

Comparative Analysis and Measuring Qualitative Factors using Colour and Gray Scale Images for LSB and DCT- Mid Band Coefficient Digital Watermarking

B.H. Barhate

Assistant Professor & HOD, Dept. of Computer Sci., Bhusawal Arst, Sci. & P.O.Nahata Comm. College, Bhusawal

R.J. Ramteke, PhD

Professor & HOD Dept. Of I.T, School of Computer Sciences, N.M.U., Jalgaon, Maharashtra (India)

ABSTRACT

In this paper the concept of Image Steganography is tested for Watermarking algorithms. Least Significant Bit (LSB) based spatial domain technique and Mid band Discrete Cosine Transform (DCT) domain techniques are compared. After computing the results using coefficient DCT Mid band watermarking algorithm is more secure than LSB.

Keywords

Watermarking, Discrete Cosine Transform(DCT), Least Significant Bit(LSB), Peak Signal Noise Ratio(PSNR), Mean Square Error (MSE)

1. INTRODUCTION

Information is mainly secured by Cryptography, Steganography and Watermarking. In Cryptography information is transferred into cipher text ie non readable text , In steganography information is hided and Digital watermarking is the technique of embedding a digital signal (audio, video or image) or hide a small amount of digital data in intelligible data which can not be easily removed is called digital watermarking. Digital watermarking is also called data embedding.[1]

2. IMAGE STEGANOGRAPHY TECHNIQUES

There are two type or techniques (1). Spatial domain based steganography (2) Transform domain based steganography.

2.1 Spatial Domain Based Steganography

Spatial steganography mainly includes LSB (Least Significant Bit) steganography Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image . The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message

2.2 Transform Domain Based Steganography

There are many frequenct based transforms that exist to transfer an image to its frequency domain, some of which are Discrete Cosine Transform, Fourier and Wavelet Transform.

3. ALGORITHMS OF WATERMARKING (STEGANOGRAPHY)

3.1 Image Embedding Algorithm(LSB) :

1. Read Cover object
2. Read the message to hide in cover object
3. Convert RGB image to grayscale Image
4. Shift the LSB of coverobject(ii,jj) to the value of watermark(ii,jj)

3.2 Image Extracting Algorithm(LSB) :

1. Read Watermarked image
2. Use LSB of watermarked image to recover watermark
 $\text{watermark}(ii,jj) = \text{bitget}(\text{watermarked_image}(ii,jj),1)$
3. Scale the Recovered watermark

