Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks

J.Samuel Manoharan samuel1530@gmail.com
Asst.Prof/ECE Dept.
Karunya University
Coimbatore, 641114,India

Dr.Kezi C.Vijila vijila_2000@gmail.com
Professor & Principal
Christian College of Engg.
Dindigul, 624619, India

A.Sathesh sathesh_ece@yahoo.com
Asst.Prof/ECE Dept.
Karunya University
Coimbatore, 641114, India

Abstract

Data hiding is an age-old technique used to conceal an image, text of vital importance inside an image or video sequence. Several attacks are prevalent in an attempt to hack the data hidden inside the image. Several algorithms have been put forward focused in making the embedding technique to be robust to such attacks. The current work is focused towards studying the behavior of Spatial and Frequency Domain Multiple data embedding techniques towards noise prone channels and Geometric attacks enabling the user to select an optimal embedding technique. The robustness of the watermark is tested by introducing several attacks and testing the watermark strength.

Keywords: Luminance, Edges, Geometric attacks, Correlation Coefficient

1. INTRODUCTION

A Digital Watermark may be a data, image or any secret piece of information embedded inside a host image or a video sequence to provide the content of the cover image or video with rightful ownership [1] in order to prevent further misuse of the image or video. Further, these techniques are also extended to carry vital information [2] inside a cover image or video for transmission and reception under privacy. Any Data Hiding Technique should have the following parameters in its algorithm namely the robustness [3] of the watermark to external attacks, Visual imperceptibility and an Optimal Embedding Capacity. The current work is focused towards an analysis over the applications involving information hiding rather than copyright protections thereby incorporating the first two parameters i.e., Robustness and Visual Imperceptibility demanding an invisible approach [4]. A general data embedding is shown in Fig 1. The Cover image and the watermark are transformed into a suitable domain for processing and the embedding sites are identified into which the watermark is inserted after using a hashing function. The Receiver side incorporates a watermark extraction process where the watermarked image is once again transformed into the same domain as that in the transmitter side and the watermark is extracted from the knowledge of

the watermark location. In between the embedding and extraction process, is the communication channel which is predominant with random and Gaussian noise which tends to corrupt and degrade the watermarked image and thus the watermark itself. The effects of those channel disturbances [2] have been simulated by addition of noise, rotating the watermarked image and cropping the image which is equivalent to a person trying to destroy the vital piece of hidden information. A Data Retrieval system is shown in Fig 2 where the watermarked image is subjected to the transformation identical to that of in the embedding system and the watermark is retrieved by using the inverse function after identifying the embedding location.

