

A Robust Image Watermarking Technique Using Luminance Based Area Selection and Block Pixel Value Differencing

Jasvinder Singh¹, Mehak Aggarwal², Kulbhushan Singla³

¹Student M.Tech Dept. of Computer Science and Engineering, Lala Lajpat Rai Institute of Engineering & Technology, Moga, Punjab, India

²Associate Prof. Dept. of Computer Science and Engineering, Lala Lajpat Rai Institute of Engineering & Technology, Moga, Punjab, India

³ Professor Dept. of Electronics and Communication Engineering, Guru Teg Bahadur Khalsa Institute of Engineering & Technology, Chhapian Wali, Malout, Punjab, India

Abstract :- This work presents a digital image watermarking technique. It is a semi-blind process to insert invisible watermarks aimed towards strengthening the robustness, imperceptibility and security of watermark embedded in the watermarked image. In direction to achieve the mentioned objectives, this work luminance based area selection and block pixel value differencing. Watermark is embedded in blocks pixels of image based on the difference of two pixels. Calculated inter pixel differencing two pairs with highest difference values are selected for embedding. This highest values of difference is compared in range table and find the maximum number of bits of information. Thus, The Quality of image is maintained by using block pixel value differencing. This method improves the embedding capacity and makes the information undetectable. The proposed algorithm is quantitatively validated using three performance metrics namely peak signal to noise ratio, mean squared error and bit error rate. This approach is tested against variety of attacks and filter which shows a great ability to preserve the watermark against these attacks.

Keywords - Color image, PVD, log average luminance, MSE, PSNR, BER, watermarking techniques

1. INTRODUCTION

In recent years, unauthorized distribution of digital media such as audios, videos and images has become the most important challenge that faces media copyright protection. The digital communication technology, like internet technology confronts various troubles related to the privacy and security of the data. Security techniques are required because of illegal access of data without permission. Many techniques are used for providing the security of digital data like encryption, decryption, cryptography, steganography and digital watermarking. Authentication and information hiding and proof ownership have also become important issues. To accomplish these issues, watermarking technology is used. Digital watermarking [1] is a method for embedding some secret information and additional information in the cover image. Digital watermarking addresses the growing concerns of

theft and tampering through the use of advanced signal processing strategies to embed copyright and authentication information within multimedia content. Digital watermarking is use to authentication, owner identification, content protection and copyright protection. In other words, a watermark is a pattern of bits inserted into multimedia data such as digital image, audio or video file that helps to identify the file's copyright information. Watermark can provide information that serves as proof of ownership. Watermark may be a visible signature or logo placed over an image to determine the owner of that image.

2. LITERATURE REVIEW

Digital watermarking techniques are classified based on two working domain spatial domain and frequency domain. The spatial domain techniques works directly on pixels. It embeds the watermark by modifying the pixels value. Most commonly used spatial domain techniques are LSB and PVD. In LSB technique, these approaches use minor changes in the pixel value intensity. The watermark data is embedded into least significant bits of pixels. In PVD, method, it uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. It offers the advantage of conveying a large amount of message, while still maintaining the consistency of an image characteristic after data embedding. Most commonly used transform domain techniques are DCT, DWT and SVD [9]. All these techniques work on frequency components of image to embed watermark data. Transform domain techniques [2] embed the watermark by modifying the transform domain coefficients.

3. LUMINANCE BASED AREA SELECTION AND BLOCK PIXEL VALUE DIFFERENCING

We proposed a new technique for watermarking embedding in digital image. The area for embedding is selected using luminance based location method [2]. J. Hussein [6], in his work had developed a method for selecting the embedding area in cover image using

Luminance of image. The image of size 512X512 is divided into 8x8 blocks and the following operations are needed and must be performed to accomplish the embedding and extracting processes. RGB YCbCr conversion

3.1 RGB to YCbCr Conversion

The RGB color space is converted to YCbCr color space for each 8x8 block using the equations (1):

$$\begin{aligned}
 Y &= 0.299 \times R + 0.587 \times G + 0.114 \times B \\
 C_b &= 0.596 \times R - 0.275 \times G - 0.321 \times B \\
 C_r &= 0.212 \times R - 0.523 \times G - 0.311 \times B
 \end{aligned}
 \tag{1}$$

where R, G, and B are red, green and blue components of RGB color space respectively.

