A Review on Digital Image Watermarking Techniques: An Intellectual and Sophisticated Analysis to find out the Best Implementable Scheme

Abhinav Sharma
B.Tech - CSE
Amity University, Noida

Arunima Jaiswal
Assistant Professor
Amity University, Noida

ABSTRACT

With the advent of internet and communication transmitting abilities, cyber-crime and piracy has increased in a tremendous rate leading to widely accepted claim that digital data is highly vulnerable and requires extremely secure procedures for data availability throughout the network connections. Due to this increasing demand for enhanced security measures, Digital watermarking provides the most efficient solution for securing copyrights and reducing vulnerability among the digital data transmission scenarios. This paper introduces the most reliable and widely acceptable techniques for Digital Watermarking on images and focuses on providing the conclusion regarding the best technique to be implemented for most secure mechanism. For this conclusion, I have implemented certain statistical comparison measures against performance and robustness capabilities of the techniques in order to find most reliable implementation and eventually provides conclusive remarks for future techniques to be invented.

General Terms

Digital Image Processing, Digital Watermarking, Image Processing, Security, Algorithms, Analysis.

Keywords

LSB (Least Significant Bit), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), PSNR (Peak-to-Signal Noise Ratio), NCC (Normalized Cross Correlation), SSIM (Structural Similarity Index Measure), MAE (Mean Absolute Error), RGB (Red-Green-Blue)

1. INTRODUCTION

With the advent of technological environment, the extent of security mechanisms that are required to introduce for preserving the resources are increasing tremendously. The demand of securing the digital data is strongly under consideration, and the solutions for the demand is still lacking in great amount. The digital data such as video, audio, image, 3D models, and other, is in great threat under several issues such as copyright infringement, owner violations, etc. Due to this, there is widespread demand for securing this data from potential threat and enabling better threat disabling scenarios.

In order to serve and neutralize these demands for better security principles and implementation, Digital Watermarking was introduced.

Digital Watermarking is a technique of hiding private and vulnerable data behind any non-essential data, such that the hiding mechanism is efficient and corresponding output will be imperceptible to human eyes. This technique has most prominent application in digital images where security leaks such as copyright infringement and violation cases can be avoided.

Digital Image Watermarking technique can be divided into two broad categories on the basis of working domain:

1. Spatial Domain
2. Transform Domain

Spatial Domain techniques are based on modifying the pixels of image for hiding and storing the vulnerable data. These pixels are modified [6] in a manner that does not entirely affect the host image and encrypted content is inserted on those selective pixels of the image. These techniques are not considered to be secure and efficient as compared to transform domain techniques.

On the other hand, transform Domain techniques are not based on altering the pixels of the images according to different bit patterns. In this scheme, the entire image is converted into frequency domain [7] using transformations like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). After conversion, vulnerable and private data is inserted into these generated frequency domains using certain transformation procedures. This technique is considered to be secure due to imperceptibility introduced by the fact that human eyes are not sensitive towards frequency alterations.

The goal of this paper is to introduce different watermarking techniques in these respective domains and implement different analytical procedures to establish statistical comparison among these techniques. This will eventually provide conclusive result to declare the best among the presented techniques.

1.1 Background Information

Digital watermarking is a concept of hiding the creator’s or owner’s information behind the vulnerable data, so to protect it from emulating or tampered to be used in some other forms.

The watermarking technique was in consideration since 1282, when demands of copyrights was first taken into action.

1. In 1282, paper watermarks creation was first initiated, where different image patterns with difference in intensity and lighting was introduced in a piece of paper for better protection of creations, or to identify the creator of the masterpiece.
2. In 1779, the word ‘Counterfeiting’ was first coined due to increase in piracy cases and infringement of analog data was found. This counterfeiting takes into account one of most tragic event in congress of

US, where several counterfeit bills were encountered in place of legal ones in congenital congress, showing greater concern in introducing better security in confidential data.

3. In 1954, watermarking music tapes and records was under consideration, due to steal and re-use of creations of musical aspects, tones and lyrical usage was found in similar looking tracks leading to lot of controversies regarding the correct owner and creator of data.
4. In 1988, 'Digital watermarking' term was first coined and used for securing the digital data and decrease the cases of digital counterfeiting or copyright infringements.
5. End of 1990s, Digital watermarking several papers was introduced, researched and described in several conferences, leading to extreme popularity and increased interest among people.

