A Novel Image Watermarking Algorithm With Enhanced Security

Miss. Megha Kashyap, Mr.Deepesh Sharma

Abstract-

The main idea of this paper is to design a novel watermarking algorithm for increasing the security so that no other person except the intended person extract the watermark from the image .In this paper cover image is first encrypted using scanning operation and then watermark is embedded Various analysis has been done to test the proposed algorithm in extracting the watermark from the watermarked image.

Keywords :

Digital watermarking, wavelets, embedding, extraction, correlation, scanning, spread spectrum, PSNR.

I. INTRODUCTION

The increasing use of internet has led everyone of us to obtain the copyrighted multimedia content quite easily. Protecting these multimedia content from unauthorized person has become the prime motive for the researcher now a days. Digital Watermarking is such type of method which are used to secure the digital content by embedding the watermark or digital signature in a digital content in such a way that only authorized person can extract and detect the watermark and hence make a decision about the data. Watermark can be any types of meaningful information or logo of the company which can be used as copyright protection. Watermarking algorithm must be clever enough to hide the information inside the digital content without producing any appreciable distortion (Artifacts)and at the same time it must survive under any kind of alteration of digital content. In a broader sense the image watermarking techniques can be divided in to two categories: frequency domain techniques and frequency domain techniques. The frequency domain technique first divide the image into various frequency domain coefficient [1], [2], [3], [4], [5], [15] using transform such as discrete fourier transform (DFT), discrete cosine transform (DCT), or discrete wavelet transform (DWT). Once the image is transformed into different frequency coefficient then the watermark is embedded in these transformed coefficient and then by applying the inverse transform, watermarked image [6], [7] is obtained.

II. DISCRETE WAVELET TRANSFORM

The inability of Fourier transform to provide the time information of the signal has made it ineffective in signal processing [8].This problem can be eliminated by using discrete wavelet transform (DWT) which is frequency domain technique [9] that converts the cover image into different frequency coefficient or divides [10] the image into different types of spectrum (Low Level (LL), Mid Level (LH, HL), High Level (HH). After the decomposition suitable spectrum is used for embedding the watermark with cover image. Finally the coefficients are inverse transformed to obtain watermarked image.

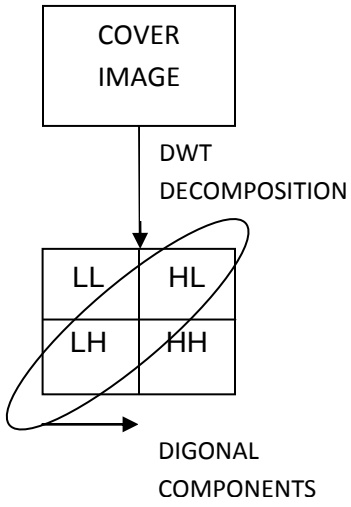

Figure 1

III. SCANNING METHOD

SCAN[11-13] is a formal language based method of accessing or arranging the position of pixels in an image. Using SCAN language, large number of scanning path can be generated. SCAN is actually a group of formal language and can be termed as Simple SCAN, Generalized SCAN, Extended SCAN. Each SCAN language follows some basic rules and grammar. There are some basic pattern of scanning and rule in each SCAN language which are used to generate some simple scanning pattern which later on can be used to generate complex scan pattern. In this proposed method four basic scan pattern has been used which are known as continuous diagonal (D), continuous raster (C) ,continuous orthogonal(O), spiral(S).Each of these basic pattern can have eight different transformations which can be numbered from 0 to 7.Transformation 0,2,4,6 are the reverse transformation of 1,3,5,7.Different types of basic scanning pattern[16] is shown in figure