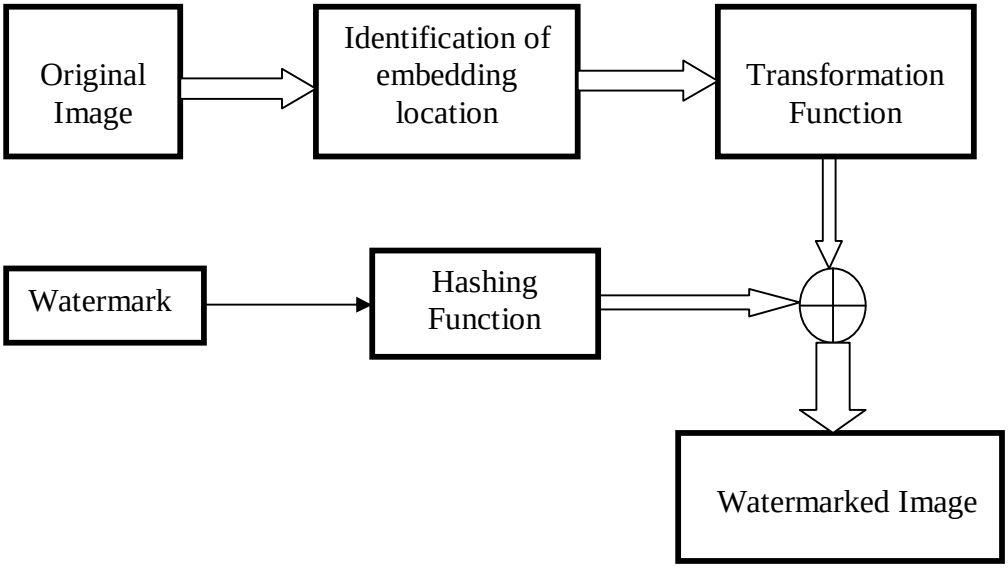

FIGURE 1: A General Data Embedding System

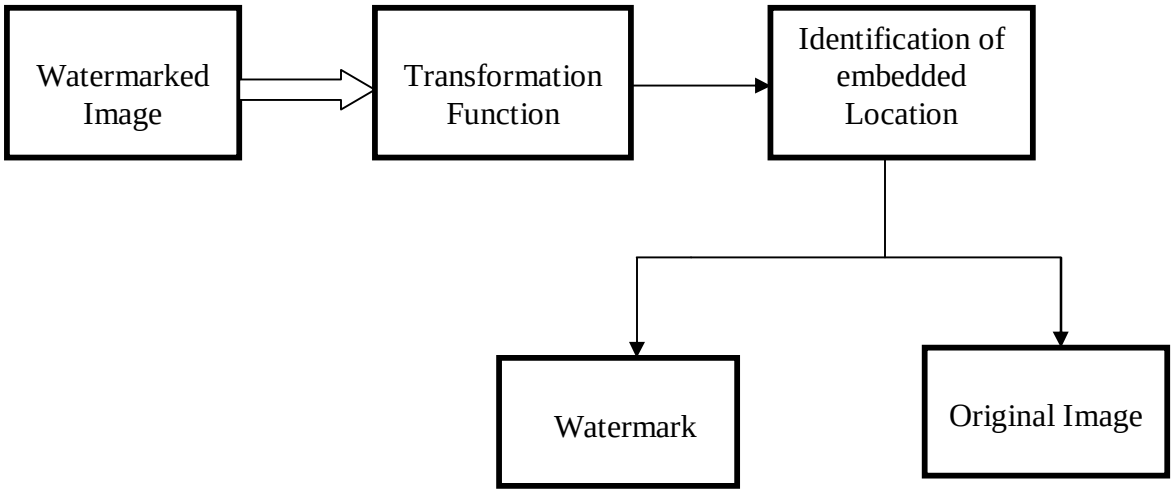

FIGURE 2: A General Data Retrieval System

In General, any watermarking technique is done either in Spatial or Frequency domain. Spatial Domain techniques are extremely simple to construct and design and they give a perfect reconstruction in the absence of noise as illustrated in the results. There are numerous techniques put forward in spatial domain embedding utilizing the luminance components [5] , manipulating the Least Significant Bits [6] as ideal locations for embedding, Manipulating the Intensity Components [7], Image Differencing [8] etc.,

On the other hand, In Frequency Domain, the cover image and the watermarks are subjected to a transformation into the frequency domain where deeper manipulations of the coefficients are possible without noticeable degradation to the cover image is possible. The transformation may be done using Discrete Cosine Transform [9], Discrete Wavelet Transform [13], Ridgelet Transform etc.,

The Discrete cosine transform classifies an image into parts [11] or spectral sub-bands of varying importance in terms of image's visual quality. DCT techniques are Frequency domain based and the watermarked image shows good robustness towards Scaling, JPEG distortion, Dithering distortion, Cropping, Printing, Scanning etc.,

DWT has been used in digital watermarking more frequently than other transforms due to its excellent spatial localization, frequency spread and multi-resolution characteristics [12]. Wavelets are special functions which, in a form analogous to sins and cosines in Fourier analysis, are used as basal functions for representing signals. For 2-D images, applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub bands LL_n, LH_n, HL_n and HH_n, as illustrated in Fig 3 and Fig 4, where n represents the level of transformation. The HH_n coefficients are the fine scale values depicting the presence of edges, while the LL_n coefficients give the coarse scale values and much of visible information. Internally, the Discrete Wavelet Transform comprises of a realization of Low pass and High Pass Filters as shown below
.