1.2 Organization of the paper

This Paper is organized into different sections. First, the topic is introduced with basic details and goals for this survey. Then, the next section introduces the watermarking framework with techniques in different working domain. Afterwards, introduced techniques will be analyzed on the basis of performance and robustness. And eventually, results and discussions will be presented thereby declaring the conclusive outcomes.

2. WATERMARKING FRAMEWORK

Digital Watermarking is the concept of embedding the digital data that is required to be secured in non-essential candidate, which can later to be extracted from the same. Thus, the watermarking framework is implemented using three basic concepts. Figure 3 depicts the watermarking framework.

2.1 Embedding:

Embedding is the concept of combining two different entities together for introducing imperceptibility and hiding the vulnerable data behind non-susceptible data. This concept can be implemented using any working domain techniques, where transform domain provides the best embedding outcomes.

2.2 Attacks:

After embedding has be successfully implemented on the digital data, modifications are made in order to check the robustness for the watermarking procedures. Modifications made to a signal, are called Attacks [1]. Using these Attacks, watermarking securing capability can be established, thereby finding the most reliable technique for the same.

2.3 Extraction:

Extraction is a concept of extracting watermarking from the embedded digital data. Watermark can only be extracted using the reverse procedure of embedding, thereby introducing security principles for the digital data. Hence, watermark extraction requires pre-requisite knowledge which eventually protects and ensures the copyrights for such encrypted data.

3. DIGITAL IMAGE WATERMARKING TECHNIQUES

The watermarking framework can be implemented in order to hide data in images using different spatial and transform domain techniques. These techniques can be explained as:

3.1 Least-Significant Bit (LSB)

Least Significant Bit [2] is a spatial domain digital image watermarking technique which modifies the actual pixels of the image in order to hide digital data inside the host image. This technique implements the concept of Least Significant Bit, which the right-most bit of any bit pattern.

In order to implement this scheme, image is first converted into RGB scale in order to extract the matrix bit pattern for the image. Afterwards, the bits of encrypted message is placed in Least Significant Bits of the image, thereby storing the data and incorporating minimal changes in the respective image. The message can be easily extracted from the host image, by getting the values in LSB of image and combining them together to get the required data.

This scheme is not considered to be secure, due to its simple and bit-value scheme. Moreover, it is highly susceptible to attacks, which can easily damage the encrypted text in the image. The LSB scheme can be shown using the below depicted design scheme.

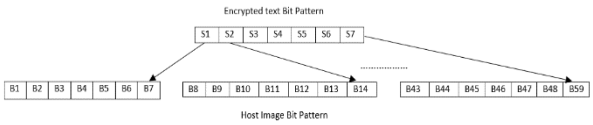


Figure 1: LSB Technique

3.2 DCT (Discrete Cosine Transform)

Discrete Cosine Transform [3] is a transform domain image watermarking technique that does not modify any pixels of the image in order to hide the vulnerable data. It uses highly reliable technique of converting the image into frequency domains and hiding the data in these frequency domains, thereby making the private data imperceptible to human eyes.

DCT creates different frequency domains or bands which can be categorized as: Low-frequency band (FL), Medium-frequency band (FM) and High-frequency band (FH). The encrypted data is hidden under these bands depending upon the coefficient values, which decide the selection of the band to be used for hiding the data. From several results obtained using this scheme, it is considered to be most reliable and efficient scenario by choosing FM band for hiding the digital message. Under this band, modifications do not affect the quality of the image, whereas hiding data in other bands, can lead to damage in quality after implementing certain modifications. Conclusively, this technique can survive attacks such as Gaussian noise or salt-pepper noise, hence considered to be much reliable then spatial domain techniques. The corresponding frequency domains of DCT can be shown as:

