SNR COMPUTATION OF VARIOUS SPATIAL AND FREQUENCY DOMAIN TRANSFORMATION

RUCHI KAWATRA [#] APNEET KAUR* SAPNA ARORA[$]
[#]*M.Tech. (IT)Guru Gobind Singh Indraprastha University. Delhi*
Ph. No. +919818495019
ruchirehani@rediffmail.com

**Lecturer(IT), RAYAT AND BAHRA INSITUTE OF ENGINEERING AND TECHNOLGY, SAHAURAN, KHARAR (Affiliated to Punjab Technical University)*
Ph. No. +919878697764
apneet@yahoo.com

[#]*M.Tech (IT) New Delhi*
Ph. No. +919868725149
er.sapna@yahoo.com

Abstract: **Embodiments of this paper includes the study of steganography and digital watermarking as a technique of hiding images. Various algorithms on spatial and frequency domain transformation have been studied and their Signal-to-Noise Ratio has been computed. The processor complexity has also been checked to find out which algorithm can efficiently work on robust environment. The original image is decomposed in DWT domain in to three hierarchical levels and watermarks it with a logo image. The watermark is added to the DWT image according to a certain threshold. The watermark can be extracted at lower resolution without computational complexity. Wavelets play an important role in the upcoming compression standards such as JPEG2000. Experimentally it has been shown that a watermark signal can be embedded in high-pass wavelet coefficients without any impact on the image visual fidelity. Many transformations techniques are there but only a few have been studied and a simple comparison and analysis is performed.**

Keywords – Digital Watermarking, Discrete Cosine Transformation, Fast Fourier Transformation, Information hiding.

I. INTRODUCTION

Currently, virtually all multimedia production and distribution is digital. The advantages of digital media for creation, processing and distribution of productions are well known: easy modification and possibility of software processing rather than the more expensive hardware alternative (if real-time processing is not a requirement). Maybe the most important advantage is the possibility of unlimited copying of digital data without any loss of quality. This latter advantage is not desirable at all to the media producers and content providers. In fact, it is perceived as a major threat, because it may cause them considerable financial loss. [3]

Digital watermarks have been proposed as a way to tackle this problem. This digital signature could discourage copyright violation, and may help determine the authenticity and ownership of an image. Ideal characteristics of a digital watermark have been stated. These characteristics include:

1. Statistical invisibility.
2. Fairly simple extraction should be.
3. Accurate detection.
4. Robustness to filtering, additive noise, compression, and other image manipulations.
5. Ability to determine the true owner of the image. [1] [8]

Steganography is the technique for hiding messages during communication. There are other methods also like, Cryptography for data hiding. In Cryptography the message is send in distorted form so that no one other then the authorized person can understand the message. Here the existence of data

in known to any intruder. But in steganography, the message is first encrypted using some stego key and then made invisible to by hiding it in some other media. A cover image is generally used to hide the information exchange. The original message is embedded in this cover image. The first challenge for a person who is illegally trying to access some confidential information will be to detect whether a secret communication is taking place or not. Different methods of steganography have been studied and understood how it is better than cryptography. For embedding data, some secret information is required that needs to be sent to the receiver. It may be in any form that can be embedded in a digital image, such as simple text, coded text, some image file etc. Secondly, an appropriate cover image needs to be selected. An 8-bit GIF file is ideal to be used as cover image for Steganography. In this file format, each pixel is represented using a single byte. This byte is used to hold a numeric value that points to a particular color index of a 256-color palette. An image file featuring 256 shades of gray color is considered best for steganography. Reason being that it is very difficult to identify shade changes in a gray scale image until the changes are very extreme.

Once the cover image file has been selected, the next step is to embed secret information in that file. Various techniques exist for this purpose and most popular ones are:

i) LSB insertion
ii) Masking and filtering
iii) Algorithms and transformation. [12]

Spatial and frequency domain transformation algorithms have been analyzed for calculating robust steganography on images. One steganography tool that integrates the compression algorithm for hiding information is Jpeg-Jsteg. Jpeg-Jsteg creates a JPEG stego-image from the input of a message to be hidden and a lossless cover image. JPEG images uses different transformation algorithm to achieve compression like DCT (Discrete Cosine Transformation), FFT (Fast Fourier Transformation) and wavelet transformation. [

II. IMPLEMENTATION

The well – known methods which are helpful for hiding information are developed in Matlab. They are

(i) Fast Fourier Transformation (FFT) of Images
(ii) Discrete Cosine Transformation (DCT) of Images

The techniques like digital watermarking (DWT), inverse digital water marking (IDWT), dithered image, rotation of image, median filter of image , salt and pepper noise on image, FFT and DCT are used. The Signal – to – Noise ratio (SNR) is computed for all these methods. Then these different values can be compared and further used for better results. It was found that Digital Water Marking has the least SNR. The work is done on grayscale image.