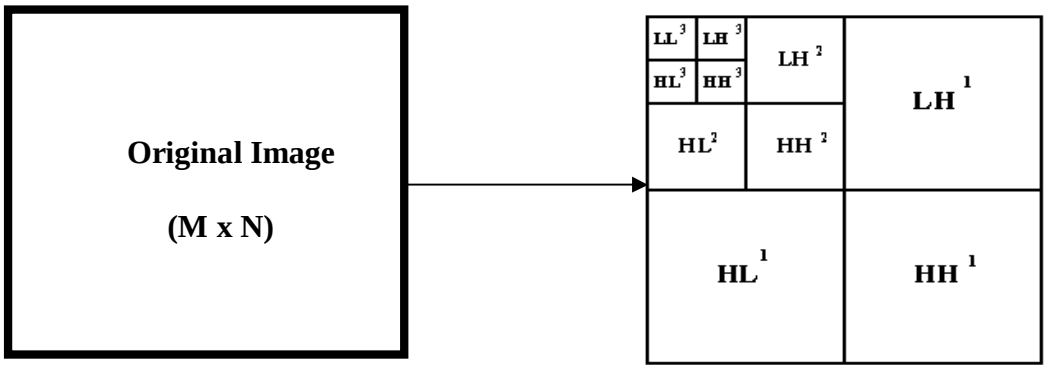

Figure 3: 3 Level Wavelet Decomposition

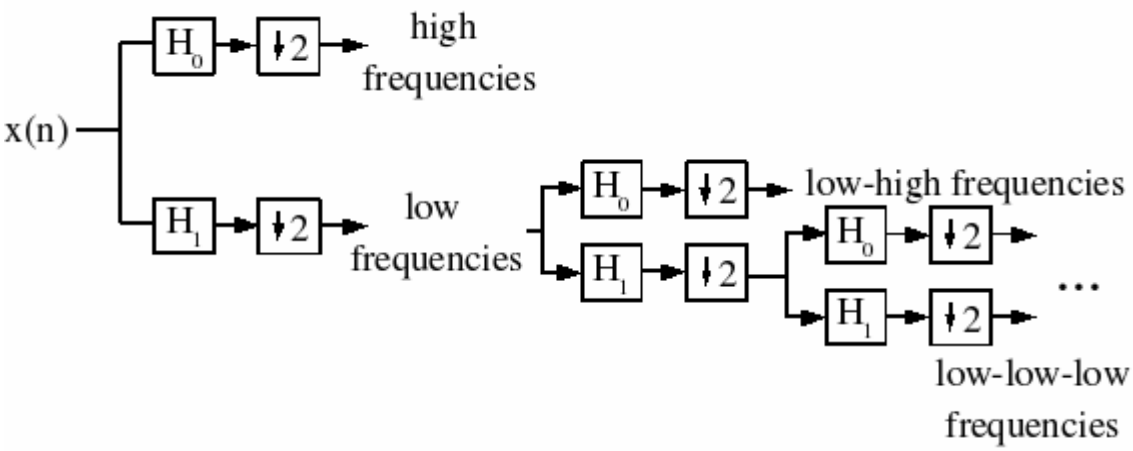

Figure 4: Filter Realization of Wavelet Transform

2. METHODOLOGY

The work is focused towards establishing a comparative study of Frequency over the Spatial Domain watermark in terms of robustness towards attacks and the reconstruction factor. Robustness is an essential parameter used to express the strength of the watermarking algorithm towards attacks. If the external attacks which may be Intentional or Unintentional tend to degrade the hidden information, it implies that the embedding algorithm is not robust enough to withstand the attacks. The strength of the embedding process is determined by exposing the watermarked image to various attacks which may be addition of noise, compressing the image, rotation, scaling etc. There are several measures to determine the strength of the embedding algorithm. It can be expressed using PSNR, Correlation Coefficient etc., We have done an analysis by exposing the watermarked image to external attacks such as noise, cropping, rotation etc., and measured the reconstruction quality in terms of the Correlation Coefficient which usually takes the value from 0 to 1 with 1 indicating a good embedding algorithm in terms of robustness while a 0 indicates the hidden information has failed totally towards external attacks. To begin with, the cover images have been subjected to Spatial as well as Frequency domain processing and the sites for ideal embedding are identified. The watermark images are then embedded into the cover images in both spatial and Frequency domain and the inverse processing is done to get the watermarked image. This image is subjected to attacks in the form of Noise to various degrees, Cropping and Rotation. The attacked watermarked image is then subjected to the processing identical to that done in the transmitter side to obtain the embedded location from which the original image and watermarked image is compared to get back the watermark. The watermark image is now compared for its degree of robustness and results tabulated and plotted.

Figure 5: Cover Images used

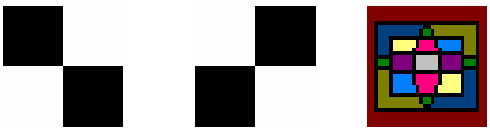

Figure 6: Watermarks used

Spatial Domain Watermarking can be implemented by directly manipulating the pixels or intensity values of the image itself to a certain extent. This work incorporates the exploitation of the luminance component of the image where visual imperceptibility is being maintained [5].. The blocks containing the highest luminance values are calculated to determine the embedding location. The watermarks are then embedded into the selected locations and the image reconverted back to obtain the original watermarks. During extraction, the original image and the watermarked image are compared to retrieve the encrypted water mark bits.