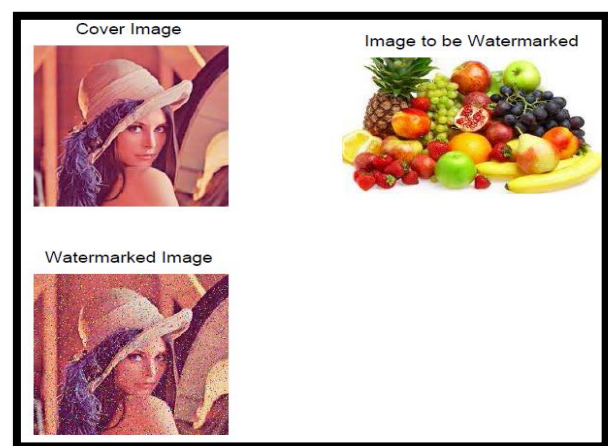


Fig 1 Watermark Embedding

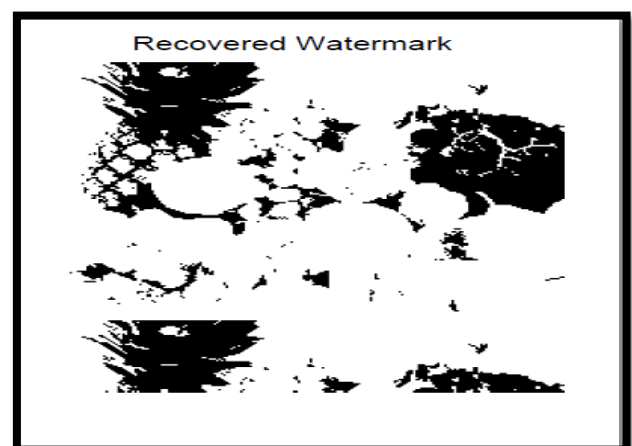


Fig 2 Watermark Extraction

MSE: 0.11 PSNR: 57.5997033

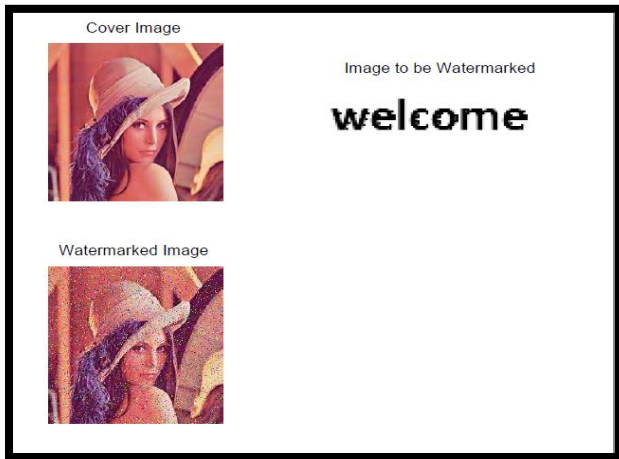


Fig 3 Watermark Embedding



Fig 4 Watermark Extraction

MSE: 0.07 PSNR: 59.9489363

Spatial domain techniques work directly on the source image by dealing with pixel intensities while embedding watermark. Though the technique is less complex, easy to implement, more capacitive but has flaws as:

- Poor robustness.
- Can be easily attached.
- Watermark can be removed or destroyed easily by applying common signal processing operations like data compression, cropping, resizing etc
- Characteristics of human perception are not taken into account.

3.3 Frequency Domain Watermarking

Transforming the signal from spatial to frequency domain is more appropriate for watermarking because of its following properties.

- Statistical independence between pixels is obtained.
- Inverse transformation evenly spreads the watermark over host image giving tough times to attackers.
- Takes HVS into consideration.

- Watermark can be embedded into significant area of host image, thus providing robustness against several attacks.
- Cropping a serious threat to spatial domain hardly impacts in transformation domain[3]

Transform Domain technique is more superior than Spatial Domain since robustness against lossy compressions and different filtering operations such as median, high-pass and low-pass, addition of noise etc . This technique gives greater assurance about quality at the receiving end. Common transform domain techniques mainly are Discrete Cosine Transform (DCT). [6]

The middle-band frequencies coefficients (FM) of an 8x8 DCT block are shown in Figure . FL is used to denote the lower frequency coefficients of the Block, while FH is used to denote the higher frequency Coefficients. FM is chosen as embedding region to provide Additional resistance to lousy compression techniques, while avoiding significant modification of the cover image. By selecting two locations from FM region from 8x8 DCT . Compare DCT (u1, v1) and DCT (u2, v2) as The DCT block will encode a “1” if DCT (u1, v1) > DCT (u2, v2); otherwise it will encode a “0”. [5][7]

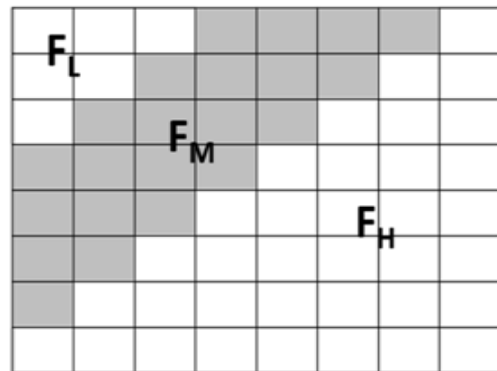


Figure 5 : DCT region for Mid-frequency

FM is chosen as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image.[7].LF, frequencies are avoided to insert secret data since human vision system is more sensible to modifications may occur in the lower frequency sub band.

