

ROBUST IMAGE WATERMARKING USING CRYPTOGRAPHIC ALGORITHM

Pankaj Gautam, Mahendra Kumar Pandey and Chetan Pathak

Dept. of Electronics and Communication Engineering, Rustamji Institute of Technology (RJIT), Tekanpur.

Abstract – In this paper, robust image watermarking technique using cryptographic algorithm has been proposed. By using Discrete Wavelet Transform (DWT) with SVD, a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using variable scaling factor. The insertion and extraction of the watermark is protected using cryptographic algorithm. The experimental results indicate the effectiveness of the proposed work on the basis of MATLAB simulation work. Performance is evaluated on the basis of different fidelity parameter like as peak signal to noise ratio (PSNR), normalized correlation coefficient (NCC) etc.

Index Terms— Image watermarking, DWT, singular value decomposition (SVD), cryptographic algorithm, PSNR, NCC.

1. INTRODUCTION

Due to rapid delivery of digital multimedia data over internet, demand of hiding techniques to secure digital data is required. Data hiding is a very active research areas. Digital watermarking is a branch of Data hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video [1-2]. Watermarking is the process of embedding the watermark into cover image with the help of embedding algorithm for security and other purposes. Later on, this embedded image can be extracted with the help of extraction algorithm. Generally, the image watermarking can be done in spatial domain or in transform domain [3]. Compared to spatial domain techniques frequency-domain watermarking techniques proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithms [4]. Commonly used frequency-domain transforms include the Discrete Wavelet Transform (DWT), the Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) etc. However, DWT has been used in digital image watermarking more frequently due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system.

2. METHODOLOGY

A. Discrete Wavelet transforms (DWT)

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is a multi-

resolution technique that can analyze different frequencies by different resolutions. For 2-D images, filters divide the input image into four no overlapping multi-resolution sub-bands.

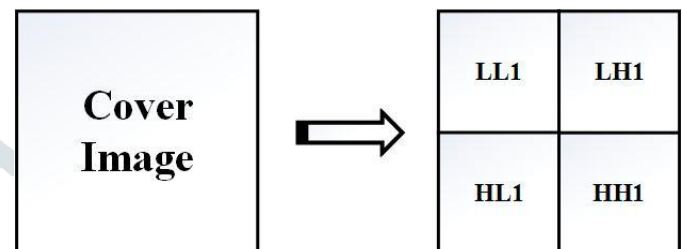


Fig. 1. Decomposition Structure “Single level DWT

Fig. 1 illustrates the DWT decomposition structure for Image, its produce the four different band of image such as LL1, HL1, LH1 and HH1 known as approximation information, horizontal detail information, vertical detail information and diagonal detail information; In wavelet analysis, maximum energy of function or image is centered at LL band means as approximation coefficient. Due to its excellent spatial-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively [5].

B. Overview of singular value decomposition (SVD)

SVD is an effective numerical analysis tool from linear algebra to decompose a rectangular matrix “A” into an orthogonal matrix U, diagonal matrix S, and the transpose of an orthogonal matrix V . SVD decomposes a given image A of size M×N as

$$A = USV^T \quad (1)$$

U and V are orthogonal matrices of size M×M and N×N, respectively. S is a diagonal matrix of size M×N having singular values .The singular vectors of an image specify the image “geometry” similarly left singular vectors represent horizontal details and right singular vectors represent the vertical details of an image, while the singular values specify the “luminance” (energy) of the image. Slight variations in the singular values do not affect the visual perception of the quality of the image [8-9].

C. Cryptographic algorithm

Here we used Arnold transform as cryptographic algorithm for the encryption of an images.

- *Arnold Transform*

The Arnold transform was introduced by Arnold. For an image C with N *N, the Arnold transform operation on the position (x, y) pixel is given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod } N \quad (2)$$

The Arnold transform, which changes the positions of the pixels, can be repeated many times in order to obtain a scrambled image. [6-7].

- *Anti-Arnold Transform*

Use of the Arnold transform periodicity on a scrambled image to recover the original image could be achieved at the expense of possibly a large computational complexity depending on how many iterations have already been used to obtain the scrambled image. The anti-Arnold transform is given by

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \text{mod } N \quad (3)$$

If a scrambled image is obtained by using n iterations of the operation of the Arnold transform, it needs the same number of iterations to recover the original image using the anti-Arnold transform.

3. PROPOSED WORK

The proposed work is divided into two parts, watermark embedding and watermark extraction.

A. Watermark Embedding

The watermark embedding process is described below:

Step.1: Load the cover image and watermark image.

Step.2: Decomposed both the image into four sub-bands using DWT for cover and encrypted watermark images respectively.

Step.3: after applying DWT, we decomposed both the image using SVD.

Step.4: Compute new singular matrix using fusion of both singular matrix.

$$S_{wm} = S_i + \alpha * S_w \quad (3)$$

where, Swm ,Si and Sw and denote the singular values of watermarked, host and water mark image, respectively.

Step.5: Using new computed singular matrix Snew, New LL band is computed with inverse SVD.

Step.6: Finally, watermarked image is obtained by merging LLnew band and remaining sub band of cover image.

B. Watermark Extraction

The watermark embedding process is described below:

Step.1: Load the cover image, watermark image and watermarked image.

Step.2: Decomposed the images into sub-bands using DWT respectively.

Step.3: after applying DWT, we decomposed images using SVD.

Step.4: The new extracted singular matrix can be calculated by:

$$S_{w_n} = (S_{wm} - S_c) / \alpha \quad (4)$$

where, Sw_n denotes new singular value.

Step.5: Using new computed singular matrix, New LL band is computed with inverse SVD.

Step.6: Finally, extracted watermark image obtained using inverse DWT based on LLnew band and reaming sub band.

