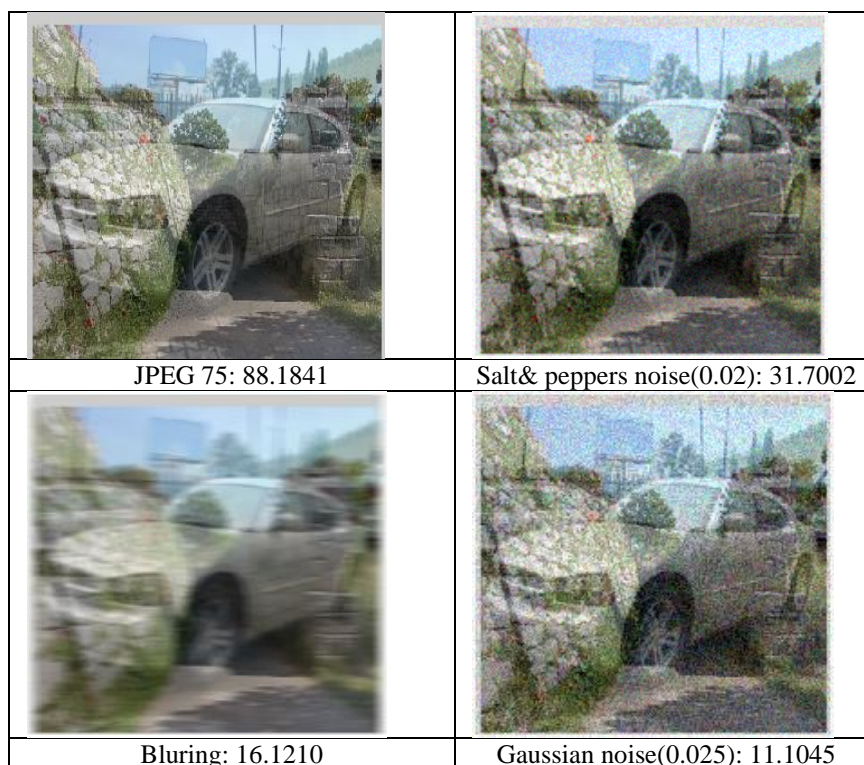
Figure 6: a) Host Image



b) Watermark Image

After running code and achieve desired result five types of attacks applied to the watermarked image. The attacked images are presented in Figure 7 together with the tools and parameters used for the attacks. The number next to the label below each image denotes the SNR value. Figure 13 contains the watermarks extracted from the watermarked for each of the attacks. The numbers next to the images are the SF values. According to

Figure 7 and Figure 13, it is possible to note the resistance of watermarked image for each attack using either subjective human evaluation or objective SF.



**Figure 7: Visible Watermarking**

## VI. CONCLUSION

In introduction we have general definition of digital image watermarking, our own work in watermarking start in experimental analysis using DWT first we decompose the host image into four bands LL, LH, HL and HH and we embedding the watermark in each band and with different values of QF and embedding factor we note that at QF=100 and alpha=0.09 we can retrieval the watermark image with SF=1, Figure 5a show watermarking image in different bands and we use SNR to compare between them, Figure 5b show extracted watermark from each band also we use SF to compare between them. Applying different type of attacks on watermarking image embedding on the LL band we record the result and note the effect of each type, LL band more robust to JPEG compression and intensity adjustment.

## REFERENCES

- [1] Mare S.F., Vladutiu M. and Prodan L., "Secret data communication system using steganography, AES and RSA", 17th International Symposium for Design and Technology in Electronic Packaging (SIITME), pp. 339-344, doi:10.1109/SIITME.2011.6102748,20-23 Oct. 2011.
- [2] Farahani M. R. D. and Pour mohammad A., "A DWT Based Perfect Secure and High Capacity Image Steganography Method", *International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, Taipei, pp. 314-317, 2013.
- [3] Wu K-S., "A secret image sharing scheme for light images", *EURASIP Journal on Advances in Signal Processing*, Springer, 49, <http://asp.eurasipjournals.com/content/2013/1/49>, 2013.
- [4] Ker A.D., Bas P., Bohme R., Coganne R., Craver S., Filler T., Fridrich J. and Pevny T., "Moving steganography and steganalysis from the laboratory into the real world", *Proceeding of the first ACM workshop on Information hiding and multimedia security (IH&MMSec '13)*, ACM, New York, NY, USA, 45-58. doi: <http://dx.doi.org/10.1145/2482513.2482965>, 2013.
- [5] Islam M. R., Siddiqa A., Md. Palash Uddin, A. K. Mandal and M. D. Hossain, "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", *International Conference on Informatics, Electronics & Vision (ICIEV)*, pp. 1-6, Dhaka, 2014.
- [6] Baykara M. and Das R., "A steganography application for secure data communication", *International Conference on Electronics, Computer and Computation (ICECCO)*, pp. 309-313, doi: 10.1109/ICECCO.2013.6718290, 7-9 November 2013.



