PERFORMANCE EVALUATION AND WATERMARK SECURITY ASSESSMENT OF DIGITAL WATERMARKING TECHNIQUES

Asim Naveed[1], Yasir Saleem[2], Nisar Ahmed[3], Aasia Rafiq[4]
[1]Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Narowal Campus, Pakistan.
[2,3]Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan.
[4]Department of Electrical Engineering, University of Engineering and Technology, Lahore, Pakistan.

[1]asimnaveed@uet.edu.pk, [2]yasir@uet.edu.pk, [3]nisarahmedrana@yahoo.com,[4]aasia03@gmail.com

ABSTRACT: *Swift growth of digital technologies has increased the requirement of ownership demonstration and copyright protection of digital media. Digital media can be reproduced easily and ownership demonstration in the form of digital watermark can serve the purpose of copyright protection. Numerous watermarking algorithms are presented in the literature but they lack evaluation on a common benchmark. Parameters for evaluation of performance and robustness of watermark are discussed and five popular transform domain and spatial domain techniques are analyzed and discussed. The goal of research is to provide a benchmark for evaluation of a watermarking technique and to introduce some improvements in their performance. A model for enhanced robustness and security of DFT based watermarking scheme is also proposed which can be further investigated for fulfillment of robustness, security and imperceptibility requirements.*

Key Words: watermarking, copyright protection, ownership demonstration, benchmark, evaluation.

1. INTRODUCTION

In 1993 Trikel used the term "Digital Watermarking" for the first time while presenting two technique for data hiding in digital images[1]. Realization of cost-effective internet, digital recording and storage media and availability of quality of service and greater bandwidth for wireless and wired network have made the creation, replication, transmission and distribution of digital media in an graceful way. Therefore, protection and implementation of intellectual property rights for such media has become of greater importance [2, 3]. Digital watermarking is a technology that insert perceptually transparent pattern (i.e. signal or watermark) in a digital media to ensure copyright protection, authentication and security. This pattern called "watermark" identify the additional properties about the image such as image owner or a particular customer to ensure image integrity. Watermark is detected and extracted from the original image to achieve copy prevention, broadcast monitoring, authentication, data hiding and as a proof of ownership [3].

Cryptographic techniques such as encryption are existing for prevention of unauthorized access to digital images. Nevertheless, image encryption has its limitation in protection of intellectual property rights once an authorized person decrypts it. One can do nothing for prevention of unauthorized replication once they get the decrypted image. An additional technology is required to provide authentication and verification method for ownership rights. This technology must verify ownership rights, track content usage, safeguard authorization, prevent illegal copying and facilitate its authentication [4].

It is evident that both encryption and digital watermarking are complementing technologies and are required as a complete security solution for multimedia data. Various data hiding and image security techniques have been developed for color and grayscale images [4]. Majority of those techniques perform minor modification to the color or luminosity values of the specific set of pixels to perform watermarking. This modification is done in such a way to prevent images from visible degradation.

A detection and extraction algorithm along with key can extract the embedded pattern or watermark. Robustness is an important property of watermark that ensures watermark is readable even after slight deterioration or common image processing o.perations. These image-processing operations may involve filtering, lossy and lossless compression, histogram manipulation, addition of noise and different geometric transformation. Watermarks specifically designed for copyright protection, access control or fingerprint must also be embedded in a confident way. The attacker with the knowledge of embedding algorithm must not be able to disrupt the watermark beyond detection.

There is a tradeoff between robustness and capacity of the watermark. The watermark can contain as low as one bit up to several hundred bits. Computational complexity of embedding and extraction algorithm is another important attribute. In several applications, there is a need of fast and simple embedding algorithm while the extraction may be computationally expensive. One such example is watermarking digital camera images for temper detection. In some other applications speed of extraction is extremely decisive such as caption extraction in digital videos.

1.1. Applications of Watermarking

Watermarking schemes are designed based on some specific application. A particular application has its own usefulness that may have a parameter of drawback for some other application. Temper detection is used in digital cameras to insert a fragile watermark for temper detection whereas the same fragility is a disadvantage in intellectual property protection application. These application range from data hiding to information integration, intellectual property rights protection, ownership demonstration and temper detection [1].