The **algorithm** used is –

1. The image is decomposed in DWT domain.
2. The DWT coefficients having high entropy values are selected for each block in which the watermark is to be inserted.
3. The number of DWT coefficients depends on total pixel in the watermark. The watermark is added in high value coefficients so that it spreads uniformly all over the image.
4. Binary watermark image pixel is selected.
5. The watermark image is obtained by taking the inverse DWT.
6. The SNR is calculated using the formula
   $S = 10 * \log_{10} S$.

DWT is a hierarchical transformation which offers the possibility of analyzing the signal at different at different resolution and different bands which is not the case of FFT and DCT.

Mathematical transformations are applied to signals to obtain further information from that signal that is not readily available in the raw signal. Most of the signals in practice are time-domain signals in their raw format.

Time domain representation is not always the best representation of the signal for most signal processing related applications. In many cases, the most distinguished information is hidden in the frequency content of the signal. The information that cannot be readily seen in the time-domain can be seen in the frequency domain.

Fourier transform (FT) is used to find the frequency content of a signal. It allows going back and forwarding between the raw and processed (transformed) signals. However, only either of them is available at any given time. That is, no frequency information is available in the time-domain signal, and no time information is available in the Fourier transformed signal. Fourier transform of a time domain signal x (t) and inverse Fourier transform (IFT) of a frequency domain signal X (f) are given below.

$$X(f) = \int_{-\infty}^{\infty} x(t) \bullet e^{-2j\Pi ft} dt$$

$$x(t) = \int_{-\infty}^{\infty} X(f) \bullet e^{2j\Pi ft} dt$$

The discrete wavelet transform (DWT provides sufficient information both for analysis and synthesis of the original signal, with a significant reduction in the computation time. The DWT is considerably easier to implement when compared to the continuous wavelet transformation (CWT).

DCT is a lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to compute DCT.

Signal-to-noise ratio (often abbreviated **SNR** or **S/N**) is a measure used in science and engineering to quantify how much a signal has been corrupted by noise. It is defined as the ratio of signal power to the noise power corrupting the signal. A ratio higher than 1:1 indicates more signal than noise. While SNR is commonly quoted for electrical signals, it can be applied to any form of signal. [21]

Spread-spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated in a particular bandwidth are deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, to prevent detection, and to limit power flux density (e.g. in satellite downlinks).