Figure 7. Original and Watermarked Images in Spatial Domain

Applying a DCT to an input image of size N by M with f(i,j) being the intensity of the pixel in row i and column j, results in DCT Coefficient F(u,v) in row k1 and column k2 of the DCT matrix. For most images, much of the signal energy lies at low frequencies and they appear in the upper left corner of the DCT. The above property of energy compaction is made use of in this embedding procedure. Embedding is achieved by inserting the watermark into a selected set of DCT coefficients [10] [11]. After embedding, the watermark is adapted to the image by exploiting the masking characteristics of the human visual system, thus ensuring the watermark invisibility. Experimental results demonstrate that the watermark is considerably robust to several signal processing techniques, including JPEG compression, addition of Gaussian noise, rotation, and random noise, scanning etc., The host image and watermark is DCT transformed and the coefficients of the image and the coefficients are grouped into blocks and embedding is done in edge blocks using a Sobel operator or any other edge finding algorithms as any change done on the edge block does not produce any visual changes thus maintaining the visual imperceptibility. The watermarked image is obtained by enforcing the modification equation shown below

$$WM\_Cff\{i,j\} = \beta * Cover\{i,j\} + \alpha * Wm\{i,j\} \qquad (1)$$

where β is the scaling factor and α is the embedding factor, WM is the watermarked image and Wm is the watermark itself. The inverse DCT is applied to obtain the watermarked image.

Figure 8: Original and Watermarked Images in the DCT Domain

The extraction is non blind and the same DCT decomposition is applied to both the original and embedded images. The coefficients of the watermarked image and the original image are compared to retrieve the watermark coefficients.

A n level DWT is performed on the cover image and the ideal bands for insertion [11] are chosen and the DWT coefficients of the data are inserted into these sub bands using the following modification.

$$WM\_C\{i,j\} = Cover\{i,j\} + \alpha * W\{i,j\} \quad (2)$$

Where Cover{i,j} are the Cover image coefficients

WM {i,j} are the watermark coefficients

α is the embedding factor which is chosen as from 2 - 3 to provide a tradeoff between invisibility and robustness.