1.2. Elements of a Watermarking System

A watermarking system is considered as a communication system whose model is based on three parts; transmitter, communication channel and receiver as illustrated in Figure 1.

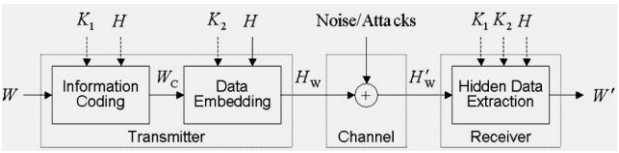

Figure 1 Model of watermarking system

Transmitter part performs the coding and watermark embedding in the cover image. Channel may be the transmission channel or storage space. All the attacks and impairments occur in this part. These attacks and impairments can be intentional by an intruder or unintentional such as bitt error or data corruption. Receiver channel performs the watermark detection or extraction for authentication purpose.

2. EXISTING WORK

Four important class of watermarking are discussed and analyzed based on the proposed evaluation criteria. They include one spatial domain technique and three transform domain watermark embedding techniques. Following subsections provide brief explanation of their working principle.

2.1. DCT based watermarking

In discrete cosine transform (DCT) based watermarking, the image is divided into 8x8 blocks and DCT transformed. Some blocks are selected based on some criteria. Highest frequency coefficients are selected from these blocks modify them according to watermark. Different frequency coefficients are robust against different types of attacks [5]. It has better robustness against noise, filtering, sharpening and tempering and is computationally less expensive then other transform domain techniques [6].

2.2. DFT based watermarking

Discrete Fourier Transform based watermarking is computationally more expensive than DCT but provide more robustness as it not only incorporate cosine but also the imaginary sine components [7]. DFT based embedding involves direct watermark embedding and template based embedding. In direct embedding approach, magnitude and phase coefficient of DFT is modified according to watermark. In template based embedding, the watermark is embedded in the form of a template to estimate transformation factor. It is robust against geometric attacks like scaling, shearing, translation and rotation along with cropping and tempering [8].

2.3. DWT based watermarking

Discrete wavelet transform (DWT) represent an image in the form of multi-resolution image [9]. Input image is decomposed into four regions of high and low frequencies and the lowest frequency region is further divided to four such region until the image is entirely decomposed. The lowest frequency components contain important components of image so are more robust to many attacks but introduce little more distortion into watermarked image [10]. This type of watermarking is computationally more expensive then DCT but less than DFT. It has better robustness DWT based image compression and to noise, half-toning and rescaling over the other techniques [11].

2.4. Linear Binary Pattern

In this approach [12] the authors has exploited Local binary pattern (LBP) operators for watermark embedding and extraction. LBP were previously used for visual inspection, texture analysis and image retrieval applications. It computes the LBP by dividing an image to blocks of certain size say 3x3 and check if the center pixel is greater or lesser then then the neighbor. The neighbors are checked in a circle like counter-clockwise and if the center pixel is greater 1 is placed otherwise a 0 is placed and an 8bit LBP vector is obtained. Following three parameters are calculated from LBP vector;

$$g_p = \{g_i | i = 0, \cdots, c, \cdots, P-1\}$$
$$m_p = \{m_i | m_i = |g_i - g_c|, i = 0, \cdots, P-1\}$$
$$S_p = \{s_i | s_i = sign(g_i - g_c), i = 0, \cdots, P-1\}$$

For watermark embedding, two Boolean functions are applied on sign vector S_p

$$f_{\oplus}(S_p) = S_0 \oplus S_1 \oplus \cdots \oplus S_{p-1}$$
$$f(S_p) = Bool(1(S_p) - 0(S_p) > N)$$

The value of S_p is changed according to watermark by selecting minimum value of m_p, it is chosen in order to minimize the change in cover image. The corresponding change is performed in spatial pixel at the same location. An advantage of algorithm is, it can locate the location of temper from watermark as the distortion occurred in corresponding LBP vectors.

3. EVALUATION OF WATERMARKING SCHEMES

Many watermarking techniques are available but their use is restricted to specific areas. An evaluation metrics is needed to assess the performance and watermark security of a watermarking algorithm. A criteria which will analyses the watermarking scheme based on its most popular applications. Following are functions for assessment of performance and security of watermarking schemes.