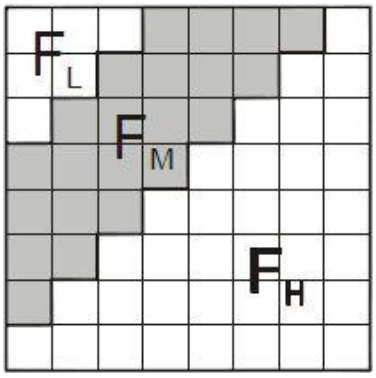


Figure 2: DCT frequency bands of 8x8 Block

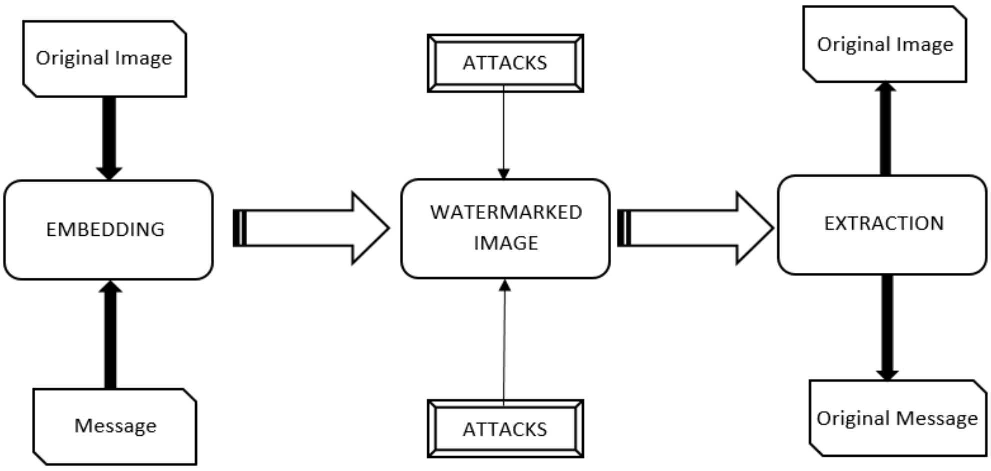


Figure 3: Watermarking Framework

3.3 DWT (Discrete Wavelet Transform)

Discrete Wavelet Transform [4] is another transform domain image watermarking technique which implements the same concept of converting image into different frequency domain using certain transformation logic, in order to hide the required message into these generated frequency domains.

In this technique, the image is divided into different components rather than bands of DCT. These components are declared as: LL (Lower resolution component), HL (Horizontal component), LH (Vertical component) and HH (Diagonal Component). This breaking process of creating different components of images can be implemented again and again in order to create multi-level wavelet transformation. Hence, there can be 2-level, 3-level, 4-level, and so on wavelet transformations depending upon component breaking scenarios. These components are thereby used to store the vulnerable message efficiently and effectively.

DWT is considered to be highly secured procedure, as different modifications does not affect the quality of the image and imperceptibility of the image is sustained during the embedding and extraction procedure. 2-level wavelet discrete transformation components can be shown as:

LL_2	HL_2	HL_1
LH_2	HH_2	
LH_1		HH_1

Figure 4: 2-Level DWT Components

4. PERFORMANCE ANALYSIS

The Performance Analysis [5] is an analytical technique of computing and evaluating performance parameters in order to find out the most suitable and sustainable procedures for specific circumstances. This analysis is implemented for different digital image watermarking techniques in order to evaluate performance factors and finding out the best performing technique under specified conditions and scenarios.

In order to analyze different techniques for performance, certain parameters are required. These parameters can be described as:

4.1 Execution Time

This is one of the most important performance parameter, as it decides the implementing procedure speed with respect to time. This is the only parameter that compares the working of the process taking into consideration the time and CPU cycles used to implement embedding and extraction process. It can be easily computed using this equation:

Start_time = CPUtime
Time_taken = CPUtime - Start_time

4.2 Peak-Signal Noise Ratio (PSNR)

PSNR is another performance calculating parameter which is used generally to evaluate the perceptibility of the image i.e. the similarity between original image and watermarked image. It can also be used to check similarity between original message and extracted message, so as to check the reliability of the respective procedure. It is declared that higher the value of PSNR, the better is the chances of imperceptibility for the human eyes, or better the message stored inside the host image.

