

Performance Evaluation of Image Steganography using Hybrid Technique in Frequency Domain

Kirti D. Nagpal¹, Prof. Vijay R. Wadhankar², Prof. D. S. Dabhade³

Research Scholar, Dept. of Electronics and Comm. Engineering, Agnihotri College of Engineering, Wardha, India¹

HOD, Dept. of Electronics and Comm. Engineering, Agnihotri College of Engineering, Wardha, India²

Asst. Professor, Dept. of Electronics and Comm. Engineering, Agnihotri College of Engineering, Wardha, India³

Abstract— Protection of digital multimedia content has become an increasingly important issue for content owners and service providers. The major methodology for protection of some digital content is- Steganography. Image Steganography is a process where information such as name of the creator, status, recipient, etc. is stored in the form of an image which is embedded into the host image in such a way that it will remain invisible or undetectable to a normal person. Only the intended recipient would be able to detect and remove the secret image. There are three main mutually conflicting properties of information hiding schemes: Imperceptibility, Robustness and Capacity. This paper measures the imperceptibility and robustness of the proposed system in terms of two parameters- PSNR and NC respectively. Now, while transmitting the image having some secret information embedded in the cover image, some attacks may arise on it which would degrade the quality of the secret image while extracting it. The technique is again tested against different attacks with varying attack intensities.

Keywords- Image Steganography, PSNR, NC, Attacks- Sharpening, Resize, Gaussian Blur.

I. INTRODUCTION

In the past few years there has been an explosion in the use and distribution of digital multimedia data. Day by day, the number of computers that are integrated onto a network has reached a drastic level, thus making it easier and faster to distribute the digital content onto the real world. The success of the Internet and digital consumer devices has intensively changed our society and made daily lives easier since the capturing, transmission, and storing of digital data has become extremely convenient. But along with the great advantages, advancement come up with few drawbacks as well. Nowadays, it has become very difficult to send some secret information secretly. Here comes a technique to hide an image having some crucial information into another image, known as Image Steganography. In this paper, an image steganography technique which is a combination of three techniques in frequency domain, is used. It is a hybrid combination of Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD). A watermark embedding procedure is truly imperceptible if the naked eye cannot distinguish the original data from the data with the inserted watermark. Watermark robustness accounts for the capability of the watermark to survive against signal manipulations. The amount of information that can be stored in a watermark is known as capacity. This paper intends to test the proposed system mainly for its imperceptibility and robustness without and with attack. The two major parameters – Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) are measured to evaluate the performance of the system.

II. TECHNIQUES IMPLEMENTED IN FREQUENCY DOMAIN

The image steganography can be implemented in spatial and transform domain [2][5][6]. The transform domain image is represented in terms of its frequencies; whereas, in spatial domain it is represented by pixels. Further, the image steganography techniques can be applied on individual basis

or some of the techniques can be combined and a hybrid class of steganography technique [3] can be formed. The proposed algorithm combines the properties of DWT, DCT and SVD techniques and forms a hybrid technique to increase the robustness of the algorithm.

A. Discrete Wavelet Transformation technique (DWT):

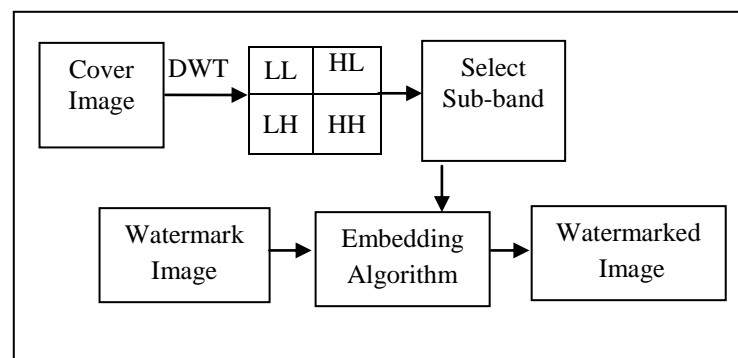


Fig. 1: General Block Diagram of DWT Technique

The Discrete Wavelet Transform (DWT) [4][6] decomposes the image into sub-images, 3 details and 1 approximation. The LL band represents the approximation of the image and is the most significant band as it carries most of the image energy. The other three bands contain the details of the image (texture of the image). The frequency bands are separated by successive filtering and down sampling of the image, first in horizontal and afterwards in vertical direction. High energy watermarks can be embedded in the regions that the human vision is less sensitive to. These regions are the high resolution detail bands (LH, HL and HH). The robustness of the watermark is increased by embedding into these bands without having additional impact on the quality of the image.