Figure 9. Original and Watermarked Images in the DWT Domain

During extraction, the original image is required in extracting watermarks. Such an extraction is classified as non-blind watermarking. The same n Level wavelet decomposition is applied to both the original and embedded images. The coefficients of the watermarked image and the original image are compared to retrieve the watermark coefficients. The watermark-embedding locations are obtained from the original image. The watermarks are obtained using the inverse transform.

3. RESULTS & FUTURE WORK

Lena, Peppers, Cameraman, Baboon and Barbara Images of 256 x 256 were taken and multiple embedding is done using Spatial, DCT and DWT domain techniques and the performance of the watermark towards geometric attacks over the transmission channel is analyzed. The Geometric attacks are introduced in the form of noise, rotation, scaling, compression etc., and its Similarity measure between the extracted and the original watermark is obtained in terms of Correlation Coefficient. Fig 10a, 10b, 10c & 10d illustrate the spatial domain watermarked image being subjected to noise, rotation and compression attacks. It can be seen that a Spatial Domain watermarked image fails totally when exposed to random noise which is a very common component present in a communication channel. On the other hand, a frequency domain watermarked image exhibits good robustness towards noise which can be seen from the visual results depicted in 11a. Figures 11b, 11c & 11d represent the Frequency domain images subjected to white noise, rotation and compression.

Figure 10. a. Random Noise b.White Noise c. Rotation d. Compression

Figure 11: a. Random Noise b. White Noise c. Rotation d. Compression

The overall response is depicted Fig 12 for Spatial domain watermarking method and Fig 13 for Frequency domain watermarking method.

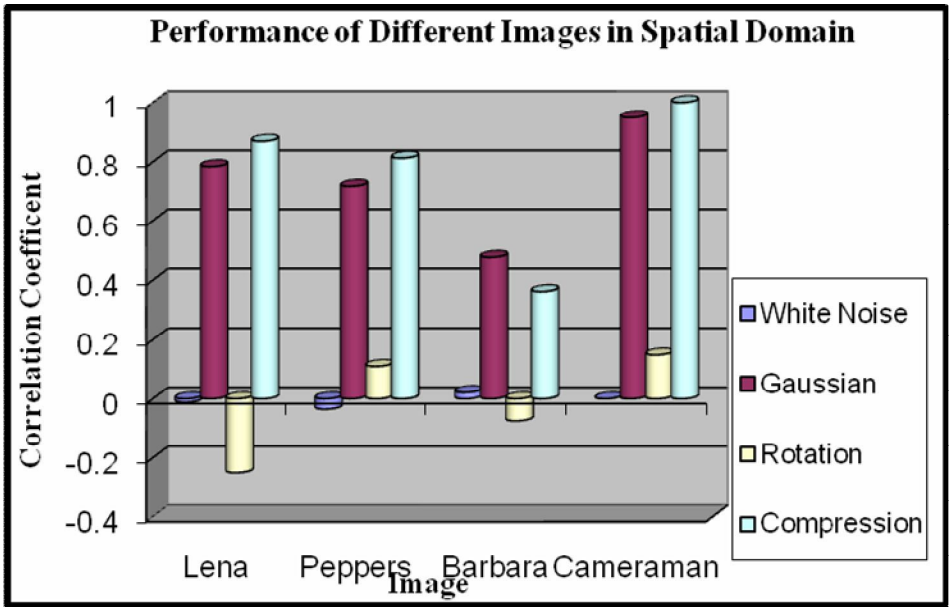

Figure 12: Behavior of Spatial Domain embedding towards various attacks

Fig 12 implies a perfect reconstruction of the watermark in absence of noise with correlation coefficients nearing 1 but becomes totally corrupted in the presence of noise. In contrast, it can be seen that Frequency domain methods show good robustness towards external attacks. It is evident that data embedded in frequency domain show considerable tolerance towards noise, compression etc., as illustrated in Fig 13. But in both cases, it can be seen that both techniques exhibit significant instability towards rotation based attacks necessitating the use of a rotation invariant transforms. The resistance towards the images towards external attacks also varies from image to image as can be seen from Fig 12 and Fig 13. Peppers image is seen to show good tolerance towards external attacks in the spatial domain, while the Cameraman Image is seen to exhibit significant tolerance towards external noise in both the domains.