3.1. Imperceptibility

Imperceptibility refers to the quality of watermarked media as noticed visually. Hence, imperceptibility depends on human visual system. Since digital watermarking embeds the watermark into a cover, image and is not directly visible to observer. Obviously, there would be distortion introduced to the digital watermarked content caused by embedding process. It is therefore desirable that an algorithm used for watermarking should add minimal distortions to the digital content.

For image perceptibility, popular evaluation criteria are based on mean-square error (MSE), Euclidean distance (ED), peak-signal-to-noise ratio (PSNR) and normalized correction (NC) [1, 2]. These parameters are explained below.

3.2. Mean Squared Error (MSE)

It is a method to check distortions between cover image and watermarked image. With the calculation of mean square error, we can detect any change in the watermarked image. Table 1 provides the result of MSE for three test images.

Here, X denotes the cover image and X* denotes the watermarked data.

$$M.S.E = \frac{1}{n}\sum_{i=1}^{n}(X_{i-}X_i^*)^2$$

Table 1 Mean square error computations for three test images.

Image	**FFT**	**DCT**	**DWT**	**LBP**
Archer	0.11186	0.35143	12.1249	0.042121
Glider	0.08416	0.28941	12.6919	0.039715
Tractor	0.129869	0.41043	9.52276	0.051961

3.3. Euclidean distance (ED)

Euclidean distance is common distance between two points in a Euclidean space. For images, two-dimensional Euclidean distance is used. Some of the specialized image Euclidean distance algorithms are also presented by the basic idea can be covered by two-dimensional Euclidean distance. Table 2 provides the results of ED for the three test images for comparison. Following formula is used to calculate Euclidean distance between two images.

$$ED(X,X') = \sum_{i=1}^{M}.\sum_{j=1}^{N}(X_{(i,j)} - X'_{(i,j)})^2$$

Table 2Eucledian distance computations for three test images

Image	**FFT**	**DCT**	**DWT**	**LBP**
Archer	106858	663410	1756321	44671
Glider	69443	116904	929019	646
Tractor	114196	171323	2515317	39362

3.4. Peak-Signal-to-Noise Ratio

PSNR is a better test to check distortions between original image and watermarked image because it uses mean squared error also. We can calculate PSNR by the following formula.

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

PSNR is most usually used to check the nature of remaking of lossy image. The image for this situation is the information, and the noise is the error. PSNR is an estimate to human view of reproduction quality. In spite of the fact that a higher PSNR shows that the recreation of image is of higher quality, sometimes it may not. Table 3 provides the results of PSNR calculation for the three test images.

Table 3 PSNR computations for three test images

Image	**FFT**	**DCT**	**DWT**	**LBP**
Archer	57.6437	52.6724	37.294	61.8859
Glider	58.88	53.5156	37.0955	62.1413
Tractor	56.9958	51.9984	38.3432	60.9740

3.5. Normalized Correction

Normalized correction is a measure of similarity of two images as a function of a time-lag applied to one of them. Table 4 provides the results of NC for the test images. Following formula is used to calculate normalized correction for two images.

$$NC(X,X') = \sum_{i}^{M}.\sum_{j}^{N}\frac{X_{(i,j)} * X'_{(i,j)}}{\sum_i^M.\sum_j^N(X_{(i,j)})^2}$$

Additionally, Hamming distance, bit correct rate (BCR) and bit error rate (BER) are used for binary images. These measures can be used to measure the accuracy of recovered watermark quantitatively. There formulas are provided below.

$$HD(Y,Y') = \sum_{i}^{M}.\sum_{j}^{N}\left|Y_{(i,j)} - Y'_{(i,j)}\right|$$

$$BER(Y,Y') = \frac{HD(Y,Y')}{M*N}X\ 100\%$$

$$BCR(Y,Y') = \left(1 - \frac{HD(Y,Y')}{M*N}\right)X\ 100\%$$

Here,
Y = original image & Y' = processed image,
M = width of the image & N = height of the image
Y(i, j) = pixel position at (i, j) location of Y & Y'(i, j) = pixel position at (i, j) location of Y'.