B. Discrete Cosine Transformation technique (DCT):

As shown in the block diagram of Discrete Cosine Transform in figure 2, the image is first divided into square blocks of size 4x4 for DCT [1][2][5] computation. The same can be done by blocks of 8x8 or 2x2 sizes as well. Dividing the image into blocks of 4x4 sizes provides ease of computation. Applying DCT to each block breaks the image into different frequency bands, which makes it easier to embed image steganography information into the middle frequency bands of the image. Now, DC components are extracted from each of the DCT transformed block and a single matrix is formed. This DC extracted block is modified with the watermark image and then inverse Discrete Cosine Transform is applied which forms the watermarked image.

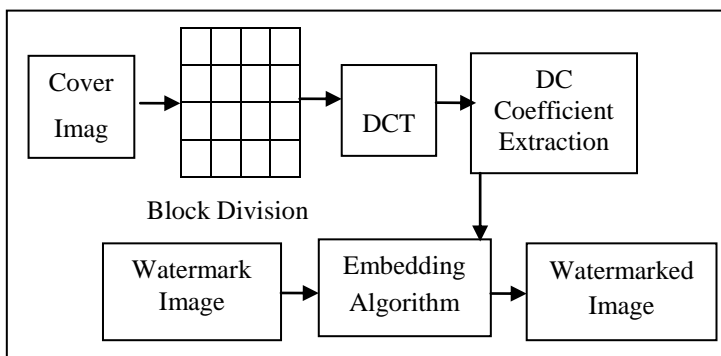


Fig. 2: General Block Diagram of DCT Technique

C. Singular Value Decomposition technique (SVD):

Singular Value Decomposition [1][3][10] is used to decompose any rectangular real or complex matrix. Every real matrix A can be decomposed into a product of three matrices as:

$$X = U S V^T$$

where, U and V are orthogonal matrices.

$$U^T U = I \quad V^T V = I \quad \text{and}$$

$$S = \text{diag} (\lambda_1, \lambda_2, \dots)$$

The diagonal entries of S are called the singular values of X with nonnegative numbers on the diagonal and zeros on the off diagonal, the columns of U are called the left singular vectors of X, and the columns of V are called the right singular vectors of X. This decomposition is known as the Singular Value Decomposition (SVD) of X. This decomposition is known as the Singular Value Decomposition (SVD) of X. The most significant information of the image is contained in the S matrix formed by the SVD technique. Embedding the watermark image into the S matrix increases the robustness of the system to a quite significant level. So, coefficients of S matrix of the cover image are modified by the coefficients of watermark image so as to obtain the watermarked image. U and V matrices are remain unaltered. The original S matrix is then replaced by the modified S matrix which improves the

capacity of the system to sustain to the attacks. This process of decomposition and embedding the watermark is depicted in the block diagram of SVD technique as shown in figure 3.

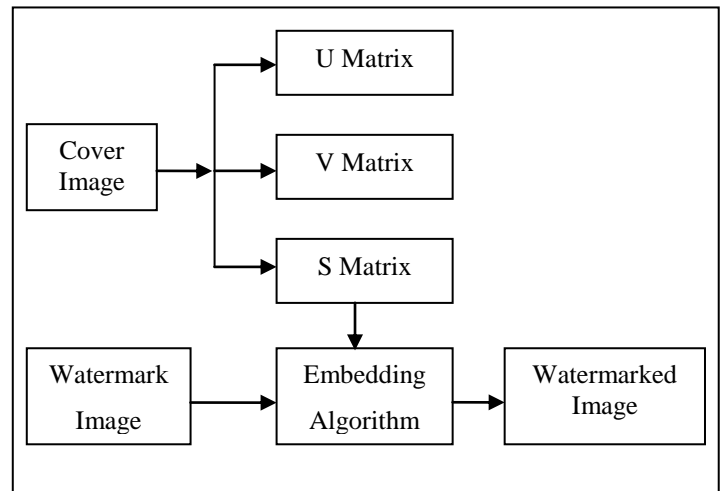


Fig. 3: General Block Diagram of SVD Technique

III. ATTACKS ATTEMPTED ON WATERMARKED IMAGES

The attacks may be due to degradations that can occur during lossy copying or due to compression of the image during re-encoding or because of change of frame rate or change of resolution etc. The following three types of attacks have been applied to the proposed image steganography system formed by the hybrid technique in frequency domain.

a. Sharpening:

Sharpening operations are used to enhance the subjective quality. Sharpening an image returns an enhanced version of the grayscale or true color (RGB) input image A, where the image features, such as edges, have been sharpened using the unsharp masking method. The boundary of an object in a gray scale image is located where the sharp changing of the gray level happens. The amount of sharpening at the Edges can be controlled by specifying the radius and amount parameters. A higher value leads to larger increase in the contrast of the sharpened pixels. Typical values for this parameter are within the range [0 2], although values greater than 2 are allowed. Very large values for this parameter may create undesirable effects in the output image.

b. Resize Attack:

Most of the time when posting a picture online or sending it via email, resizing the picture may be necessary. It is a non-trivial process that involves a trade-off between efficiency, smoothness and sharpness. In case of resize attacks, basically the size of the original image is changed by either increasing or decreasing the total number of pixels in the image, and then trying to recover the hidden information from the resized image.

c. Gaussian Blur:

A Gaussian blur is also known as Gaussian smoothing. It is the result of blurring an image by a Gaussian function. Gaussian smoothing is also used as a pre-processing stage in

computer vision algorithms in order to enhance image structures at different scales. In case of Gaussian noise, the parameter variance plays an important role in changing the content significantly. Hence, a trial is made by attacking the watermarked image with additive noise. The image is corrupted by keeping the mean value to zero and assigning different values to variance.

IV. DESIGN AND IMPLEMENTATION USING DWT-DCT-SVD

A. Watermark Embedding Procedure:

In the proposed work a colour image of size 512 x512 is considered as cover image. DWT technique is applied to decompose the colour spaces into different frequency bands using dB1 filter. Watermark size determines the selection of frequency band. Each band is divided into many blocks of size 4x4 and DCT is applied to all the blocks. In DCT transformed block the energy is compact in its DC component significantly. DC matrix is formed by collecting DC components of all the blocks and it is decomposed by SVD technique to get the singular matrix in which the singular matrix of the watermark of size 64x64 is to be hidden. After obtaining the modified DCT coefficients, the modified DCT coefficients are mapped back to their original positions and then inverse DCT and inverse DWT is performed to produce the watermarked image by concatenating the RGB planes of the color image.

B. Watermark Extraction Procedure:

To extract the watermark, the previous watermarked image is taken. The watermarked image is first split into R, G and B planes. DWT technique is applied over the image. The same band selected while embedding the watermark is taken which is divided into blocks of 4x4 sizes. DCT is applied to all these blocks of which DC components are extracted from all the DCT transformed blocks. Another block is formed by combining only the DC components. Now, SVD is applied over this DC block. On the other hand, SVD technique is applied over the host image. The singular matrix of the watermarked image is compared with the host image singular values. The obtained singular values are then combined with the orthogonal matrices of watermark obtained from the watermarked image to extract the watermark.

V. RESULT ANALYSIS

Image steganography is implemented on different images using hybrid technique DWT-DCT-SVD. In order to test the quality of watermarked image and extracted watermark both subjective and objective measurements are used as shown in Table I. Typical values for the PSNR are between 30 and 50 dB, provided the bit depth is 8 bits. Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB [15].

The proposed algorithm was implemented using MATLAB 2013a 32bit (win32) and was tested on Windows 7 and Windows 8.1 platforms. A color image of 512x512 is used as the cover image to form the watermarked or stego image, concealing a 64x64 watermark or secret image. Both the watermark image and the cover image are in the .jpeg format.

Selected embedding intensity value is 0.25 for all frequency bands.

To check the robustness of the system against various attacks, the proposed hybrid technique DWT-DCT-SVD is tested for different attacks. Cover test image 1 as shown in Table I is selected with the same watermark image as taken earlier. The PSNR and NC values obtained after the effect of attacks on the watermarked image are shown in the Table II.

TABLE II. PSNR AND NC VALUES FOR DWT-DCT-SVD WITH ATTACK

Test Image Number	Attack	PSNR	NC
1	Sharpening	31.3584	0.898627
	Resize (By half)	38.9725	0.673421
	Gaussian Blur	49.6768	0.624850
2	Sharpening	31.3789	0.783503
	Resize (By half)	36.9596	0.676775
	Gaussian Blur	48.0952	0.776659
3	Sharpening	39.4234	0.667204
	Resize (By half)	37.3265	0.672678
	Gaussian Blur	43.4538	0.500087

Table III shows the values of PSNR and NC obtained by varying the strength of the Sharpening attack. The parameter radius is kept constant at 2 and the strength of sharpening is varied by changing the value of parameter amount as indicated in the table III.