3.2 Log-Average Luminance

The block selection criteria are dependent on log-average luminance for the entire image and log-average luminance for each block. The log-average luminance Y_{avg} is calculated as shown in the equation (2)

$$L_{avg} = \exp(\sum \log(\delta + Y_{x,y})/N) \tag{2}$$

L_{avg} : Log-average luminance

$Y_{x,y}$: Luminance Y of the pixel at x,y

δ : A small value to avoid taking the log of a completely black pixel whose luminance is zero

N: The number of pixels in the image.

3.3 Block Selection Criterion

When 512x512 host image is divided into 8x8 blocks, 4096 blocks are produced. Since the watermark size is 32x32 pixels and if we consider minimum embedding capacity of 1 bit, each block can be used to embed 32 bits minimum and thus we require only 256 blocks to embed the entire watermark.

After finding the log-average luminance for the entire image and for each block; the best blocks are chosen from the blocks that have log-average luminance closer to the log-average luminance of the entire image [6]. To do that we select the blocks with log average luminance in the range $[Y_{avg}-\beta, Y_{avg}+\beta]$ where Y_{avg} is the log average luminance of the image and β is the minimum floating-point value that is enough to determine adequate number of blocks.

3.4 Embedding process

Now in selected blocks separate RGB components of color image. We can embed our watermark using block pixel value differencing. In this method, from a selected block, we further divided the block into segments of 2x2 pixels (for each color plane). In each segment, we calculated inter pixel differences and two pairs with highest difference values are

selected for embedding the information. This highest values of difference is compared in range table and we find the maximum number of bits of information (from secret message). This method not only improves the embedding capacity, but also makes the information undetectable. The complete embedding and extracting method is described in following section.

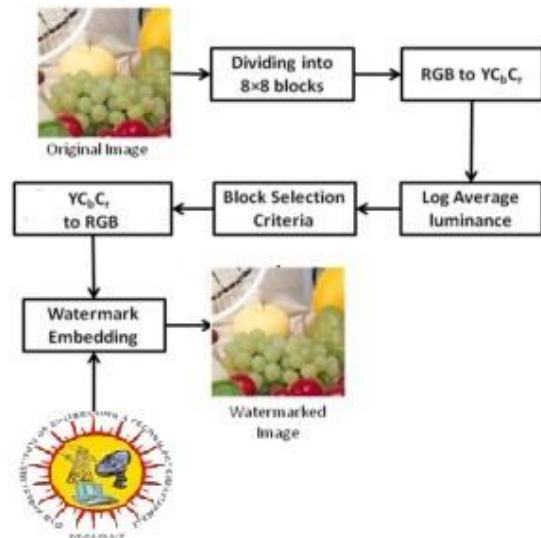


Figure 1 Watermarking Embedding

3.4.1 Embedding Algorithm

- i. Read this Cover –Image and separate its RGB components.
- ii. Divide the selected block of size 8X8 into the segments of 2X2 pixels.
- iii. Calculate the difference value d_i' for each segment of two consecutive non-overlapping pixels $p(i)$ and $p(i+1)$ and is given by $d_i = |p(i) - p(i+1)|$
- iv. Now find the two highest difference value among four difference values of each colour plane which are not made by common pixel value.
- v. Making the optimal range Table R_i for the d_i such that

$$R_i = \min (u_i, d_i), \text{ where } u_i \geq d_i$$

This is the optimum range where the difference lie.