Table 4 Normalized Correction computations for three test images

Image	**FFT**	**DCT**	**DWT**	**LBP**
Archer	1.0000	1.0000	1.0011	1.0006
Glider	1.0000	0.9998	1.0006	1.0009
Tractor	1.0000	0.9998	1.0015	1.0008

3.6. Structural Similarity Index (SSIM)

The structural similarity index measure the similarity between two images based on perceived change in image structure [13]. It is a full reference metric to replace the shortcoming of PSNR and other image quality metrics. The structural perception is made based on pixels interdependence with its neighboring pixels making it a better measure then PSNR and MSE, which calculate the perceived error in specific pixels. Neighboring pixel dependencies contain important information about the structural content of image. It is superior to PSNR in some cases but perform just the same in the other cases.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(u_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

μ_x the average of x & μ_y the average of y.
σ_x^2 the variance of x & σ_y^2 the variance of y
σ_{xy} the covariance of x and y
$c_1 = (k_1L)^2, c_2 = (k_2L)^2$ two variables to stabilize the division with weak denominator

Table 5 SSIM computation results for three test images

Image	**FFT**	**DCT**	**DWT**	**LBP**
Archer	0.9981	0.9818	0.9713	0.9888
Glider	0.9984	0.9980	0.9798	0.9832
Tractor	0.9983	0.9971	0.9661	0.9831

3.7. Robustness

It is a property to check resistance against any external attacks. Now a day in many applications the strength of the watermarked image to bear noise is important. The researchers can check robustness of watermarked image through doing attacks on watermarked image, by this way they can measure the strength of robustness. With the help of experiments we can say that a strong robustness means that a watermarked image has degraded their visual quality.
That watermark robustness is the term for your ability of a specific watermarking structure to detect and as well extract the particular embedded watermark from standard processing procedure may be applied toward data, with or without intent for you to counteract detection from the embedded watermark.
Powerful watermarks are needed to remain within the watermarked image despite many specialists have mauled. The attacks may very well be hostile attacks such as

statistical averaging, point out processing, watermark analysis and doing away with, watermark counterfeiting. The attacks can be casual or perhaps unintended attacks which are routine photograph processing such as filtering, compression setting, running, cropping. Some of the important attacks, which must be tested for analysis of a watermarking scheme, are provided below.

3.7.1. Compression Attack

Compression attack is an important metrics to perform for robustness testing as almost all type of images goes to some type of compression before transmission or storage. Lossy compression usually result in loss of data so it must be checked either a scheme withstand lossy compression or not. JPEG compression is used at different quality factors and then watermark is recovered from the image. A readable recovered watermark shows permanence to compression attack. Figure 3 (a) contain the image with compression attack and figure 4-7 (a) contain the logo extraction from the corresponding watermarked image.

3.7.2. Noise Attack

In multimedia communication, channel noise is the most unavoidable noise especially in wireless communication. Simulated noise can be added to watermarked image and later the watermark will be extracted for analysis. Gaussian, Poisson, Salt & Pepper, and Speckle are among the noises that could be used for this purpose. Additive white Gaussian Noise (AWGN) is simulated and quality of recovered watermark is analyzed to check the resistance to noise. Figure 3 (b) contain the image with additive white Gaussian noise with mean 0 and variance 0.01 and figure 4-7 (b) contain the logo extraction from the corresponding watermarked image.

3.7.3. Cropping

Some parts of the watermarked image are cropped and the message signal is extracted from the watermarked image. If the extraction algorithm is non-blind, it's better to join cropped parts of the image for better recovery of the message. Figure 3 (c) contain the image with lower quarter region cropped and figure 4-7 (c) contain the logo extraction from the corresponding watermarked image.

3.7.4. Blurring

Blurring is a common operation, which is performed to destroy the watermark. Slight blurring reduce the visual quality of image marginally however, intense blurring (more number of operations or larger kernel size) can affect the visual perceptibility of image. Figure 3 (d) contain the image blurred with 3×3 kernel and figure 4-7 (d) contain the logo extraction from the corresponding watermarked image.