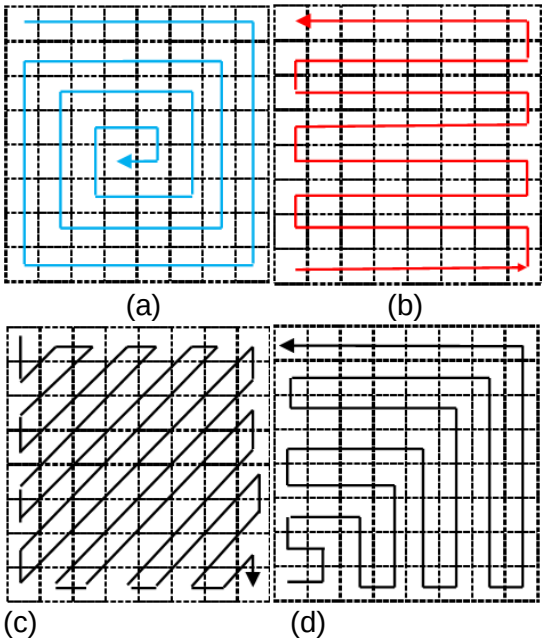

Figure: 2 (a) Spiral (b) Raster (c) Diagonal (d) Orthogonal

We can apply each of these basic pattern individually in single image or alternatively divide the image into different parts and apply these basic pattern in different parts.

A. *Partition Pattern*

Partition pattern define the order by which each subregions of the image are scanned and these partition order are denoted by letter A,B, C and E. Each partition order can also have six different transformations or pattern.

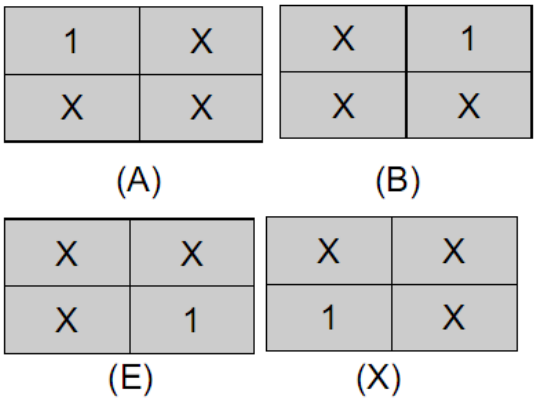

Figure 3 Partition order for Different letter

Here letter A represent the partition order which starts from left upper (denoted by 1). And goes to the rest of the three part in 6 different ways or in other words has 6 different transformation.

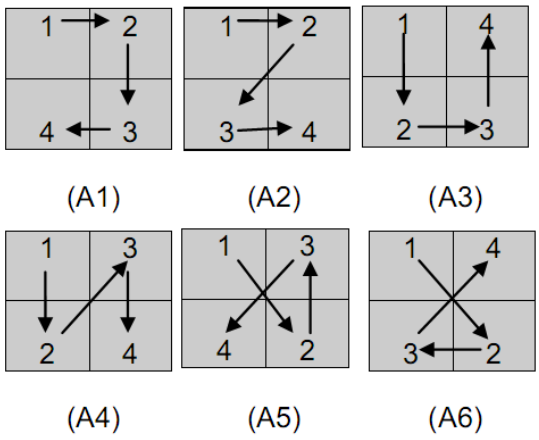

Figure 4 Partition pattern for 'A'

B. Key Generation

In order to generate a key for this encryption and decryption we encode all the scanning pattern and its eight-transformation as C1-C8(for continuous raster), D1-D8(for Diagonal),O1-O8(for orthogonal),S1-S8(for Spiral).

