IJCAT - International Journal of Computing and Technology, Volume 3, Issue 11, November 2016
ISSN : 2348 - 6090
www.IJCAT.org

A Robust Digital Image Watermarking Approach Based on DWT Features and LSB Embedding

[1] Dhiraj Singh Kushwah, [2] Pragyesh Kumar Agrawal

[1] Research Scholar, Atal Bihari Vajpayee Hindi University,
Bhopal, Madhya Pradesh 462003, India

[2] Professor, Institute for Excellence in Higher Education,
Bhopal, Madhya Pradesh 462003, India

Abstract - With the expansion in the digital media transfer, editing and alteration of an image has become an easy task. But this easiness and independence become a problem when an authorized proprietor loses proprietorship due to duplication of images. Keeping this issue in mind this paper focuses on the development of technique for increasing the robustness of the image against various attacks. A new approach for protecting watermark of the fragile images is presented in this paper. DWT and LSB techniques are utilized efficiently in order to satisfy the requirements. Experiments are performed on standard images under various attacks. The results of research work show that proposed technique is better than previous ones.

***Keywords* - Digital Image Watermarking, DWT, LSB, Evaluation Parameters.**

1. Introduction

As digital world is developing radically individuals are moving towards different services provide by it. Some of these services are social networking and online shopping. This development also gives rise to new problems of piracy. In other words, it can be said that the proprietary may get easily stolen. A large amount of multimedia information is transmitted over internet now-a-days. Privacy is a major challenge especially while using images. Different techniques are used for preserving the proprietary of the owner. Invisible digital watermarking is one of approaches to provide privacy to the proprietorship. This is sub-branch of the information hiding where the watermark is considered as the hidden information while original information like, photographs, digital music, or digital video is considered as the carrier. Digital image watermarking is the process of hiding some information into a digital image which may be used to verify its authenticity or identity of its proprietor in the same manner as paper bearing a watermark for visible identification. If the image is copied, the information in watermark also is carried in the copy [1].Watermarking is broadly divided into two categories, first is visible watermarking and other is invisible watermarking [2]. Watermark information seen by naked eyes is considered as visible watermarking as shown in Fig. 1.

Fig. 1 Visible watermark in image data

Fig. 2 Invisible watermark in image data

Generally invisible watermark is used by photographers, movies, etc., which contain the watermark data either in the form of text or image.

IJCAT - International Journal of Computing and Technology, Volume 3, Issue 11, November 2016
ISSN : 2348 - 6090
www.IJCAT.org

2. Related Work

A new concept is developed in [3] which is termed as content reconstruction using self-embedding. The fountain coding paradigm is adopted in this paper and an adaptive content reconstruction scheme has been designed and proposed. External watermark is not embedded in [4] in the image. As per the algorithm proposed in this paper original image is such that it creates its own watermark bits for the image. This paper concentrates on the image expansion where spatial domain is used for embedding and supporting data is stored in the image which is essential during extraction. Robustness of image against scaling and compression attacks are also covered. In [5] watermark is hidden in the edge portion of the image. This paper adopts DAM and BCV techniques. The entire work is performed for the binary image only as the DAM is based on the binary image. Hence, the image has to be in binary format in this method and watermark information is also required to be in binary format. With this limitation it is found that the robustness of the algorithm is quite good against different attacks of noise. The extension of paper [5] is reported in [6] where hiding is done at the edge by using same DAM and BCV techniques. Here edge selection region is increased by searching surrounding region of the evaluating pixel. It is reported in the result that with this new approach robustness will increase and therefore the watermark data may be increased within the original image. Fifth order MSB is used in [7] for information collection. Here two different approaches are applied, first is constant fidelity and other is flexible rotation. A new approach of pyramidal decomposition of image blocks is used. At last reconstruction of image is made from different scattered binary matrices. Reconstruction of the image is done in [8] by inverse half toning with dithered binary version. Watermark acts as noise with the modification in image after embedding, so restoration of image is not possible. DCT technique is used in [9] where scattered image blocks are implemented with random Gaussian matrix. Here separate reference information is used for single block, so the whole bit stream is scattered on image. Coefficient within each group is recovered in the reverse process of content reconstruction. In [10] watermark is embedded into the LL band of carrier image after applying DWT and pixels are selected by applying hash function. Embedded image with some supporting information is supplied at the extraction end for creating the original image and watermark bits. This recovery of original watermark is done through the reversible watermarking scheme. In [11] information spreading is done by the LT code method on image. Here image fragmentation quality reduces the image reconstruction techniques. Spatial technique is applied in [12] for embedding the watermark into carrier image. An image is taken in RGB format where the Blue matrix of the image is chosen for embedding the watermark information. It is observed that image quality is not affected by the embedding of watermark. This work is defensive for compression attack as it affects the MSBs while LSBs remain unaffected during the attack. An algorithm is developed in [13] using the PCA and DWT techniques. In this algorithm watermark image is embedded in the video frame. Each video frame is decomposed into sub images using 2 levels. DWT and PCA transform is applied to each block in the two bands LL and HH. Experimental results show that there is no visible difference between watermark frame and original video frame. This technique is more robust against a wide range of attacks such as salt & pepper noise, gaussion noise, median filtering, rotation, cropping, etc.