III. EXPERIMENTAL RESULTS

A. SNR Computation of Original image

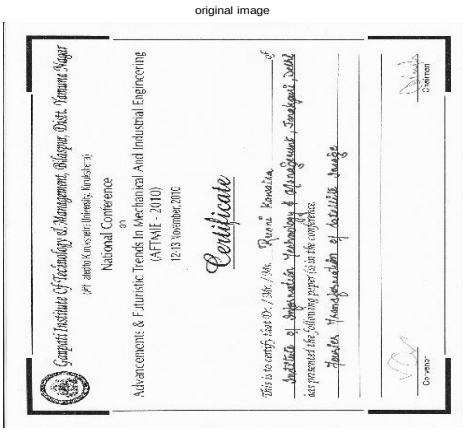

Fig.1 Original Image

SNR OF WATER MARKED IMAGE WITH ORIGINAL= 23.033223

B. SNR after applying DWT is found to be

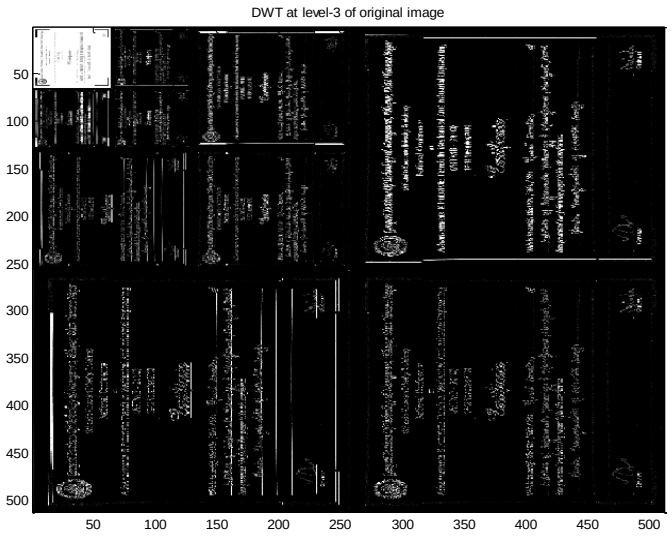

Fig. 2. DWT Image

SNR with JPEG 100 = 23.936378
NC of ch2 extraction = 85.563973
NC of ch3 extraction = 94.149832
NC of cv3 extraction = 96.254209

SNR with JPEG 80 = 23.743093
NC of ch2 extraction = 78.829966
NC of ch3 extraction = 93.223906
NC of cv3 extraction = 95.159933

SNR with JPEG 50 = 22.983594
NC of ch2 extraction = 55.303030
NC of ch3 extraction = 88.425926
NC of cv3 extraction = 91.750842

SNR with JPEG 30 = 22.087644
NC of ch2 extraction = 42.045455
NC of ch3 extraction = 46.675084
NC of cv3 extraction = 42.340067

SNR with JPEG 10 = 20.027448
NC of ch2 extraction = 25.252525
NC of ch3 extraction = 32.070707
NC of cv3 extraction = 33.122896

SNR of blurred image = 16.483627
NC of ch2 extraction = 44.949495
NC of ch3 extraction = 84.890572
NC of cv3 extraction = 27.062290

SNR of de-blurred image = 20.130243
NC of ch2 extraction = 65.614478
NC of ch3 extraction = 88.299663
NC of cv3 extraction = 68.181818

C. SNR of FFT image is found to be

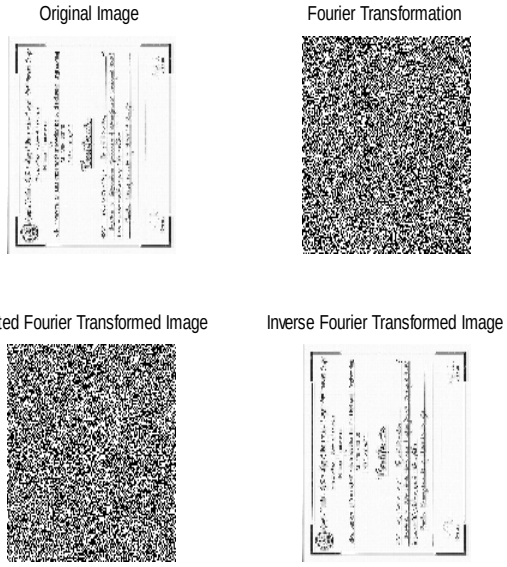

Fig.3. FFT Image

SNR of Fourier transformed image = -102.101785
NC of ch2 extraction = 50.547138
NC of ch3 extraction = 49.663300
NC of cv3 extraction = 49.116162

D. SNR of DCT image is found to be

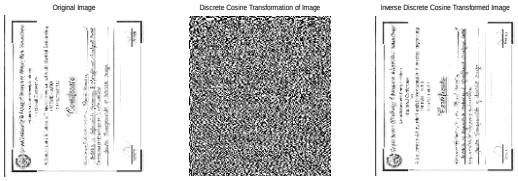

Fig.4. DCT Image

SNR of DCT image = -48.061190
NC of ch2 extraction = 48.779461
NC of ch3 extraction = 49.537037
NC of cv3 extraction = 50.294613

E. SNR after Rotation of image by 4 degrees

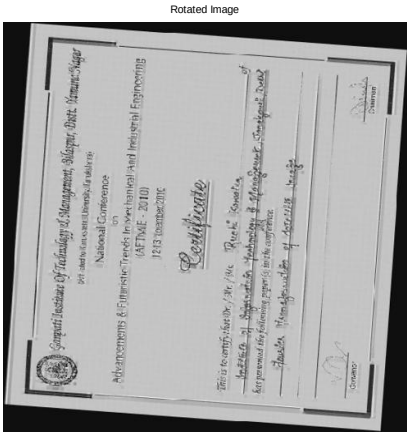

Fig. 5. Image rotated by 4 degrees

SNR of rotated image = 7.535249
NC of ch2 extraction = 13.425926
NC of ch3 extraction = 35.185185
NC of cv3 extraction = 34.469697