- vi. Compute the number of secret data $bits 't'$ to be embedded in selected pixel pair from the width w_i of the optimum range, can be defined as

$$t = \log_2 w_i.$$

- vii. Read t' bits from secret message and convert it into its decimal value b.

- viii. Now finding the new difference value d_i' using $m = d_i' = l_i + b$.
- ix. Modify the values of p_i and P_{i+1} by the original PVD method as discussed in review section. (Where p_i and P_{i+1} are R and B components). Here only R and B components are selected because these two components add very little to Y value and uniformly distributing the difference does not alter their values to much extent and Y values remains almost same
- x. Now repeat the steps for next segment in selected block and repeat the process for all selected blocks depending upon the size of watermark.

Range table:-

Range	Difference	Number of bits
0-8	8	2^3
9-16	8	2^3
17-32	16	2^4
33-64	32	2^5
65-128	64	2^6
129-256	128	2^7

3.4.2 Quality measurement

The quality of the watermarked image is measured by finding Mean Square Error and peak signal to noise ratio (PSNR) values of the watermarked image and the original image. Lower MSE values and higher PSNR values imply good embedding results.

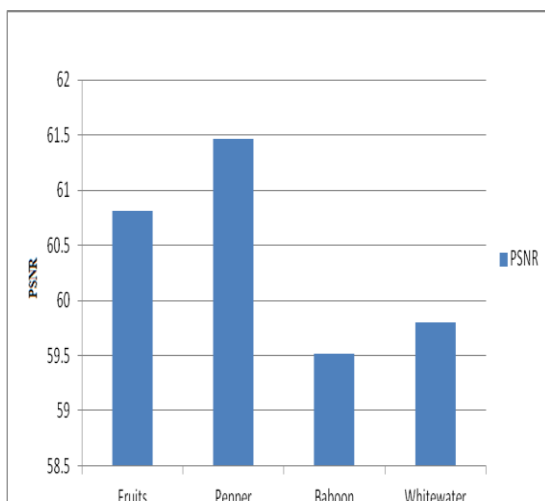


Figure 2 PSNR values of various images

3.4.3 Extraction Algorithm

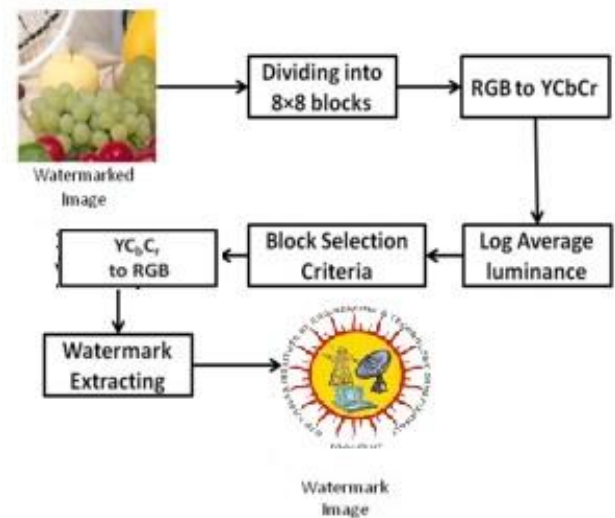


Figure 3 Extraction process

For the extraction process, the blocks are selected in the same manner as discussed in embedding procedure. While decoding the data from the watermarked-image, the range table, which is used at encoding, is required. The following steps used for extracting the hidden data:

- i. Read this Cover -Image and separate its RGB components.
- ii. Divide the selected block of size 8X8 into the segments of 2X2 pixels.
- iii. Calculate the difference value d_i' for each segment of two consecutive non-overlapping pixels $p(i)$ and $p(i+1)$ and is given by

$$d_i = |p(i) - p(i+1)|$$
- iv. Now find the two highest difference value among four difference values of each colour plane which are not made by common pixel value.
- v. Compute the b' by $b' = d_i - l_i$. Convert b' into binary of t' bits, where $t = \log_2 w_i$. These t bits are the hidden secret data.