3. Methodology

This paper focuses on invisible digital image watermarking technique. Two steps are involved in this technique; embedding and extraction. In case of embedding, the watermark is hidden in the original data in a way that the visibility of the watermark is not possible by naked eyes. In case of extraction, the watermark should be successfully retrieved from the received data without any loss of information from of the original data.

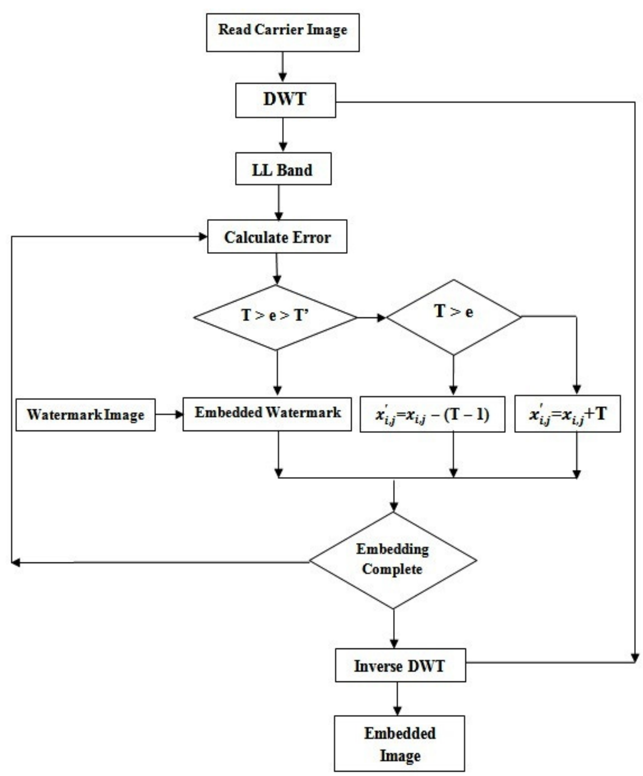

Fig. 3 Invisible watermark in image data

3.1 Pre-Processing

An image is a rectangular array of dots called pixels. Each pixel is treated as single value which is a kind of cell in a matrix. For a grayscale image, the pixel value is a single number that represents the brightness of the pixel. For the grayscale format it is in the range of 0-255. Reading an image means making a matrix of the same dimension as that of the image and then filling the matrix corresponding to the pixel value of the image at the cell in the matrix.

3.2 DWT (Discrete Wavelet Transform)

Apply DWT on pre-processed image. The effect of compression attack is very less as the images are modified in the low frequency region. The chances of watermark recovery are decreased if the direct change is done at this level. Quality of image is also degraded as at high frequency region human can detect it easily. Here whole image is divided into four parts named as LL, LH, HL and HH bands where the LL band is a low frequency band.

3.3 Calculation of Error

Here a block is read from the image which is of *{8, 12,16…..}* size and then the central pixel of that block is subsequently selected. It is replaced with the new value which is the average of all surrounding pixel values:

$$\tilde{x}_{i,j} = \frac{x_{i-1,j} + x_{i+1,j} + x_{i,j-1} + x_{i,j+1}}{4} \quad (1)$$

After that, local predictor $v_{i,j}$ is computed by solving $y_{i,j}=X_{i,j}v_{i,j}$. Here $X_{i,j}$ and $y_{i,j}$ are the averages of the selected row and column of the block.

The Error is calculated by the following formula and this error will decide that whether that pixel should be selected for the embedding of the watermark or not:

$$\hat{x}_{i,j} = v_0 + \sum_{p=1}^{k} v_p x_{i,j}^{p} \quad (2)$$

Here v_0 is a constant.
The prediction error is computed by the following expression:

$$e_{i,j} = x_{i,j} - \hat{x}_{i,j} \quad (3)$$

3.4 Embedding

Now the next step is to read each pixel from the block and then finding the mid value of the pixel. The estimated error value is calculated and then compared with the threshold.