F. SNR after applying dithering attack

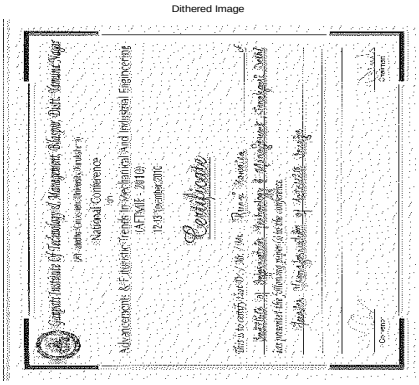

Fig.6. Dithered Image

SNR for dithered image= 14.800224
NC of ch2 extraction = 53.956229
NC of ch3 extraction = 64.309764
NC of cv3 extraction = 60.437710

G. SNR after applying Median Filtering

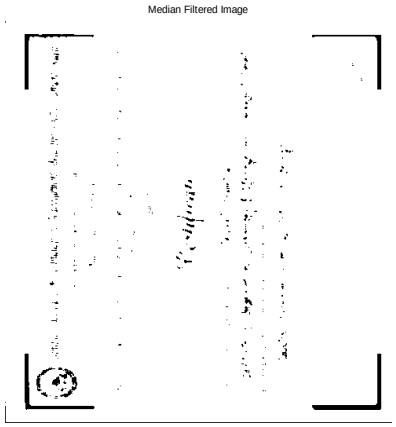

Fig.7. Median Filtered Image

SNR of median filtered image= 0.034791
NC of ch2 extraction = 0.000000
NC of ch3 extraction = 23.779461
NC of cv3 extraction = 23.106061

H. SNR after applying Average Filtering

Fig.8. Average Filtered Image
SNR of average filtered image= 16.814682
NC of ch2 extraction = 33.796296
NC of ch3 extraction = 80.092593
NC of cv3 extraction = 75.084175

I. SNR after adding Salt and Pepper Noise

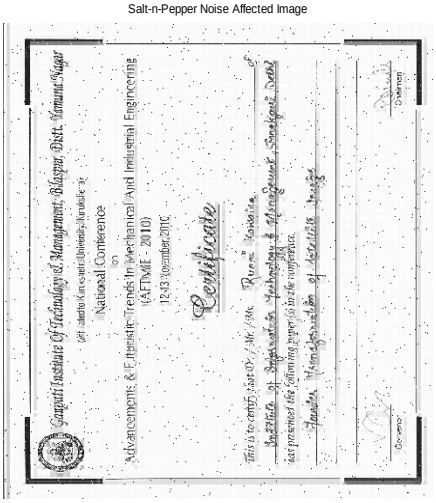

Fig.9. Salt-n-Pepper Noisy Image
SNR OF SALT N PEPER NOISE IMAGE = 20.479266
NC of ch2 extraction = 81.481481
NC of ch3 extraction = 81.018519
NC of cv3 extraction = 83.712121

SNR of AWGN noised image= 22.615116
NC of ch2 extraction = 32.281145
NC of ch3 extraction = 47.390572
NC of cv3 extraction = 45.959596

J. SNR calculated for blurred image

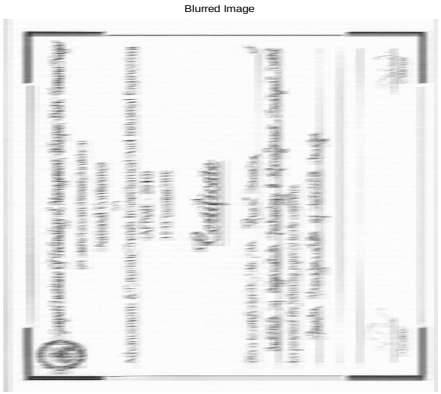

Fig. 10. Blurred Image

SNR of blurred image = 16.483627
NC of ch2 extraction = 44.949495
NC of ch3 extraction = 84.890572
NC of cv3 extraction = 27.062290

Table 1. SNR Computation of Various Transformations

S. No.	ATTACKS	SNR
1	JPEG Compression, Q.F – 100%	23.936378
2	JPEG Compression, Q.F –80%	23.743093
3	JPEG Compression, Q.F – 50%	22.983594
4	JPEG Compression, Q.F – 30%	22.087644
5	JPEG Compression, Q.F – 10%	20.027448
6	BLURRED	16.483627
7	DEBLURRED	20.130243
8	ROTATED 4 DEGREE	7.535249
9	AVG FILTERED	16.814682
10	SALT N PEPER NOISE	20.479266
11	AWGN NOISE	22.615116
12	DITHERED	14.800224
13	MEDIAN	0.034791
14	DISCRETE COSINE TRANSFORMATION	-48.061190
15	FAST FOURIER TRANSFORMATION	-102.101785
16	SPREAD SPECTRUM	1.352877