Now repeat the process for other pixels by moving right to left and then to top for an image and extract the message bits before the previously extracted bits. After that these binary information is converted in to watermark image

4. Experimental Results

The imperceptibility and robustness of the proposed scheme demonstrated is using MATLAB, quality measures such as are used. The images used to calculate the PSNR (peak signal to noise ratio), BER (bit error ratio) and MSE (mean square error) are fruits, peppers, Baboon, whitewater images and the results of proposed method on these images have been described in Table 1. The proposed method is

tested with various attacks and the quality parameters like highpass, lowpass, Gaussian, median and JPEG compression are listed in Table 2. The result values of Table 1 clearly indicate the robustness and quality of the image is not degraded. The efficiency of the proposed method in this paper is compared against DCT method.

of the embedded watermark. The blocks for embedding are selected using luminance of the image. The watermark is embedded using block pixel value differencing, which is more effective than DCT method. only the blocks with log-average luminance close to the log-average luminance of the entire image are used to embed the watermark. The test results show that these blocks do not degrade the image when the pixels' luminance value is increased or decreased. The experimental results show a high degree of robustness against a number of unintentional attacks such as highpass filter, lowpass filter, Gaussian, median, impulse and JPEG compression. The efficiency of the embedding process is measured by using PSNR value between the original and the watermarked image.

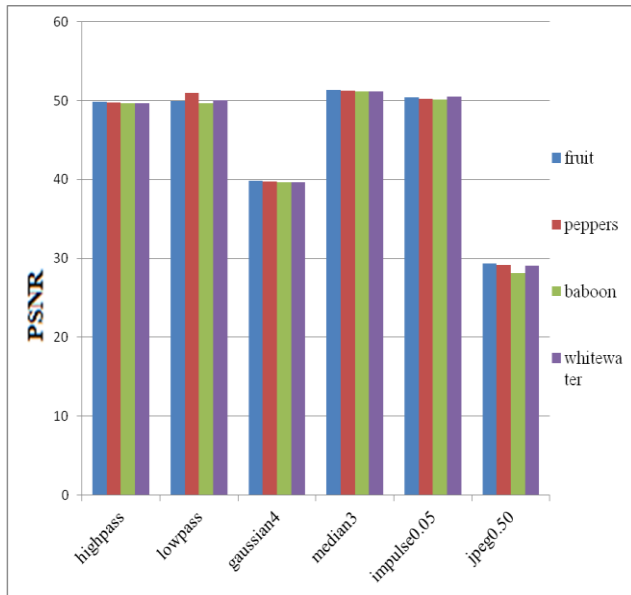


Figure 4 PSNR values after various attacks

Table 1: Comparison of Results of Hussein's and Proposed Method

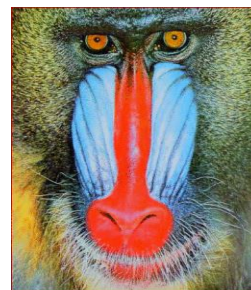
Images	J.A.Hussein[6] method	Proposed Method		
	PSNR	PSNR	MSE	BER
Fruits	32.512	60.809	0.217	0.0164
Peppers	35.000	61.460	0.187	0.0163
Baboon	34.990	59.510	0.293	0.0168
White Water	32.650	59.797	0.274	0.0167



Fruits Image



pepper Image



Baboon Image



Whitewater Image



Watermark Image

5. CONCLUSION

In this research paper, a new approach has been proposed. This approach achieves high imperceptibility and robustness