3.7.5. Gamma Correction

Gamma correction is performed to adjust the brightness of image. Value of gamma exponent is varied to affect the quality of watermark. Figure 3 (e) contain the gamma corrected image with γ=5 and figure 4-7 (e) contain the logo extraction from the corresponding watermarked image.

3.7.6. Permutation of Pixels

Pixel permutation (scrambling) can be performed to reorder the position of image pixel to destroy the watermark. Permutation block size define how finely the pixels are permuted. Figure 3 (f) contain permuted image with Mersenne twister and figure 4-7 (f) contain the logo extraction from the corresponding watermarked image.

3.7.7. Median Filtering

Median filtering is a commonly used method to remove noise. Salt & paper noise is most efficiently removed by median filtering. Kernel size will define the effect of filtering on watermark. Figure 3 (g) contain image median filtered with 3×3kernel and figure 4-7 (g) contain the logo extraction from the corresponding watermarked image.

3.7.8. Histogram Equalization

Histogram equalization distributes the image histogram to complete scale for an even distribution of brightness of pixels. Image contrast is reasonable improved in most cases. The effect of histogram equalization of watermark is mainly based on histogram distribution of image before the test. Figure 3 (h) contain histogram equalized image and figure 4-7 (h) contain the logo extraction from the corresponding watermarked image.

3.7.9. Rotation

Rotation does not cause the change in pixel values of the image but it change their position entirely as it is in permutation. The image remain exactly the same but watermark discovery becomes difficult. Figure 3 (i) contain image rotated at 45 degrees and figure 4-7 (i) contain the logo extraction from the corresponding watermarked image.

3.8. Capacity

Capacity represents the amount of bits, which can be embedded to a watermarked media by the water marking algorithm. Capacity is directly proportional to the number of bits added by the algorithm to the cover image. Nevertheless, it is a common observation that the quality of watermarked image is degraded with the increase in number of bits added by the algorithm. Hence, capacity and perceptibility are inversely related.

3.9. Security

Security is related with the strength of embedded watermark protection in watermarked media. The security is assessed on the basis of length of time it takes to break the watermarking algorithm and reveal the hidden watermark.

(a) (b)

Figure 2 (a) Original Archer Image (b) watermark (UET Logo)

(a) (b) (c)

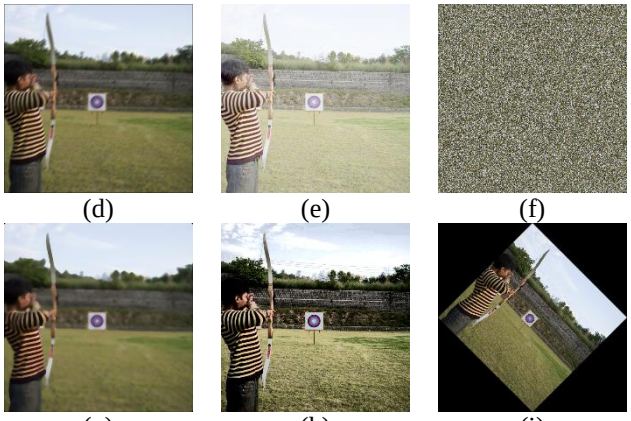

Figure 3 (a) Compressed at QF 90. (b) AWGN with mean 0 and variance 0.005. (c) Cropped by 1/4. (d) Motion blur simulated by 3×3 kernel. (e) Gamma correction at γ=5. (f) Permuted at pixel level. (g) Median filtering with 9×9-kernel size. (h) Histogram equalized image (i) Rotated at -45^o.