1. Original DCT coefficient values.
2. Quantized DCT coefficient values.
3. New quantized DCT coefficient values.
4. The values of the binary secret bits.[8]

4. RANDOM MIDBAND EXCHANGE COEFFICIENT ALGORITHM

1. Select grayscale image that be the original image. Size of the original image is 512 × 512.
2. Determine maximum size of cover image
3. Select Watermark image , size is 32x32 up to 60x60
4. The host image is divided into a number of blocks; the size of each block is 8×8

5. Convert the watermark image in to a linear vector of '1' and '0'.
6. For each host image block compute the DCT transform coefficients.

4.1 Watermark Embedding Algorithm

In this algorithm, each 8 x 8 DCT block of an image is used to hide a single bit of watermark image. This embedding algorithm is based on some mathematical evaluation of 2 randomly selected mid band coefficients of F_m region which provides robustness to the proposed method. Algorithm is as follows:

1. If $DCT(u_1, v_1) > DCT(u_2, v_2)$ then DCT block will encode 1 otherwise 0
2. Take Inverse DCT of each block to reconstruct the watermark Image.
3. Display the gray level Watermarked image.

OR

1. Set minimum coefficient difference
2. Read cover image
3. Read message image
4. Reshape the message to a vector
5. Process the image in blocks
6. Transform block back into spatial domain
7. Apply step six to each block

4.2 Watermark Extraction Algorithm

Read Watermarked object

1. Determine size of watermarked object
2. Determine block size
3. Read original watermark
4. Process image into blocks
5. Transform blocks into DCT
6. Reshape embedded message



Fig.6 Histograms of the images

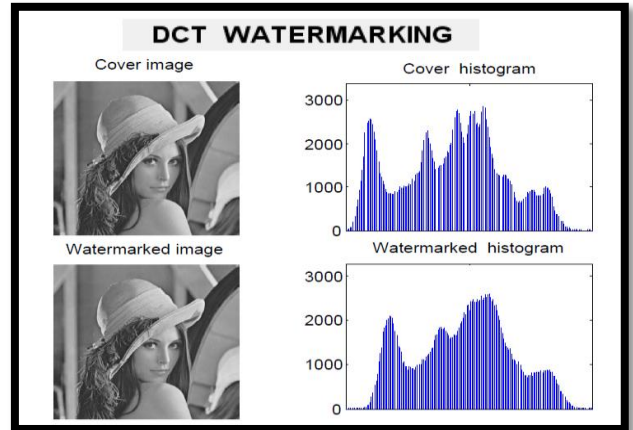


Fig. 7

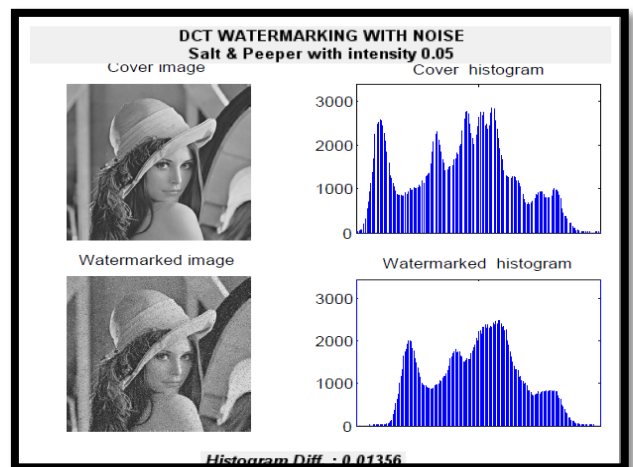
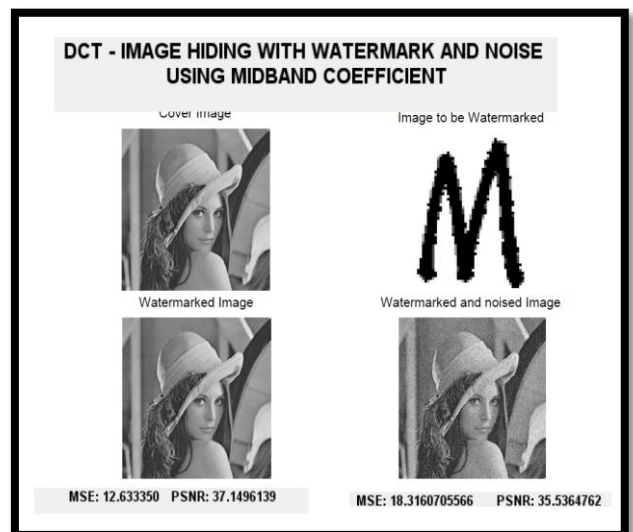