TABLE III: RESULTS WITH DIFFERENT STRENGTHS OF SHARPENING ATTACK

Sharpening (DWT-DCT-SVD)		
Strength of Sharpening	PSNR	NC
0.8	34.1592	0.814371
1	33.9947	0.813696
2	33.2372	0.805412
2.5	32.9036	0.802158
3	32.5691	0.798379
3.5	32.2318	0.793406
4	31.9131	0.788232

Table IV shows the values of PSNR and NC obtained by adding Gaussian blur attack to different levels by keeping noise mean as 0 and changing the noise variance.

TABE IV: RESULTS OF DWT-DCT-SVD WITH DIFFERENT INTENSITIES OF GAUSSIAN BLUR ATTACK

Gaussian Blur (DWT-DCT-SVD)		
Noise Variance	PSNR	NC
0.0001	49.6521	0.623790
0.001	49.6748	0.624932
0.01	49.8074	0.629962
0.05	50.0981	0.637996
0.1	50.2929	0.642834
0.5	50.7938	0.657562
1	50.9215	0.662911

VI. CONCLUSION

The PSNR values obtained were good with the hybrid technique DWT-DCT-SVD, thus indicating good imperceptibility. NC values were found around 0.99 in all the images giving good quality of extracted watermark showing quite high robustness of the proposed system. Also, while experimenting with the effect of various attacks made on the watermarked image, the Normalized Correlation values obtained are found to be good. The robustness of the proposed hybrid technique DWT-DCT-SVD was found to be quite high such that it gives quite acceptable objective values even if the intensity of various attacks increased as shown in Table III and IV.

REFERENCES

[1] Kirti D. Nagpal, Prof. D. S. Dabhade, "Analysis of Wavelet Based Digital Image Steganography using Hybrid Technique in Frequency Domain," International Journal on Recent and Innovation Trends in Computing and Communication, Volume .3, Issue 5, May 2015.

[2] Kirti D. Nagpal, Prof. D. S. Dabhade, "A Survey on Image Steganography & its Techniques in Spatial &

Frequency Domain" International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue: 2, February 2015

[3] C. S. Rawat, Sneha M. Shivamkuty, 'Watermarking of Images using Hybrid Technique', International Technological Conference-2014, International Journal of Application or Innovation in Engineering & Management

[4] Vijay Kumar, Dinesh Kumar, 'Performance Evaluation of DWT Based Image Steganography' IEEE 2nd International Advance Computing Conference 2010

[5] Navnidhi Chaturvedi, Dr. S .J. Basha, 'Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the Basis of PSNR', International Journal of Innovative Research in Science, Engineering and Technology, December 2012

[6] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, 'Implementation of Image Steganography Using 2-Level DWT Technique', International Journal of Computer Science and Business Informatics, May 2013

[7] M.Vijay, V.Vignesh Kumar, 'Image Steganography Method Using Integer Wavelet Transform', International Journal of Innovative Research in Science, Engineering and Technology, 2014

[8] Gurmeet Kaur, Aarti Kochhar, 'Transform Domain Analysis of Image Steganography', International Journal for Science and Emerging Technologies with Latest Trends, 2013

[9] Barnali Gupta Banik Prof. Samir K. Bandyopadhyay, 'A DWT Method for Image Steganography', International Journal of Advanced Research in Computer Science and Software Engineering, June 2013

[10] N.Anil Kumar, M.Haribabu and Ch.Hima Bindu, 'Novel Image Watermarking Algorithm with DWT-SVD', International Journal of Computer Applications Volume 106 – No.1, November 2014

[11] Mehdi Hussain and Mureed Hussain, 'A Survey of Image Steganography Techniques', International Journal of Advanced Science and Technology, May 2013







[12] T. Morkel, J.H.P. Eloff, M.S. Olivier, 'An Overview of Image Steganography', Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria, South Africa

[13] Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, 'A Review of Different Techniques on Digital Image Watermarking Scheme', International Journal of Engineering Research, Volume No.2, Issue No.3, pp : 193-199

[14] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, 'Image Steganography Techniques: An Overview', International Journal of Computer Science and Security (IJCSS), Volume 6, Issue 3, 2012

[15] <https://en.wikipedia.org/wiki?curid=128145>

TABLE I: PSNR AND NC VALUES FOR HYBRID TECHNIQUE USING DWT-DCT-SVD IN HL BAND FOR DIFFERENT COLOR IMAGES (WITHOUT ATTACK)

DWT-DCT-SVD						
Test Image No.	Cover image	Watermark	PSNR (dB)	NC	Watermarked Image	Extracted Watermark
1		HK	36.8469	0.998921		HK
2		HK	30.7657	0.997639		HK
3		HK	33.1021	0.997788		HK