Table 2: Values of Various Parameters after Attacks

Images		Attacks					
		Highpass	Lowpass	Gaussian4	Median 3	Impulse 0.5	Jpeg 0.50
Fruits	MSE	17.0518	19.7868	27.0390	15.4781	16.5282	37.5176
	PSNR	49.8845	49.9668	39.8655	51.3963	50.3883	29.3479
	BER	0.0200	0.0202	0.0251	0.0195	0.0198	0.0341
Peppers	MSE	17.8893	10.9906	27.9048	16.3753	17.4190	38.4130
	PSNR	49.7523	50.9845	39.7286	51.2545	50.2477	29.1999
	BER	0.0201	0.996	0.0252	0.0195	0.199	0.342
Baboon	MSE	18.5009	18.4421	28.6055	16.9961	18.0203	39.0512
	PSNR	49.6582	49.6672	39.6209	51.1589	50.1552	28.1078
	BER	0.201	0.0201	0.0252	0.0195	0.0199	0.0344
White Water	MSE	18.5054	16.1416	28.6351	17.0277	18.0790	39.1310
	PSNR	49.6575	50.0329	39.6164	51.1541	50.5463	29.0956
	BER	0.0201	0.0200	0.0252	0.0195	0.0199	0.0344

Table 3: Watermark extract using median filter after adding Impulse noises

Images		Impulse(0.10)	Median filter(3)
Fruits	MSE	39.6673	7.8026
	PSNR	20.8411	52.8480
	BER	0.0480	0.0189
Peppers	MSE	38.2848	7.0640
	PSNR	21.1668	53.0171
	BER	0.0472	0.0189
Baboon	MSE	38.7398	6.2177
	PSNR	21.0569	53.2194
	BER	0.0475	0.0188
Whitewater	MSE	38.8564	7.0485
	PSNR	21.1048	52.3472
	BER	0.476	0.0188

REFERENCES

[1] Shraddha S. Katariya, Digital Watermarking: Review, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 2, February 2012 .

[2] Agarwal Aditi, Bhadana Ruchika and Chavan Satishkumar, "A Robust Video watermarking Scheme using DWT and DCT" International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 1711-1716 (2011)

[3] Chan Pik-Wah and R. Lyu Michael, "A DWT-based Digital Video Watermarking Scheme with Error Correcting Code" Information and Communications Security Volume 2836 of the series Lecture Notes in Computer Science pp 202-213 (2003)

[4] Gupta Preeti, Cryptography based digital image watermarking algorithm to increase security of watermark data" International Journal of Scientific & Engineering Research, Volume 3, Issue 9, (2012)"

[5] J.A.Hussein,Luminance-based Embedding Approach for Color Image Watermarking, I.J. Image, Graphics and Signal Processing, 2012, 3, 49-55.

[6] J. A. Hussein, Spatial Domain Watermarking Scheme for Colored Images Based on Log-average Luminance, Journal of Computing, vol. 2, No. 1,2010, pp. 100-103.

[7] Mandal J. K. and Das Debashis, "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow." CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 93-102,(2012)

[8] Mohan B.Chandra Kumar S. Srinivas, "A Robust Image Watermarking Scheme using Singular Value Decomposition" JOURNAL OF MULTIMEDIA, VOL. 3, NO. 1,(2008)

[1] Md. Maklachur Rahman, A DWT, DCT and SVD based watermarking technique to protect the image piracy, International Journal of Managing Public Sector

Information and Communication Technologies
(IJMP ICT) Vol. 4, No. 2, June 2013.

- [2] Saxena Divya, " Digital Watermarking Algorithm based on Singular Value Decompositio and Arnold Transform" International Journal of Electronics and Computer Science Engineering ISSN- 2277-1956/V1N1-22-27(2012)
- [3] Tang Chih-Wei and Hangin Hsueh-Ming, "A robust digital image watermarking scheme that combines image feature extraction and image normalization"IEEE Transactions on Signal Processing (Volume: 51, Issue: 4 , Page(s): 950 - 959)(2003)
- [4] Yassin¹ Nisreen I., Salem² Nancy M., and Adawy Mohamed I. El, "Block Based Video Watermarking Scheme Using Wavelet Transform and Principle Component Analysis" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3,(2012)