Fig.8

Fig.9 indicates the calculated Quality measures MSE and PSNR are varies if noise passes in cover image PSNR declines and MSE improves.



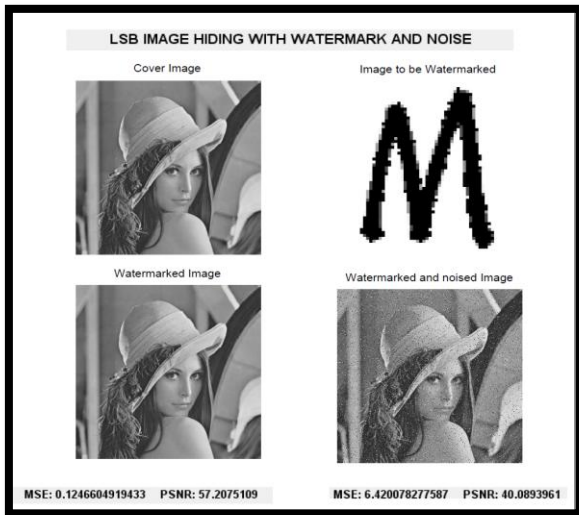


Fig.10

MSE: 12.435394 PSNR: 37.2182037

Table 1 : Effects on Images of LSB and DCT

Various Noises	LSB Algorithm	DCT Midband Coefficient Algorithm
	Recovered Images	
Without any attacks the extracted watermark		
Under the salt and pepper noise of 0.01 strength		
Under the Gaussian Filtering with sigma 0.5		

5 COMPARISONS – LSB AND DCT MID BAND

For checking security , complexity and robustness between spatial and transform domain watermarking algorithms following points are concluded .

- LSB algorithm is simple to implement than Mid band DCT algorithm .
- LSB algorithm works well for simple attacks like addition of noise but it cannot provide robustness

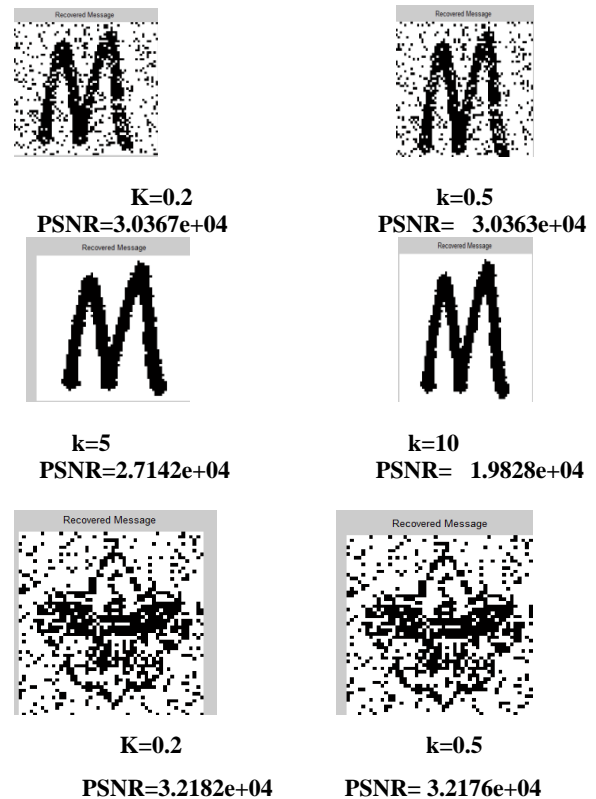
against different attacks while Mid band DCT algorithm is more robust to different attacks like filtering, addition of noise etc.