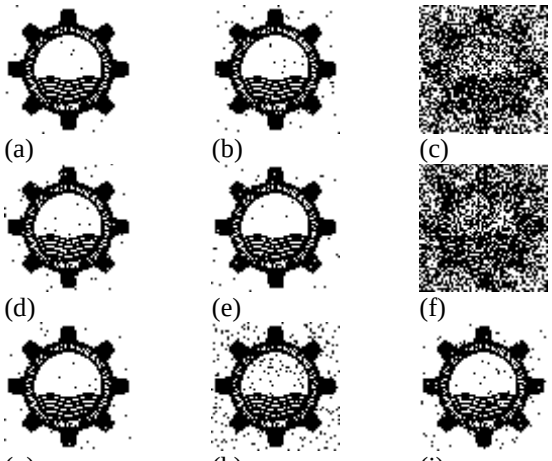

Figure 4 Watermark recovery results for DFT based technique

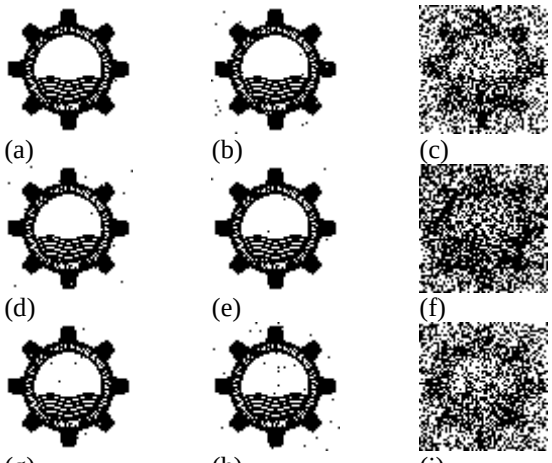

Figure 5 Watermark recovery results for DCT based technique

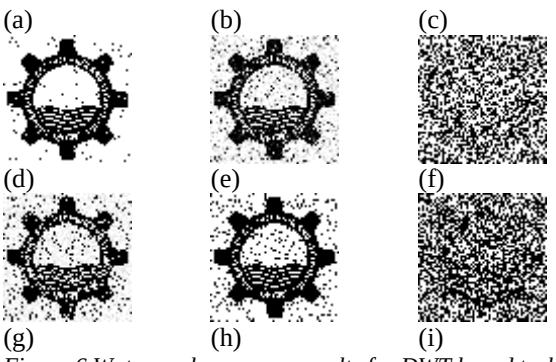

Figure 6 Watermark recovery results for DWT based technique

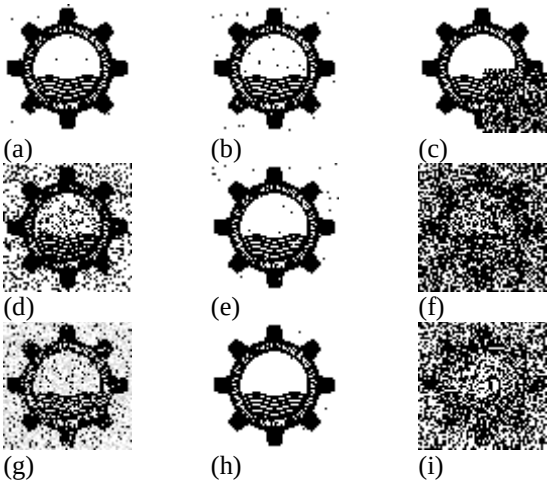

Figure 7 Watermark recovery result for LBP based technique

4. DISCUSSION

The watermarked image quality has been assessed on the basis of five quality parameters. The spatial domain technique LBP has shown minimum error in MSE test whereas wavelet based technique has shown maximum mean squared error. The same relation holds in Euclidian distance as the wavelet based technique has shown maximum deviation and LBP has shown minimum. The results of PSNR also correlated with MSE. Whereas in normalized correction test, the DWT based technique has still shown the maximum deviation but minimum deviation is shown by DFT based technique. Structural similarity index has shown the similar trend by nominating DFT based technique for minimum distortion and DWT based for maximum distortion. None of these techniques has shown robustness against permutation. Only DFT based technique has shown some robustness against geometric distortion attack. Cropping attack has also resulted in severe degradation except in case of LBP where only the corresponding cropped or tempered area has shown some distortion.

4.1. Suggestions

The results of analysis has shown the DFT based techniques, despite of having high computational complexity, has better robustness. These techniques can be further improved to obtain more robust watermarking techniques. LBP based technique has also shown reasonable robustness against some attacks and provided localization of tempering. It can also survive minor cropping as only the corresponding cropped region of the watermark will be distorted.