IV. CONCLUSION

(i) After studying and developing the various transformation methods in Matlab. It can be concluded that DWT is much better among all.
(ii) The estimated SNR value is used as the characteristic of steganography classification.
(iii) An 8 bit grayscale image is used.
(iv) TIFF image is used as it is better then JPEG image. The experimental results have shown the effectiveness of different methods, which indicates that spatial domain embedding in JPEG covers is highly insecure.
(v) What if the image sent during communication is destroyed by an intruder. To resolve this issue - Associative memory can be used to compare the original image with the one received by the receiver.

The future works which can be performed are:

i) The algorithms can also be used on colored images with some variation in time frequency.
ii) Most existing steganalysis methods for JPEG stegos usually assume the quantization table previously used and the length of the hidden message is usually fixed, and thus their conclusion about the weakness of JPEG decompressed images used as spatial-based covers seems not very interesting.
iii) The algorithms can also be used for different image formats.

REFERENCES

[1] Er-Hsien Fu, "Literature Survey on Digital Image Watermarking". *EE381K Multidimensional Signal Processing*, 19 Aug. 1998.
[2] SANS Security Essentials, (volume 1.4, chapter 4) Encryption and Exploits, 2001.
[3] Petitcolas, Fabien A.P., "Information Hiding: Techniques for Steganography and Digital Watermarking", 2000.
[4] StegoArchive, "Steganography Information, Software and News to enhance your Privacy", 2001, URL: www.StegoArchive.com
[5] Kandrapa Kumar, "Matlab Demystified", Vikas Publications.
[6] Peter Wayner, "Information Hidinig: Steganography and Water marking", 2009.
[7] Proakis and Manolakis "Digital signal processing – Principles, Algorithms, and applications," 2nd edition Maxwell- Macmillan pub.
[8] Petitcolas, Fabien A.P., "The Information Hiding Homepage: Digital Watermarking and Steganography", URL: http://www.cl.cam.ac.uk/~fapp2/steganography/
[9] Johnson Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index.html
[10] Kumar, M., Newman, R., "J3 High payload histogram neutral JPEG steganography", Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on 17-19 Aug 2010, pg no. 46-53.
[11] D. Artz, Los Alamos Nat. Lab., NM ;"Digital Steganography hiding data within data", Internet Computing, IEEE on May/Jun 2011, pg no. 75-80.
[12] S.Changder , D.Ghosh, N.C. Debnath, Dept. of Comput. Applic., Nat. Inst. of Technology, Durgapur, India ; "LCS based text steganography through Indian Languages" , Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on 9-11 July , pg no. 53-57
[13] El Safy, R.O. Zayed, H.H. El Dessouki, A Faculty of Eng., Benha Univ., Banha; " An adaptive steganographic technique based on integer wavelet transform " , Networking and Media Convergence, 2009. ICNM 2009. International Conference on 24-25 March 2009, pg no. 111-117.
[14] P. Marwaha, Infosys Technology Ltd., Bangalore, India, "Visual cryptographic steganography in images", Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on 29-31 July 2010, pg no. 1-6.
[15] Liu Jing, Kang Zhiwei, "Steganography based on wavelet Transform and modulus function" Journal of Systems Engineering and Electronics, Volume 18, Issue 3, 2007, Pages 628-632.
[16] Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, member, IEEE, "Spread Spectrum Watermarking for multimedia" in Proc. IEEE Transaction on Image Processing, Vol. 6, NO. 12, December 1997.
[17] L.F. Turner, "Digital data security system", Patent IPN WO 89/08915, 1989.
[18] URL: http://en.wikipedia.org/wiki/Spread_spectrum.
[20] Ms Suneeta Parida. Steganography – A technique of hiding information. National Conference on Advanced Computing and Communication Technology, ACCT-10.
[21] URL: http://en.wikipedia.org/wiki/Signal-to-noise_ratio
[22] URL: http://en.wikipedia.org/wiki/Associative_Memory
[23] URL: http://en.wikipedia.org/wiki/Steganography