If T'> e >T // Here T and T' are threshold values

$$x'_{i,j} = x_{i,j} + e_{i,j} + b \quad (4)$$

//Where b is the watermark bit
End if

If this error is less than the threshold, then the watermark is embedded in the image and the pixel value gets changed. For embedding the watermark bit in the pixel, the LSB of the pixel value is replaced with the watermark bit. Here a single watermark bit is embedded in the pixel value.

If e >= T

$$x'_{i,j} = x_{i,j} + T \quad (5)$$

Else if e<= T'

$$x'_{i,j} = x_{i,j} - (T - 1) \quad (6)$$

End if

If the error is greater than the threshold or less than the negative value of the threshold, then only changes are found in the pixel value without any watermark insertion. This is done just for the detection of the carrier image. This step is repeated for each pixel for the whole LL band and finally stopped for the last block.

3.5 Inverse DWT

As the entire work is done on the LL band or the actual part of the DWT image, so to obtain a complete image it is required that rest of the region is again merged into it. This process is done by inverse DWT. Finally inverse the discrete wavelet transform function to regenerate the whole image which is termed as embedded image.

Input: Original Image OI, watermark Image WI, T
Output: Embedded Image EI

1. LL←DWT(OI)
2. Loop i =1:n
3. Loop j =1:m
4. Extract the $B \times B$ block centered on $x_{i,j}$
   // Here B={8, 12,16…..}
5. Replace the central pixel in the block with
   $$\tilde{x}_{i,j} = \frac{x_{i-1,j} + x_{i+1,j} + x_{i,j-1} + x_{i,j+1}}{4}$$
6. Compute the local predictor $v_{i,j}$ by solving $y_{i,j}=X_{i,j}v_{i,j}$
   // Here $X_{i,j}$ and $y_{i,j}$ are the average of the selected row and column of the block.
   $$\hat{x}_{i,j} = v_0 + \sum_{p=1}^{k} v_p x_{i,j}^{p}$$
7. Compute the prediction error

$$e_{i,j} = x_{i,j} - \hat{x}_{i,j}$$

8. If $e_{i,j} < T$ *// Here T is a threshold*

   $$x'_{i,j} = x_{i,j} + e_{i,j} + b$$

   //Where b is the watermark bit

9. Else // Here watermark is not embedded

   If $e_{i,j} >= T$

   $$x'_{i,j} = x_{i,j} + T$$

10. Else if $e_{i,j} <= -T$

    $$x'_{i,j} = x_{i,j} - (T - 1)$$

11. End if
12. End Loop
13. End Loop
14. EI←IDWT(LL,OI)

3.6 Extraction

This step takes embedded image and key as inputs. The result of this step will be the carrier image. Now the next step is to read each pixel from the block and then find the mid value of the pixel. Further, the estimated error value is calculated which is then compared with the threshold.

If $T' > e > T$ *// Here T and T' are threshold values*

$$x = \frac{x'_{i,j} + \hat{x}_{i,j} - b}{2} \quad (7)$$

//Where b is the watermark bit
End if

If the error is less than the threshold, then embed the watermark in the image and pixel value get change.

If $e_{i,j} >= T$

$X_{i,j} = X'_{i,j} - T$ (8)

Else if $e_{i,j} <= T'$

$X_{i,j} = X'_{i,j} + (T-1)$ (9)

End if

If the error is greater than the threshold or error is less than the negative value of the threshold, then only there will be a change in the pixel value without any watermark insertion. This is done just for the detection of the carrier image. Now repeat this step again for each pixel for the whole LL band and then stop for the last block.

Finally inverse the discrete wavelet transform function, to regenerate the whole image which is termed as carrier image.

Input: Embedded Image EI, watermark Image WI, T
Output: Original Image OI

1. LL←DWT(EI)
2. Loop i =n:1
3. Loop j =m:1
4. Extract the $B \times B$ block centered on $x_{i,j}$

   // Here B={8, 12,16…..}

5. Replace the central pixel in the block with

   $$\tilde{x}_{i,j} = \frac{x_{i-1,j} + x_{i+1,j} + x_{i,j-1} + x_{i,j+1}}{4}$$

6. $\mathbf{y}_{i,j} = \mathbf{X}_{i,j} * \mathbf{v}_{i,j}$

   // Here $\mathbf{X}_{i,j}$ and $\mathbf{y}_{i,j}$ are the average of the selected row and column of the block.