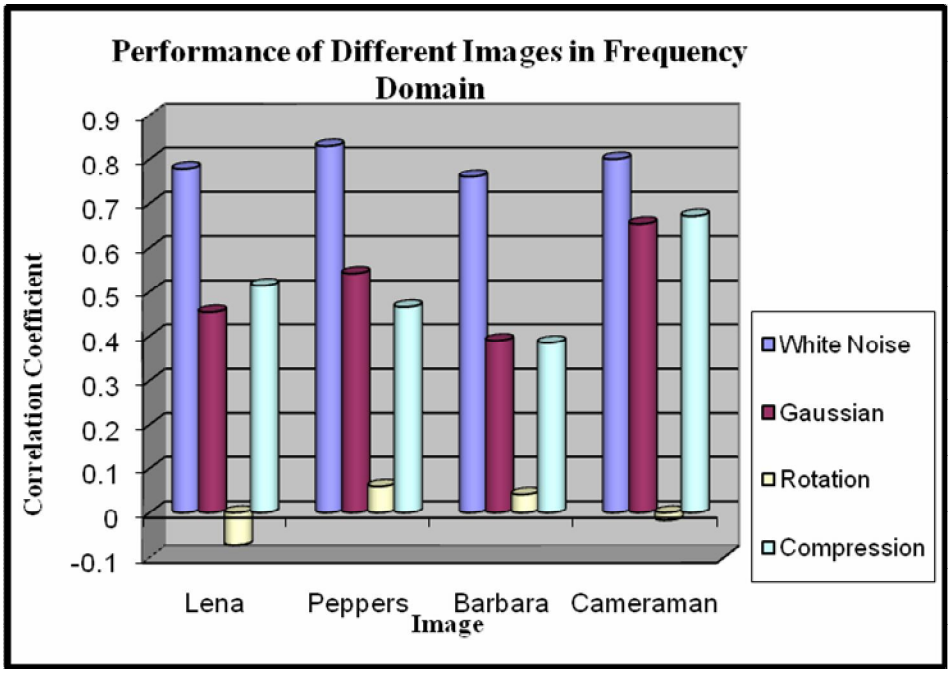

Figure 13: Behavior of Frequency Domain embedding towards various attacks

We have then turned our attention to a specific analysis of how the watermarked image behaves towards a noisy transmission channel with more of white noise present with zero mean. Figure 14 gives a comparative illustration of the performance of a Lena Image in the three methods of embedding when subjected to white noise.