PSNR can be calculated using the following formulae. It uses MSE (Mean square error) for computation:

$$\textbf{PSNR} = 10 \log_{10} (255^2 / \textbf{MSE})$$

PSNR is a ratio between maximum possible powers of signal to corrupted noise which can be computed using MSE. 255 pixels represent maximum possible power of signal. MSE can be computed as:

MSE = [∑Ni=1∑Nj=1(X(i,j) - Xw(i,j))2] / N2

Where, N represents number of rows and columns and X(i,j) represents original image pixel and Xw(i,j) represents watermarked image pixel.

4.3 Normalized Cross Correlation (NCC)

This technique is another performance calculating parameter which evaluates the similarity between original image and watermarked image. It can also be used for extracted message comparison scenarios. Again, higher the value of NCC, higher is the similarity chances. This parameter can be calculated as:

$$\mathbf{NCC = \sum i \sum j\ (\ I(i,j) - Iw(i,j)) \ / \sum i \sum j\ (\ I(i,j) + Iw(i,j))}$$

where, I(i,j) represents the original image pixels and Iw(i,j) represents watermarked image pixels.

4.4 Structural Similarity Index Measure (SSIM)

SSIM is another performance evaluating parameter that calculates the similarity index between original image and embedded image in order to analyze the sustainability and perceptibility of the image. It can also be implemented for checking similarity value between extracted message and original message. It is considered to be more improved way of finding similarity then PSNR and MSE. SSIM values lie between -1 and 1, where 0 value declares that two images are identical. It can be calculated as:

$$\mathbf{SSIM(x,y)=(2\mu x\mu y+)(2\sigma xy+C2)\ /(\mu x2+\mu y2+C1)(\sigma x2+\sigma y2+C2)}$$

Where, µx is the average of x, µy is the average of y, σxy is the co-variance of x and y, C1 and C2 are constants, σx is the variance of x and σy is the variance of y.

The performance can be efficiently analyzed using these respective parameters and it is broadly depicted in the table 1, with all the respective values calculated using same image and message to be embedded and extracted.

5. ROBUSTNESS ANALYSIS

Robustness defines the ability to resist changes even after excessive modifications on images. Images with hidden messages can be easily tempered using modification, thereby discouraging the real feature and goal of digital image watermarking implementation. Hence, this analysis is incorporated in order to identify and evaluate the robustness of different techniques used in order to create watermarked images. Those images which can resist modifications and provide the similar message after extraction, are considered to be robust and the implemented technique is considered to be efficient and secure.

Robustness can be analyzed by evaluating different techniques under certain circumstances of modifications. These circumstances can be created by attacking the watermarked image, which contains the hidden message. These attacks can be described as:

1. Rotation: Using this attack, the watermarked image is rotated by 180° and then hidden message is extracted.

2. Blurring: Using this attack, the watermarked image is blurred at certain angle, and then hidden message is extracted.

3. Cropping: The watermarked image is cropped with certain dimension, and then extraction procedure is implemented.

4. Gaussian Noise: The watermarked image is introduced with Gaussian noise with mean of 0.1 and variance of 0.5, and then extraction takes place.

5. Salt pepper Noise: The watermarked image is introduced with salt pepper noise, with the density of 0.5, and then extraction is implemented.

6. Scaling: The watermarked image is scaled to 50% of its size, and then message is extracted.

Mean Absolute Error (MAE) and PSNR is calculated after these modifications, between original and extracted message and the corresponding results are depicted in Table 2, with respect to different image watermarking techniques.

6. RESULTS AND DISCUSSION

In order to find the most efficient and sustainable technique among several digital watermarking techniques, I have implemented embedding and extraction mechanism on the image and respective message using Matlab 2014a.

The watermark is created using different techniques on the basis of working domain such as spatial and transform domain. The watermarking schemes are thereby inspected for performance and robustness analysis by calculating different performance parameters such as PSNR,NCC, etc. and by implementing different attacks on watermarked content such as Blurring, Salt pepper noise, etc.