   $$\hat{x}_{i,j} = v_0 + \sum_{p=1}^{k} v_p x_{i,j}^{p}$$

7. Compute the prediction error

   $$e'_{i,j} = x'_{i,j} - \hat{x}_{i,j}$$

8. if $-2T <= e'_{i,j} < 2T+1$ *// Here T is a threshold*

   $$x = \frac{x'_{i,j} + \hat{x}_{i,j} - b}{2}$$

   //Where b is the watermark bit

9. Else // Here watermark is not embedded

   If $e_{i,j} >= T$

   $X_{i,j} = X'_{i,j} - T$

10. Else if $e_{i,j} <= -T$

    $X_{i,j} = X'_{i,j} + (T-1)$

11. End if
12. End Loop
13. End Loop
14. OI←IDWT(LL,EI)

4. Experiment and Results

This section presents the experimental evaluation of the proposed Embedding and Extraction techniques. All algorithms and utility measures were implemented using the MATLAB tool. The tests were performed on 2.27 GHz Intel Core i3 machine, equipped with 4 GB of RAM running under Windows 7 Professional operating system.

IJCAT - International Journal of Computing and Technology, Volume 3, Issue 11, November 2016
ISSN : 2348 - 6090
www.IJCAT.org

Dataset: Experiments were performed on the standard images such as mandrila, lena and pirate, etc. Results were compared in two conditions; first is without attack and another is at compression attack.

Original Image Data Set

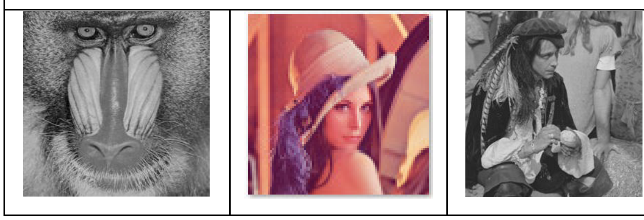

Fig. 4 Image Data Set

4.1 Evaluation Parameter

Peak Signal to Noise Ratio: PSNR is used to find the amount of data present from the received signal because it might corrupt by the presence of some noise. Therefore, it is termed as the peak signal to noise ratio. PSNR is the ratio between the maximum possible received information and the noise that affects the fidelity of its representation.

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right) \quad (10)$$

Extraction Rate: This is the reverse of the Bit Error Rate where value is obtained by the ratio of the correct bits received after extraction to the total number of bits embedded at the sender. The extraction rate η is defined as follows:

$$\eta = \frac{n_c}{n_a} \times 100 \quad (11)$$

Where n_c is the number of correctly extracted bits, and n_a is the total number of embedded bits.

4.2 Results

Table 1: Results from proposed algorithm after no attack

PSNR Values of Images Under No Attack		
Image	**Previous Work**	**Proposed Algorithm**
Mandrila	19.3955	20.4742
Lena	10.0904	19.8031
Pirate	16.5093	28.3737
SNR Values of Image Under No Attack		
Image	**Previous Work**	**Proposed Algorithm**
Mandrila	62.9725	63.0512
Lena	52.5548	62.2676
Pirate	58.1921	70.0565
Extraction Rate Values of Image Under No Attack		
Image	**Previous Work**	**Proposed Algorithm**
Mandrila	100	100
Lena	100	100
Pirate	100	100

Table 2: Results from proposed algorithm after noise attack

PSNR Values of Images Under Noise Attack		
Images	***Previous Work***	***Proposed Algorithm***
Mandrila	-42.5177	-42.5176
Lena	-42.4057	-42.4056
Pirate	-41.6194	-41.6194
SNR Values of Images Under Noise Attack		
Images	***Previous Work***	***Proposed Algorithm***
Mandrila	0.0594	0.0594
Lena	0.0588	0.0589
Pirate	0.0634	0.0634
Extraction Rate Values of Images Under Noise Attack		
Images	***Previous Work***	***Proposed Algorithm***
Mandrila	37.5	75
Lena	25	75
Pirate	12.5	50

Table 3: Results from proposed algorithm after filter attack

PSNR Values of Image Under Filter Attack		
Images	***Previous Work***	***Proposed Algorithm***
Mandrila	*-24.2675*	*-24.2675*
Lena	*-22.7333*	*-22.7329*
Pirate	*-21.5439*	*-21.5437*
SNR Values of Image Under Filter Attack		
Images	***Previous Work***	***Proposed Algorithm***
Mandrila	*18.3095*	*18.3095*
Lena	*19.7311*	*19.7315*
Pirate	*20.1389*	*20.1391*
Extraction Rate Values of Image Under Filter Attack		
Images	***Previous Work***	***Proposed Algorithm***
Mandrila	*62.5000*	*37.5000*
Lena	*25*	*62.5000*
Pirate	*37.5000*	*50*

From table 1, 2 and 3 it is seen that proposed method performs better than previous work reported in [10] named as Local Prediction Difference Expansion (LPDE). It is obtained that use of DWT function for randomization has increased the robustness of the image against different attacks.