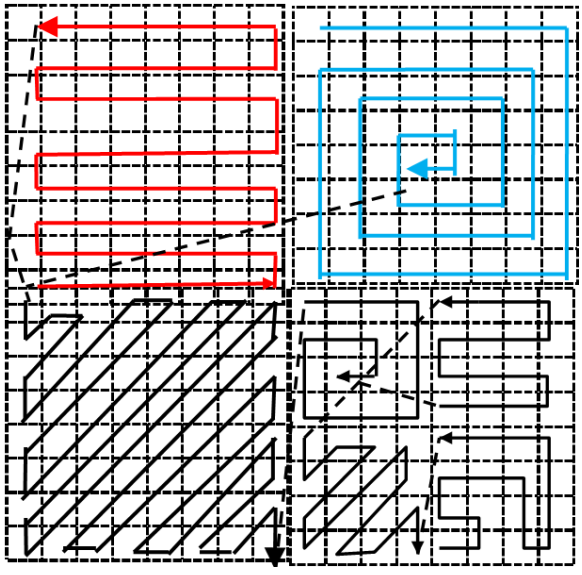

Figure 5 SCAN Pattern Diagram

In a similar way in this method,4- different partition order (A,B,E,X) and its six transformation are being used therefore it can be encoded as A1-A6,B1-B6,E1-E6,X1-X6.

For example the key for following figure is shown below

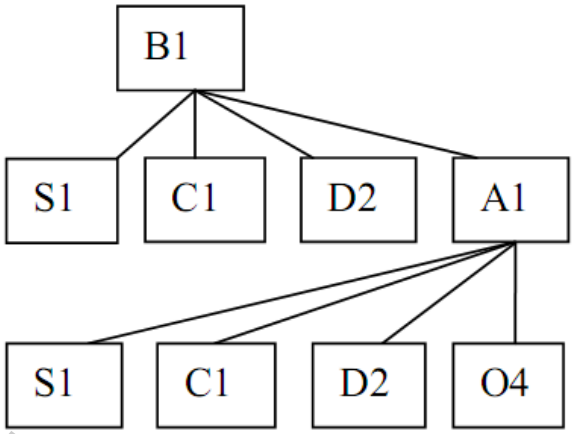

Figure 6 Encryption Key Generation

IV. SPREAD SPECTRUM TECHNIQUE

The simplest spatial-domain image watermarking technique is to embed a watermark in the least significant bits (LSBs) of some randomly selected pixels. The watermark is invisible to human eyes but the watermark can be easily destroyed if the watermarked image is lowpass filtered or removing (zero out) the least significant bits of the pixel or upon JPEG compression. To overcome the limitations in watermarking due to methods like LSB (least significant bit) substitution and to make the system more robust against attacks, the watermark can be spread across the cover object by using more number of bits than the minimum required. This scheme of hiding the data ensures the survival of watermark under various attacks due to redundancy.

Generally the message used to watermark is a narrow band signal compared to the wide band of the original image(cover image). Spread spectrum techniques [1] applied to the message allows the frequency bands to be matched before

embedding the watermark through the original image. Spred spectrum uses secrete key to control a pseudonoise generator. Pseudo noise sequences are used for watermarking because of their very good correlation properties, noise like characteristics, easier to generate and resistance to interference. Pseudorandom sequences are used as the spreading sequences. Pseudonoise is generated by using matlab function rand with initial seed and round the random numbers to its nearest integer and thus generating 0 and 1 [2].

V. PROPOSED METHOD

A. *Embedding Process*

Proposed watermark embedding process consist of two phase. In the first phase the cover image is encrypted using scanning technique. Scanning technique changes only the pixel position (not pixel value) of the cover image Once the cover image is encrypted using scanning techniques then watermark is embedded in the blue component of encrypted cover image using spread spectrum technique. Blue component of image has been chosen because it is least perceptual to human eye[4]. In order to embed the watermark in a cover image using spread spectrum technique, first of all a pseudorandom sequences is generated by providing the key as the initial seed.This sequence is added to the horizontal and vertical DWT coefficients[1] (HL, LH) of the original image according to the equation (1)

$$IW(x,y) = I(x,y) + k \times pn(x,y) \quad \text{if } W=0$$
$$= I(x,y) \quad \text{if } W=1$$
$$\text{.....(1)}$$