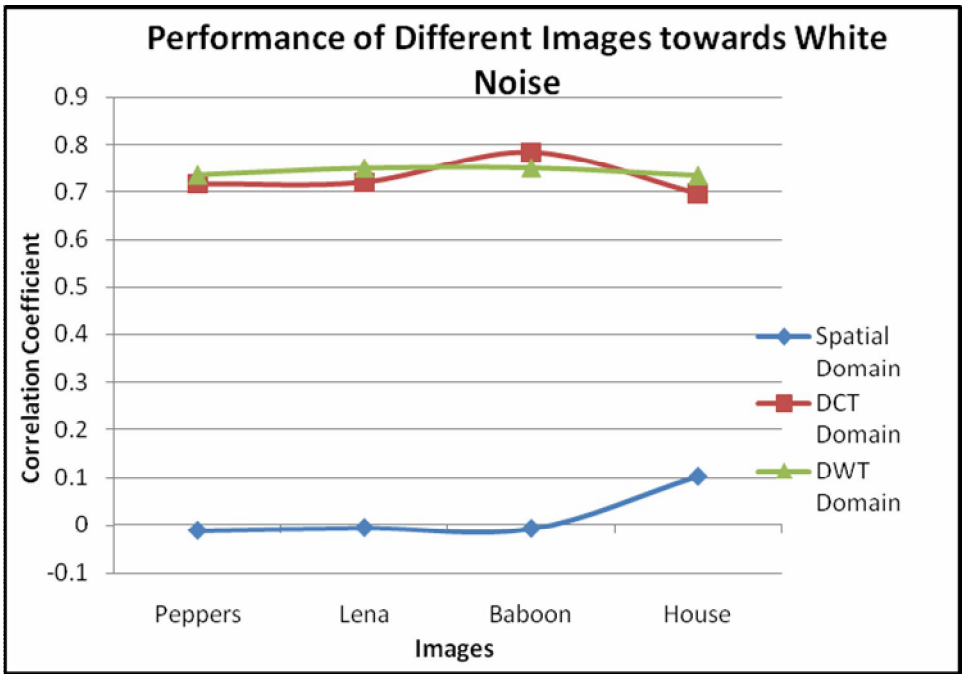

Figure 14: Performance of Different Images towards White Noise

From Fig 14, it can be seen that once again Frequency domain techniques show a relatively better response when compared to their spatial domain counterparts when exposed to white noise condition. Amongst, the Frequency domain techniques, it can be seen that the DWT techniques have a marginal edge, in terms of the robustness, over the DCT techniques. Depending on the type of channel to be employed in transmitting or receiving, the choice can be made between the DCT and DWT techniques or a combination of both.

Finally, we have turned to a more specific analysis to illustrate the response of a 256 x 256 Lena image embedded with more than one number of data in different locations and using the above domains. The results are depicted in Fig 15 which shows the response of Lena image under increasing conditions of Noise Levels in the Transmission Channel. The responses of individual watermarks 1 and 2 have been depicted below with the DWT techniques showing a considerable edge over the spatial domain techniques.

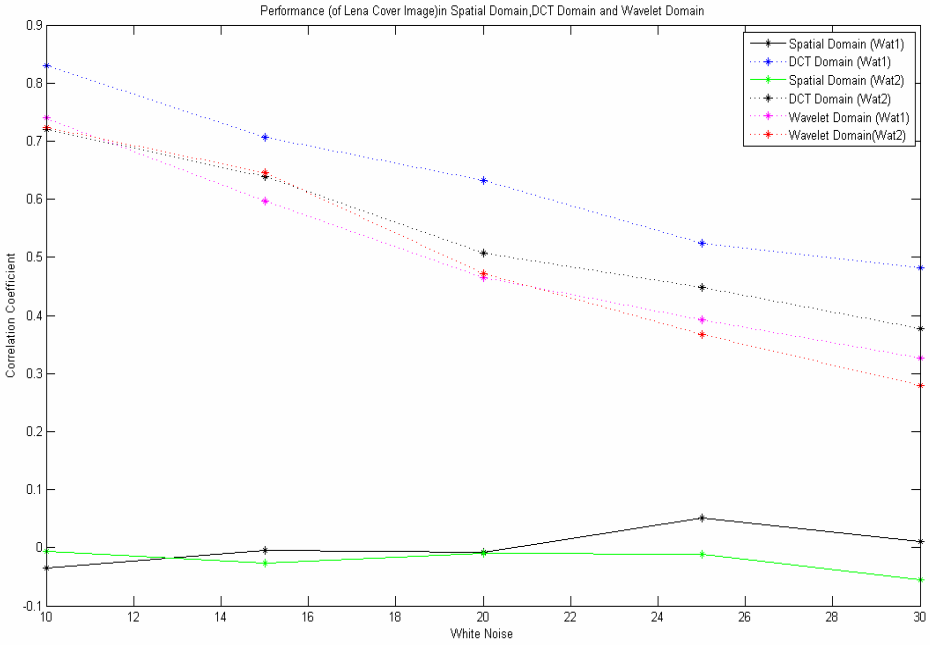

Figure 15: Overall Performance of Lena Image towards the three domains of watermarking