The watermark insertion process in DFT based watermarking scheme can be improved for more robustness and security at slightly decreased imperceptibility. Following steps can be incorporated for enhanced performance.

a. Divide the DFT of cover image in four equal parts.
b. Create a scrambled watermark matrix based on some pseudorandom sequence for enhanced security.
c. Create a band size, based on length of pseudorandom sequence and image size.
d. Insert the watermark matrix in lower frequencies of DFT in a circular fashion with a scaling factor α_1.
e. Insert the same watermark in higher frequencies with a scaling factor α_2.
f. Make sure $\alpha_2 < \alpha_1$ as DFT coefficient at higher frequencies has lesser magnitude.

Watermark insertion process based on above strategy will be more robust then the simple DFT based watermarking scheme. On set of attacks (geometric and cropping) will be resisted by high frequency watermark whereas the other set of attacks (JPEG compression, AWGN, filtering (blurring, denoising etc.), gamma correction and histogram equalization will be resisted by watermark at lower frequencies. More severe attacks can make it difficult to extract watermark but it can still serve the purpose of authentication by watermark detection.

5. CONCLUSION

The paper discusses five image quality analysis criteria to quantify the quality of watermarked image. The same test is applied to judge the watermarked image quality done by four different techniques. LBP based technique has shown minimum deviation against Euclidian distance, mean squared error and peak signal to noise ratio. Whereas DFT based watermarking scheme has provided better results against normalized correction and structural similarity index. Wavelet based watermarking technique has shown power image quality against all test. In robustness analysis, DFT based technique has comparatively better performance against different attacks. Technique based on LBP has shown reasonable performance against several attacks but is better suited for localization of tempering. DWT based watermark embedding technique is not secure enough neither it provide good imperceptibility so need to explore further dimension to embed watermark. The research can be further extended to investigate DFT based techniques and construct a technique with superior robustness to satisfy all the requirements of a robust watermarking system.

REFERENCES

1. Barni, M. and F. Bartolini, "Watermarking systems engineering: enabling digital assets security and other applications", *CRC Press*: (2004).
2. Lu, C.-S., "Multimedia security: steganography and digital watermarking techniques for protection of intellectual property", *IGI Global*: (2005).
3. Ahmed, H.E.-d.H., H.M. Kalash, and O.S.F. Allah, "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images" in *Electrical Engineering, 2007. ICEE'07. International Conference on*, IEEE: (2007).
4. Nisar Ahmed Rana, M.G., "Image Encryption: With MATLAB Implementation", LAP Lambert Academic Publishing **1**(1): (2012).
5. Barni, M., et al., "A DCT-domain system for robust image watermarking" *Signal processing*, **66**(3): p. 357-372 (1998).
6. Lin, S.D., S.-C. Shie, and J.Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression*" Computer Standards & Interfaces*, **32**(1): p. 54-60 (2010).
7. Piva, A., et al., "Improving dft watermarking robustness through optimum detection and synchronization*" GMD Report*, **85**: p. 65-69 (1999).
8. Xiao-dan, Z., "Research on Watermarking Algorithm of Strong Robustness Based on DFT*" Journal of Chongqing Normal University (Natural Science)*, **6**(1): p. 016 (2010).
9. Daren, H., et al. "A DWT-based image watermarking algorithm" in *Proceedings of the IEEE International Conference on Multimedia and Expo*. (2001).
10. Chan, P.-W. and M.R. Lyu, "A DWT-based digital video watermarking scheme with error correcting code", in *Information and Communications Security*, Springer. p. 202-213 (2003).
11. Mohidul Islam, S., R. Debnath, and S. Alamgir Hossain, "DWT based digital watermarking technique and its robustness on image rotation, scaling, JPEG compression, cropping and multiple watermarking", in *Information and Communication Technology, ICICT'07. International Conference on*. 2007. IEEE, (*2007).*
12. Wenyin, Z. and F.Y. Shih, "Semi-fragile spatial watermarking based on local binary pattern operators*", Optics Communications*, **284**(16): p. 3904-3912 (2011)
13. Hore, A. and D. Ziou, "*Image Quality Metrics: PSNR vs. SSIM*", in *ICPR*, (2010)