Where

I(x,y) = DWT coefficient of original image

IW(x,y)=DWT coefficient of watermarked

K= gain factor

W=watermark bit

pn(x,y)= pseudorandom sequence

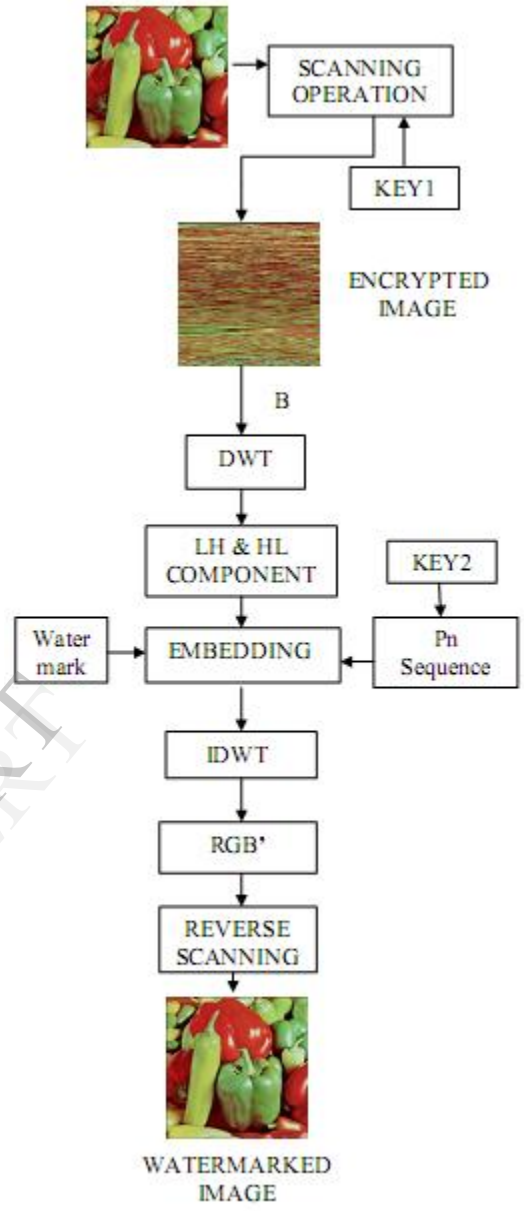

Figure 7 Embedding Operation

Gain factor decides the invisibility as well as the robustness of the watermarked image .The robustness of the watermarked image increases with the increase in k but increasing k, degrade the quality of the watermarked image, therefore it is selected carefully. and then reverse scanning operation is performed to get back the original cover image .This cover image has embedded watermark in it.