5. Conclusion

This research paper is based on the watermarking by utilizing DWT and LSB techniques. It is obtained that DWT has improved image by embedding information in LL part, while LSB makes minor changes in the image as compared to MSB and hence, LSB is more fruitful for embedding. Experiments were performed on standard images and comparison is done on evaluation parameters. It is obtained that proposed work is best for all the parameters in presence of different attacks such as filter and noise. Under ideal conditions, extraction rate is 100 percent on all the images. In future other different transform techniques can be utilized for improving watermarking techniques such as DCT, DFT. One can adopt other features of image for increasing robustness of embedded image like edge, color, corner etc.

References

[1] S. S. Katariya, "Digital Watermarking: Review," International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, No. 2, pp. 143-153, Feb. 2012.

[2] D. S. Kushwah and P. K. Agrawal, "A Survey on Features Combination for Image Watermarking," International Journal of Modern Trends in Engineering and Research, Vol. 02, No. 01, pp. 534-540, Jan. 2015.

[3] P. Korus and A. Dziech, "Efficient Method for Content Reconstruction with Self-Embedding," IEEE Transactions on Image Processing, Vol. 22, No. 3, pp. 1134-1147, Mar. 2013.

[4] A. Piper and R. Safavi-Naini, "Scalable Fragile Watermarking for Image Authentication," In IET Information Security, Vol. 7, No. 4, pp. 300–311, 2013.

[5] K. Yamato, M. Hasegawa, Y. Tanaka and S. Kato, "Digital Image Watermarking Method Using Between-Class Variance," In IEEE International Conference on Image Processing, pp.2185-2188, Sep. 2012.

[6] A. Rajpoot , R. Batham and N. Chourasia, "Spatial Domain base Image Watermarking by Edge Features," International Journal of Current Engineering and Technology, Vol.4, No.5, pp. 3596-3601, Oct. 2014.

[7] X. Zhang, S. Wang, Z. Qian and G. Feng, "Reference Sharing Mechanism for Watermark Self-embedding," In IEEE Trans. Image Processing, Vol. 20, No. 2, pp. 485–495, Feb. 2011.

[8] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "A Secure and Improved Self-embedding Algorithm to Combat Digital Document Forgery," Signal Processing, Vol. 89, pp. 2324–2332, Dec. 2009.

[9] X. Zhang, Z. Qian, Y. Ren, and G. Feng, "Watermarking with Flexible Self-recovery Quality Based on Compressive Sensing and Compositive Reconstruction," IEEE Transactions on Information Forensics and Security, Vol. 6, No. 4, pp. 1223–1232, Dec. 2011.

[10] I. C. Dragoi and D. Coltuc, "Local-Prediction-Based Difference Expansion Reversible Watermarking," In IEEE Transactions on Image Processing, Vol. 23, No. 4, pp. 1779-1790, Apr. 2014.

[11] M. Luby, "LT codes," In Proc. of the 43rd Symposium on Foundations of Computer Science, Washington, DC, pp. 271–280, Nov. 2002.

[12] L. M. Vargas and E. Vera, "An Implementation of Reversible Watermarking for Still Images," In IEEE Latin America Transactions, Vol. 11, No. 1, pp. 54-59, Feb. 2013.

[13] M. A. Chimanna and S.R. Khot, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery," International Journal of Engineering Research and Applications, Vol. 3, No. 2, pp. 839-844, Mar. - Apr. 2013.

Author Profile:

Dhiraj Singh Kushwah has received MCA degree from RGPV, Bhopal in 2006 and M.Phil. degree from Aisect University, Bhopal, in 2014. Presently He is a Ph.D. research scholar at Atal Bihari Vajpayi Hindi University, Bhopal M.P., India. He has published 03 research papers in International Journal. His areas of interest are digital image processing and image watermarking.

Pragyesh Kumar Agrawal, Ph.D. is a gold medalist in M.Sc. Physics and is presently working as the Professor of Physics at the Institute for Excellence in Higher Education (IEHE), Bhopal, M.P., India. He has a teaching experience of over twenty-three years. He has published more than 50 research papers and edited several books. He is at present the Chief Editor of a Journal Yuyuts published by IEHE.