With the introduction of such scenarios, these techniques are tested and analyzed in order to find out the best among them, which can be used for future implementation procedures. These working scenarios can be shown as:

Figure 5.1: Host Image

Figure 5.2: Host Message

Figure 6.1: LSB Image

Figure 6.2: LSB Message

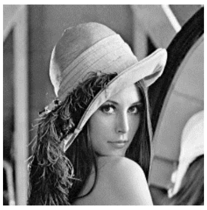


Figure 7.1: DCT Image

Figure 7.2: DCT Message

Figure 8.1: DWT Image

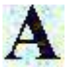


Figure 8.2: DWT Message

Table 1: Performance Analysis

S.No.	Working Domain	Technique	Mode of operation	Execution Time (seconds)	PSNR (dB)	NCC	SSIM
1.	Spatial Domain	LSB	Embedding	2.2113	57.2619397	1.0000	0.9999
			Extraction	0.8707		0.7456	0.2919
2.	Transform Domain	DCT	Embedding	1.9703	41.4160	0.9963	0.1696
			Extraction	0.8173		0.9988	0.9687
3.		DWT	Embedding	1.4577	51.7030735	0.9954	0.9715
			Extraction	1.6017		0.9975	0.8115

Table 2: Robustness Analysis

S.No.	Working Domain	Technique	Attacks	Embedding Execution Time (sec)	Extraction Execution Time (sec)	PSNR (dB)	Mean Absolute Error
1.	Spatial Domain	LSB	Without Attack	4.1555	0.9440	+7.56728	47.76172
			Rotation(180°)		0.7971	+4.68922	90.06250
			Blurring		0.6707	+2.93865	133.40137
			Cropping		0.5564	+12.15336	18.41504
			Gaussian Noise		0.7100	+3.41026	119.95801
			Salt Pepper Noise		1.0908	+6.61321	58.81738
			Scaling to 50%		0.6035	+3.16679	126.71582
2.	Transform Domain	DCT	Without Attack	2.3841	0.9386	+32.60967	2.90723
			Rotation(180°)		0.6212	+2.71473	140.31836
			Blurring		1.1612	+2.13119	160.09961
			Cropping		1.2535	+1.57368	181.65039
			Gaussian Noise		1.0905	+4.24507	99.46777
			Salt Pepper Noise		0.4078	+9.20823	33.60645
			Scaling to 50%		0.8935	+3.05841	129.85254
3.		DWT	Without Attack	2.201	1.7016	+24.14975	31.83550
			Rotation(180°)		1.5147	+23.71837	33.50093
			Blurring		1.5895	+8.85155	188.51761
			Cropping		1.1873	+16.73699	75.20500
			Gaussian Noise		1.5559	+4.08857	355.20902
			Salt Pepper Noise		1.5370	+8.86266	198.59262
			Scaling to 50%		1.2571	+21.74100	43.77043

The above images shows the appropriate working of these techniques by successful implementation of embedding and extraction watermark framework. These extracted and watermarked images can be used for performance and robustness analysis. The Normalized cross correlation of these techniques can be shown using below images, which clearly signifies the performance patterns of these techniques.