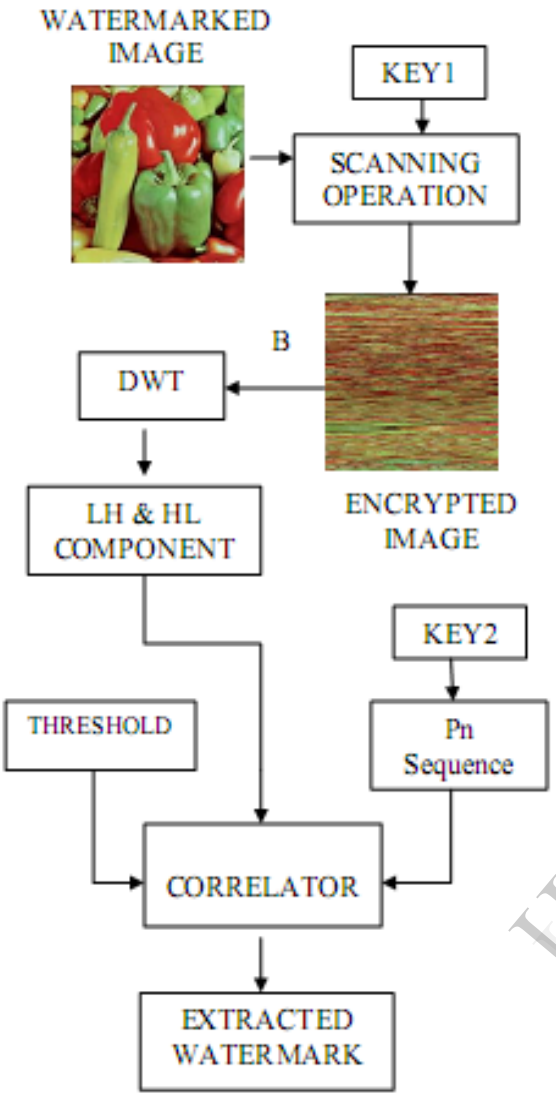

Figure 8 : Extraction Process

The whole extraction process is shown in figure 8. Correlation [1],[14] is used to extract the watermark

Since in this method two key are used one for scanning based image encryption and second is for pn sequence generator, therefore security of this watermark gets enhanced double fold.The person who knows both the key is only able to extract the watermark.

B. Extraction Process

The extraction process is summarized as -

1. Get the Watermarked Image.
2. Using key1 encrypt the watermarked Image.
3. Get the Horizontal and Vertical DWT component of encrypted image.
4. Generate the pn sequence using key2.
5. Find the one dimensional Correlation matrix1 between Horizontal component and pn sequence.
6. Find the one dimensional Correlation matrix2 between vertical component and pn sequence .
7. Find the correlation matrix by formula Correlation=Correlation matrix1+Correlationb matrix2.
8. Set the watermark image as

WM=0 if correlation >mean correlation
=1 if correlation <mean correlation

VI. EXPERIMENTAL RESULT

Proposed method is implemented in the computer having dual core processor and 2GB RAM. In order to test the performance of proposed method in extracting the watermark, PSNR is computed between original and extracted watermark for different values of gain factor k and for different size of cover image and is shown in Table 1 and Table 3.To test the effect of watermark on the quality of cover image, PSNR between original and watermarked image is computed for different size of k and for different size of cover image and is shown in Table 2 and Table 3.Moreover execution time of proposed method is also computed to check the speed of proposed method and is shown in Table 4

Figure 9 Watermark

abcd

Figure 10 (a) Original Image (b) Original Image after Scanning Encryption (c) Watermarked Image (d) Extracted Watermark

From these table it is clear that as the value of k is increased from .1 to .7, the PSNR between original and extracted watermark is increased which clearly indicate that the quality of extracted watermark is increased as k is increased. On the other hand the quality of watermarked image is decreased as the k is increased which is shown by decreasing value of PSNR in table 2.From these table it is clear that the optimum value of k is .5 for which the quality of extracted watermark and watermarked image is very good.

It is clear from the analysis that this method of watermarking perform very well under different parameter condition and encrypting the cover image using scanning techniques doesn't affect the performance of watermarking algorithm and at the same time enhance the security of the watermark within the image manifold.

TABLE 1: PSNR Between Original and Recovered watermark

S.N.	K	PSNR between Original and Recovered Watermark (For Lenna Image)
1.	0.7	31.37
2	0.6	31.21
3	0.5	30.43
4	0.4	30.07
5	0.3	25.23
6	0.2	17.10
7	0.1	12.19

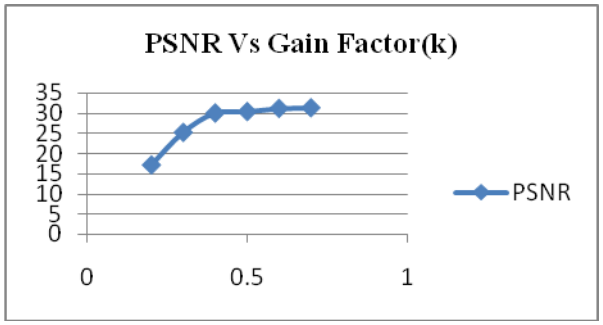

Figure 11: Comparison between Original and Recovered Watermark

TABLE 2: PSNR between Original and Watermarked Image

S.N.	K	PSNR between Original and Watermarked Image (For Lenna Image)
1	0.7	61.9601
2	0.6	62.6296
3	0.5	63.3807
4	0.4	64.3904
5	0.3	65.6377
6	0.2	70.4111
7	0.1	71.5981