The above analysis has been done with an objective to aid the designer of a watermarking system to take into account the factors discussed for optimal embedding for the right application. Since, Visual Imperceptibility, Robustness are critical criteria dealing with privacy and strength respectively, we hope this analysis would be helpful to choose the combination of right transform along with the right location for embedding for desired results. However, there exists another criteria namely the Embedding capacity which determines the maximum information that can be embedded into the image without degrading watermarked image performance. We are in the process of establishing a performance analysis in order to determine a tradeoff between the image quality and the embedding capacity using a genetic based optimization approach. Apart from this, these results would provide an useful platform for us to exploit the avenues in inserting a patient information record inside a medical image (EPR) using a transform based approach. Further study is also being done to introduce wavelet based medical image embedding for increasing the optimality in determining embedding locations as well as to exploit the denoising property of wavelet transforms [14]. We are also investigating the possible incorporation of a RST invariant algorithm to make the resultant embedded image resistant towards translation, rotation and invariance attacks.

REFERENCES

[1]. Y. Wang, J. F. Doherty and R. E. Van Dyck, "*A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images*", IEEE Transactions on Image Processing, Vol. 11, Issue 2, pp. 77-88, 2002

[2]. Chun Shien Lu, H.Y.M.Liao, "*Multipurpose watermarking for image authentication and protection*", IEEE Transactions on Image Processing., Vol.10, Issue 10, pp.1579-1592, 2001.

[3]. V. Licks and R. Jordan, "*On Digital Image Watermarking Robust to Geometric Transformations*," Proceedings of 2000 International Conference Image Processing (ICIP 2000), Vol. 3, pp. 690-693, 2000.

[4]. Dipti Prasad Mukherjee, Subhamoy Maitra, Scott T. Acton, "*Spatial domain Digital Watermarking of Multimedia Object for Buyer Authentication",* IEEE Transactions on Multimedia, Volume 6, No.1, pp. 1- 15, 2004

[5]. Jamal Hussein, "*Spatial domain Watermarking scheme for color images based on log average luminance*", Int'l Journal of Computing, Volume 2, Issue 1, 2010

[6] Nikolaidis, Pitas, "Robust Image Watermarking the Spatial Domain", International Journal of Signal Processing", Vol.66, Issue 3, pp. 385 – 403, 1998.

[7] Verma P, D.P. Agarwal, Jain S, "*Spatial Domain Robust Blind Watermarking for Color Image*", Asian Journal of Information Technology, Vol. 6, Issue. 4, pp. 430 – 435, 2007.

[8] Wu, D. C., Tsai, W. H., "*Spatial-Domain Image Hiding Using an Image Differencing"*, *IEEE Proceedings -Vision, Image and Signal Processing*, Vol. 147, Issue. 1, pp. 29 – 37, 2000.

[9]. Juan Hernandez, Martin Amado, Fernando Perez, "*DCT Domain Watermarking Techniques for Still Images: Detector Performance analysis and new structure*", IEEE Transactions on Image Processing, Vol. 9, No.1, pp. 55 – 68, 2000.

[10]. Saraju P.Mohanty, K. R. Ramakrishnan and Mohan S. Kankanhalli, "*A DCT Domain Visible Watermarking Technique for Images*" by ICME, vol.2 , pp. 1029 - 1032, 2000

[11]. Mauro Barni. Franco Bartolini, Vito Cappellini, Alessandro Piva., "*A DCT domain system for robust image watermarking*", International Conference on Signal Processing, Vol.66, Issue.3, pp. 357-372, 1998.

[12]. A.Lumini, D.Maio, "*A Wavelet Based Image watermarking scheme"*, The International Conference on Information Technology: Coding and Computing (ITCC), pp. 122-127, 2000

[13]. Ali Al-Haj, "*Combined DWT – DCT Digital Image Watermarking",* Journal of Computer Science, Vol.3, Issue.9, pp.740-746, 2007.

[14] Sathesh, Samuel Manoharan, "*A Dual Tree Complex Wavelet Transform Construction and its application to Image Denoising,* International Journal of Image Processing, Vol.3, Issue.6, pp.293 – 300,2010.