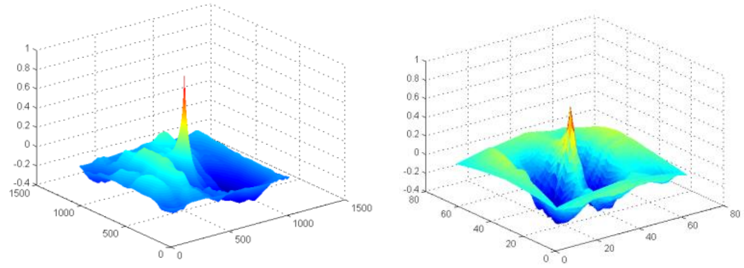


Figure 9: LSB Embedding and Extraction NCC comparisons

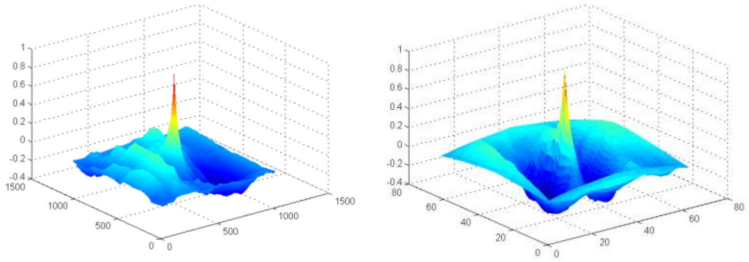


Figure 10: DCT Embedding and Extraction NCC comparisons

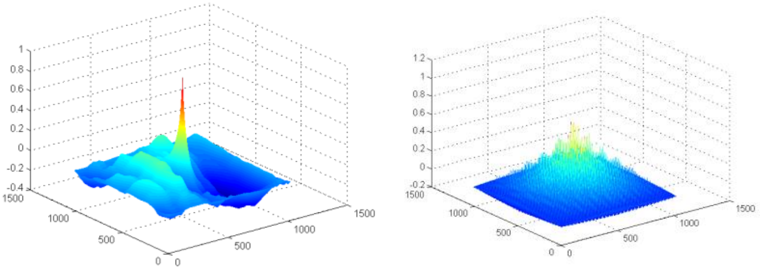
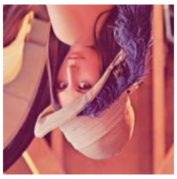


Figure 11: DWT Embedding and Extraction NCC comparisons

Using different performance techniques and parameters, performance patterns can be established as shown in the Table 1.Similarly, different robustness results can be established using different attacks such as Rotation, Blurring, Gaussian Noise, etc. Some results can be shown using Rotation attack as:



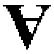
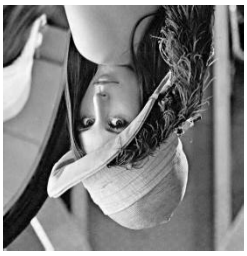


Figure 12.1: LSB Rotated Message

Figure 12.2: Extracted



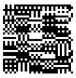
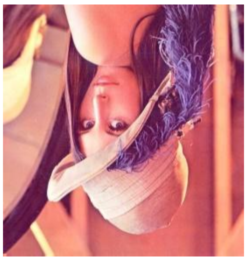


Figure 13.1: DCT Rotated Message

Figure 13.2: Extracted



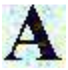


Figure 14.1: DWT Rotated Message

Figure 14.2: Extracted

Using different robustness techniques and attacking scenarios, robustness patterns and conclusions can be generated which are successfully shown in Table 2.

7. CONCLUSION

The analysis of different digital image watermarking techniques emphasize on the aspect of better and more advanced improvements in the field of this technology. There are still certain scenarios and considerations that requires better algorithms and procedures to be implemented in order to achieve more sustainable and sophisticated security procedures.

Conclusively, this review clearly explains and underlines the considerations that requires improvement and eventually provides conclusive result to elect the best and most reliable digital image watermarking technique depending upon the statistical comparisons on the basis of performance and robustness. In order to identify the most efficient watermarking technique, a statistical rating parameter is created, which is used to overall rate or provide considerable value on overall performance of the respective technique. This rating value can be calculated using above formalized system shown as:

Table 3: Rating scale Formalization

S.No.	Performance Criteria	Value	Robustness Criteria	Value
1.	Acceptable	2	Attack Survived	1
2.	Moderately Acceptable	1	Attack Not Survived	0
3.	Not Acceptable	0		
	Maximum Value	8	Maximum Value	6

Table 4: Concluding Table

S.No.	Working Domain	Technique	Overall Performance Level		Overall Robustness Capability		Overall Rating
1.	Spatial Domain	LSB	Execution Time	High	Rotation Attack	✓	4.285
			PSNR	High	Blurring Attack	×	
			Cross Correlation	Moderate	Cropping Attack	✓	
			Similarity Index	Low	Gaussian Noise Attack	×	
					Salt Pepper Noise Attack	✓	
					Scaling Attack	×	
2.	Transform Domain	DCT	Execution Time	Low	Rotation Attack	×	5.000
			PSNR	Low	Blurring Attack	×	
			Cross Correlation	High	Cropping Attack	×	
			Similarity Index	Moderate	Gaussian Noise Attack	✓	
					Salt Pepper Noise Attack	✓	
					Scaling Attack	×	
3.		DWT	Execution Time	Moderate	Rotation Attack	✓	6.429
			PSNR	Moderate	Blurring Attack	×	
			Cross Correlation	High	Cropping Attack	✓	
			Similarity Index	Very High	Gaussian Noise Attack	×	
					Salt Pepper Noise Attack	×	
					Scaling Attack	✓	