- In LSB algorithm shifting of watermark bit embedding position from LSB to MSB, the watermarked Image starts distorting while in the Mid band DCT algorithm embedding watermark in the low frequency coefficients, the watermark Image get distorted.
- In LSB algorithm the capacity of bit embedding per Image is more as compared to Mid band DCT algorithm Security in Mid band DCT algorithm is more as compared to LSB algorithm.
- LSB algorithms for watermarking can not responds or results better in strong attacks bit DCT Mid band works and results properly.

Table 1 : Comparative features

Features	LSB	DCT
Invisibility	Low	High
Payload capacity	High	Medium
Robustness against statistical attacks	Low	High
Robustness against image manipulation	Low	Medium
Independent of file format	Low	Medium
PSNR	High	Medium
MSE	Less	Medium

Following fig. shows recovered watermark from LENA image with various constant k (coefficient difference)





k=5

PSNR=2.8613e+04



k=10

PSNR=2.0599e+04



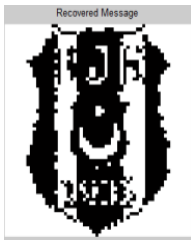
K=0.2

PSNR=2.0549e+04



k=0.5

PSNR=2.8402e+04



k=10

PSNR=3.1897e+04



k=5

PSNR=3.1902e+04

6 CONCLUSION

In this paper analysis of LSB & DCT methods has been successfully implemented and results are delivered. The MSE and PSNR of the methods are also compared. In LSB Watermarking the Quality measure PSNR is very good MSE is low and in DCT watermarking PSNR is low and MSE is medium. As per the security issue no any intruder or hacker hack secret message from DCT Watermarking hence is more secure than LSB. In the compared algorithms of LSB and DCT with midband coefficient results generated by DCT is robust for most of the common image processing attacks .The algorithm can be applied on color images.

7. REFERENCES

- [1] Dr. Ajit Preeti Kalra Sonia Dhull, “ DIGITAL WATERMARKING” , International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013 ISSN: 2277 128X, pg- 4
- [2] Gurmeet Kaur and Aarti Kochhar, “ A Steganography Implementation based on LSB & DCT” , International Journal for Science and Emerging Technologies withLatest Trends” 4(1): 35-41 (2012) , ISSN No. (Print): 2277-8136, pg 7
- [3] Shahid Bashir Dar1, Aasif Bashir Dar, “Watermarking in Frequency Domain A Review” , International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 11 November, 2014 Page No. 9215-9218, pg-4
- [4] Suchitra. B, Priya. M, Raju.J, “ Image Steganography Based On DCT Algorithm for Data Hiding” , International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 11, November 2013, ISSN: 2278 – 1323, pg-3003-3006
- [5] Mrs. Rekha Chaturvedi, Mr. Abhay Sharma, Mr. Naveen Hemrajani, Mr. Dinesh Goyal, “Analysis of Robust watermarking technique using Midband DCT domain fot different image formats” , International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012 ISSN 2250-3153, pg- 1-4
- [6] Dr. Harsh Vikram Singh, “Digital Image Watermarking Algorithm Based on DCT and Spread Spectrum”, UACEE International Journal of Advances in Electronics Engineering Vol:1 Issue:1 ISSN 2278 - 215X, pages-6
- [7] Alisha Parnami , Ankit Gupta ,Gagan Parnami ,” A Robust DCT based Digital Image Watermarking using Random Mid-band Coefficient Exchange Scheme for Gray Scale Images”, International Journal of Computer Applications (0975 – 8887) Volume 100– No.8, August 2014, pg 6-10.
- [8] Shinu, Vijay Laxmi, “ Mid Band DCT Coefficients Based Steganography”, International Journal of Scientific Engineering and Technology Research, ISSN 2319- 8885 Vol.03, Issue.48 December-2014, Pages:9838-9842