- [7] Sirsikar S. and Salunkhe J., "Analysis of Data Hiding Using Digital Image Signal Processing", *International Conference on Electronic Systems, Signal Processing and Computing Technologies (ICESC)*, Nagpur, pp. 134-139, 2014.
- [8] Farahani M. R. D. and Pour mohammad A., "A DWT Based Perfect Secure and High Capacity Image Steganography Method", *International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, Taipei, pp. 314-317, 2013.
- [9] Iwakiri M. and Thanh T.M., "Fragile watermarking based on incomplete cryptography for copyright protection", *Applied Informatics*, Springer, 2:7 doi: 10.1186/s40535-015-0012-8, 2015.
- [10] Nyeem H., Boles W. and Boyd C., "Digital image watermarking: its formal model, fundamental properties and possible attacks", *EURASIP Journal on Advances in Signal Processing*, Springer, 135, <http://asp.eurasipjournals.com/content/2014/1/135>, 2014.
- [11] Stacey D., "Passive warden using statistical steganalysis", *Proceeding of the 3rd annual conference on Research in information technology (RIIT '14)*. ACM, New York, NY, USA, doi: pp. 27-32, <http://dx.doi.org/10.1145/2656434.2659756>, 2014.
- [12] Zielinska E., Mazurczyk W. and Szczypiorski K., "Trends in steganography", *Communication ACM* 57, 3 (March 2014), pp. 86-95, doi: <http://dx.doi.org/10.1145/2566590.2566610>, 2014.
- [13] H.Abdel-Nabi and A. Al-Haj, "Efficient joint encryption and data hiding algorithm for medical images security," *2017 8th International Conference on Information and Communication Systems (ICICS)*, Irbid, doi: 10.1109/IACS.2017.7921962, pp. 147-152, 2017.
- [14] Reddy H.S.M., Sathisha N., Kumari A. and Raja, K.B., "Secure steganography using hybrid domain technique", *3rd International Conference on Computing Communication & Networking Technologies (ICCCNT)*, pp. 1-11, doi: 10.1109/ICCCNT.2012.6396010, 26-28 July 2012
- [15] Ren-er Y., Zhiwei Z., Shun T. and Shilei D., "Image Steganography Combined with DES Encryption Pre-processing", *16th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*, pp. 323-326, doi: 10.1109/ICMTMA.2014.80, 10-11 January 2014.
- [16] Islam S., Modi M.R. and Gupta P., "Edge-based image steganography", *EURASIP Journal on Information Security*, vol. 2014:8, 2014.
- [17] I. Sikder, P. K. Dhar and T. Shimamura, "A semi-fragile watermarking method using slant transform and LU decomposition for image authentication," *2017 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Cox's Bazar, doi: 10.1109/ECACE.2017.7913027, pp. 881-885, 2017.
- [18] Ker A.D., "Know Your Steganographic Enemy", *Communications of the ACM*, Vol. 57, No. 5, doi:10.1145/2601402, May 2014.
- [19] Nam-Tuan Le and Yeong Min Jang, "Invisible embedded techniques for optical camera communications," *2017 International Conference on Information Networking (ICOIN)*, Da Nang, doi: 10.1109/ICOIN.2017.7899566, pp. 599-603, 2017.
- [20] Dagadita M.A., Slusanschi E.I. and Dobre R., "Data Hiding Using Steganography", *IEEE 12th International Symposium on in Parallel and Distributed Computing (ISPD)*, pp.159-166, doi: 10.1109/ISPD.2013.29, 27-30 June 2013.
- [21] R. K. Hemalatha and P. Maneesha, "Unified embedding method for color image steganography," *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, doi: 10.1109/ICICES.2016.751887, pp. 1-5, 2016.
- [22] D. Zheng, Y. Liu, J. Zhao, and A. E. Saddik, "A survey of RST invariant image watermarking algorithm," *ACM Comput. Surv.*, vol. 39, no. 2, pp. 1-91, Jun. 2007, Article 5.
- [23] J. O'Ruanaidh and T. Pun, "Rotation, scale, and translation invariant digital image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 303-317, 1998.
- [24] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans. Image Process.*, vol. 9, no. 6, pp. 1123-1129, Jun. 2000.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Narendra. M. Jathe." Image Security through Visible and Invisible Watermarking Techniques." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 10, 2019, pp. 01-09.