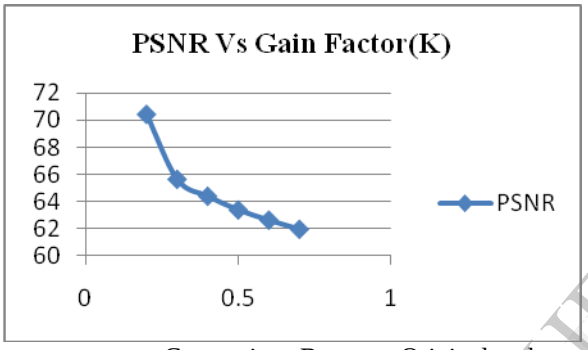

Figure 12: Comparison Between Original and Watermarked Image

TABLE 3: PSNR comparison for Different size of Image

S.N.	Image Size	PSNR Between Original and Watermarked Image	PSNR Between Original and Recovered Watermark
	For k=.5 and for Lenna Image		
1	512x512	33.4612	70.1185
2	256x256	30.43	63.3807
3	128x128	29.3892	46.8412
4	64x64	24.6156	40.3276

TABLE 4:Execution Time Comparison

S.N.	Image Size	Execution Time (In second)
1	512x512	92
2	256x256	69
3	128x128	61
4	64x64	52

References:

[1] Arvind Kumar Parthasarathy and Subhash Kak "An Improved Method of Content Based Image Watermarking "IEEE Transaction on broadcasting, Vol. 53, No. 2, June 2007, PP 468-479.

[2] Ibrahim Nasir, Ying Weng, Jianmin Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain"

[3] Deepa Kundur and Dimitrios Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition"

[4] Peter Meerwald, "Digital image watermarking in thewavelet Transform domain "P.Hd thesiss

[5] Chirawat Temi, Somsak Choomchuay, and Attasit Lasaku "A Robust Image Watermarking Using Multiresolution Analysis "Wavelet- Proceedings of ISCIT2005

[6] Xiang-Gen Xia, Charles G. Boncelet and Gonzalo "Wavelet Transform based watermark for digital Images", R. Arce : OPTICS EXPRESS, 7 December 1998 / Vol. 3, No. 12, PP 497-511

[7] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, "A Dual Digital-Image Watermarking Technique", Transaction on Engineering, computing and technology, Vol 5, April 2005 ISSN 1305-5313

[8] Rafael C. Gonzalez, R.E.Woods, Steven:, "Digital image processing using MATLAB:"

[9] Vallabha V Hampiholi, " Multiresolution Watermark Based on Wavelet Transform for Digital images"

[10] www.amara.com/current/wavelet.html " An introduction about Wavelets- Amara Graps "

[11] Mortazavi, M. Bourbakis, N.G. "A Generic floorplanning methodology," in proceedings of IEEE Conference on 20-22 Sept. 1994, pp. 749-763.

[12] N.Bourbakis, "A Language for Sequential Access of Two Dimensional Array Elements," IEEE Workshop on LFA, Singapore, 1986, pp 52-58.

[13] N-Bourbakis, C.Alexopoulos, "A Fractal Based Image Processing Language– Formal Modeling," Pattern Recognition Journal, vol 32, no 2, 1999, pp 317-338.

[14] M. Kuttera and F. A. P. Petitcolas, " A fair benchmark for image watermarking systems"

[15] D. Taskovski, S. Bogdanova, M. Bogdanov, "Digital watermarking in wavelet domain"

[16] S.S. Maniccam, N.G. Bourbakis, "SCAN Based Lossless Image Compression and Encryption", in Proceedings of IEEE International Conference on 31 Oct.-3 Nov. 1999, pp. 490-499