Total Value Attainable = *Maximum Value attainable from Performance + Maximum Value Attainable from Robustness*

Rating Formula = *(Value Attained from Performance + Value Attained from Robustness) / Total Value Attainable*

Using the above rating consideration, the best and most reliable technique can be easily decided depending upon the rating attained in performance and robustness testing. Hence, concluding table can be shown in the Table 4.

Taking into consideration the conclusive results, Discrete Wavelet Transform (DWT) technique turns out to be most secure and reliable digital image watermarking technique. The above result is generated using several statistical performance and robustness parameters, which eventual leads to calculation of rating parameter, where DWT receives the highest rating among all other image watermarking techniques. Unfortunately, DWT techniques suffers a major drawback of not able to extract the embedded image under different noises such as Gaussian noise or salt-pepper noise. This drawbacks limits the DWT techniques towards usage among the fields where noise exposure is high. This drawback provides the future scope for generation of better and reliable technique that does not suffers this unacceptable drawback. Under such scenarios, combination of DCT and DWT techniques can be implemented which can be a very effective solution. Such combination will increase robustness of the watermarking scheme, as DCT will resist the noise exposure problems that cannot be dealt with DWT and DWT will resist the rotation, cropping and scaling attacks which cannot be dealt with DCT. Hence, the combination of these two techniques together can provide the most efficient and reliable solution for securing the images against copyrights claims and violation cases.

8. FUTURE SCOPE

This paper provides the pre-requisites of searching better and secure digital image watermarking techniques. These pre-requisites can be used to search and create algorithms that can solve the problems and scenarios which was encountered in the implementation of these techniques.

1. Discrete Wavelet Transform (DWT) cannot eventually resolve the watermark extraction under noise exposure, thereby DWT is not the most secure technique after all.

2. These technique do not provide solution for blurring attack, thereby requires more efficient algorithm that can deal with such attacks.

3. Execution time still needs to be reduced for better execution and working scenarios in mobile platforms and other time-critical conditions.

9. ACKNOWLEDGEMENTS

I am extremely grateful and remain indebted to our guide Ms. Arunima Jaiswal for being supportive and providing required information which is required for the completion of this research paper. I am thankful to her for her constant constructive criticism and invaluable suggestions, which benefited me a lot while developing the plan for creating this research paper. She has been a constant source of inspiration and motivation for hard work. She has been very co-operative throughout this development. Through this column, it would be my utmost pleasure to express my warm thanks to her for her encouragement, co-operation and consent without which I mightn't be able to accomplish this creation.

10. REFERENCES

[1] Craver, S., N. Memon, B.L. Yeo and M.M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks and implications". IEEE J. Selected Areas Commun, 1998

[2] D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.

[3] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, , "Secure spread spectrum watermarking for multi-media," IEEE Trans. on Image Processing 6 (1997), 1673-1687.

[4] Tay P., Havlicek J.P., "Image Watermarking using Wavelets". IEEE, pp 258-261, 2002.

[5] Taha El Areef, Hamdy S. Heniedy, S . Elmougy, and Osama M. Ouda, "Performance Evaluation of Image Watermarking Techniques", Third International Conference on Intelligent Computing and Information Systems, Faculty of Computer & Information Sciences, ICICIS 7002 ,March 15-18, 2007, Cairo.

[6] Mustafa Osman Ali , Elamir Abu Abaida Ali Osman, Rameshwar Row, Electronics & Communication Engineering Dept., Biomedical Engineering Dept., University College of Engineering, Osmania University, "Invisible Digital Image Watermarking in Spatial Domain with Random Localization", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 5, November 2012.

[7] Bijan Fadeena and Nasim Zarei,"Hyprid DCT-CT "Digital Image Adaptive Watermarking", 3rd International Conference on Advances in Database, Knowledge, an data Applications, IARIA 2011.