4. RESULTS AND DISCUSSION

In this section, performance analysis of proposed work has been presented. The simulation work using MATLAB illustrate the efficiency and performance of proposed work on the basis of fidelity parameters.

A. Fidelity Parameters

The performance of watermarked images is determined by using peak signal-to-noise ratio (PSNR) and Normalized Correlation coefficient (NCC).

- **Peak signal-to-noise ratio (PSNR) :-**

For measurement of imperceptibility, PSNR in dB is given by:

$$MSE = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M (f_c(i, j) - f_{wm}(i, j))^2 \quad (5)$$

$$PSNR = 10 \log_{10} \frac{f_c^2(i, j)}{MSE} \quad (6)$$

where, fc2 (i, j) indicates the peak brightness value of pixel and fc, fwm represent the brightness of host and watermarked images at different pixels values.

- **Normalized Cross Co-Relation (NCC):-**

To check the robustness and image quality, the value of normalized cross co-relation (NCC) is measured by:

$$NCC = \frac{\sum_{i=1}^N \sum_{j=1}^M g_w(i, j) * g'_w(i, j)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^M g_w^2(i, j)} \sqrt{\sum_{i=1}^N \sum_{j=1}^M g_w'^2(i, j)}} \quad (7)$$

where, gw and gw' are the brightness level of original and extracted watermark at different value of pixel.

B. Simulated Results

Simulated results on MATLAB platform using proposed watermarking technique in terms of fidelity parameters have been presented by considering Lena and RJIT Logo as a host and watermark image respectively [14].

• **Sample images**



Figure 2: Lena



RJIT Logo

Fig. 2 shows the original image and Fig. 3(b) shows the watermark image for embedding of watermark in the original image

Scaling factor	Proposed work	
	MSE	PSNR
α		
0.01	4.6931	41.4502 dB
0.02	18.5150	35.4896 dB
0.03	41.2935	32.0060 dB
0.05	113.5479	29.7725 dB
0.1	433.2378	21.7975 dB
0.2	1.5661e+03	16.2167 dB
0.5	6.6703e+03	9.9233 dB
1.0	1.3523e+04	6.8539 dB

Table I: MSE, PSNR Value for different scaling factor.

Scaling factor α	Recovered NCC
0.01	0.9915
0.02	0.9934
0.03	0.9936
0.05	0.9929
0.1	0.9795
0.2	0.9195
0.5	0.7614
1.0	0.5316

Table II: NCC Value for different scaling factor.

C. Visual Presentation of simulation results

Scaling factor	Proposed work	
	Watermarked image	Recovered Watermark
α		
0.01		
0.02		
0.03		
0.05		
0.1		
0.2		
0.5		
1.0		

Fig.3 shows the visual representation of watermarked and recovered watermark image at different value of SF.

5. ATTACKS

Resistance of the watermarked image under various attacks is called robustness [10]. Robustness of presented work under various attacks has been tested and presented with NCC values in given below in fig4.












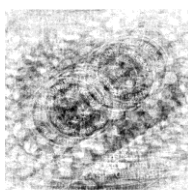
Attacks	Attacked Watermarked image	Recovered Watermark
Salt & Pepper Noise		
NCC	0.9978	
Gaussian Noise		
NCC	0.9037	
Speckle Noise		
NCC	0.9862	
Poisson Noise		
NCC	0.7370	
Resize attack 50%		
NCC	0.9930	
Median Filter [3*3]		
NCC	0.3838	

Fig.4 shows the visual representation of Attacked watermarked and recovered watermark image under various attacks.

As seen in simulated results shown in tables, it has been concluded that the value of scaling factor is varied from 0.01 to 1. As the value of scaling factor decreases, the value of PSNR increases but the same time the value of NCC decreases. The simulated experimental results also evaluated with visual representation of watermarked and extracted watermark image for human vision system (HVS). Hence it can be concluded that the proposed work provides robustness and perception transparency to the watermarked image and original image against different kind of attacks like noises, filtering and scaling.

6. CONCLUSION

In this paper, an analysis of image watermarking technique using cryptographic algorithm has been implemented. This technique can embed the watermark into salient features of the image using different scaling factor. Experiment results shows that the quality of the watermarked image and the recovered watermark are dependent only on the scaling factors. Results are clearly seen that the proposed methodology is robust against various attacks.

References

- [1] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding", IBM System Journal, Vol. 35, NOS 3&4, pp. 313-336, 1996.
- [2] P. H. W. Wong, O. C. Au and G. Y. M. Yeung, "A Novel Blind Multiple Watermarking Technique for Images", IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection and Information Hiding, Sept. 2003.
- [3] E. T. Lin and E. J. Delp "A Review of Data Hiding in Digital Images", Proc. of the Image Processing, Image Quality, Image Capture Systems Conf. (PICS' 99), pp. 274-278.1999.
- [4] L. Hu, F. Wan, "Analysis on wavelet coefficient for image watermarking", Int. Conf. MINES'10, pp. 630-634, 2010
- [5] CH.-Ch. Chang, K.-N. Chen, M.-H. Hsieh, "A robust public watermarking scheme based on dwt", 6th IHH-MSP'10, pp. 21-26, 2010.
- [6] L. Wu, J. Zhang, W. Deng and D. He, "Arnold Transformation Algorithm and Anti-Arnold

- transformation Algorithm", Proc. Information Science and Engineering Inter. Conf., Nanjing, China, Dec. 2009.
- [7] Dr. J. Abdul Jaleel, Jisha Mary Thomas , "Guarding Images Using A Symmetric Key Cryptographic Technique: Blowfish Algorithm", ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 2, August 2013.
- [8] M. Ibrahim, M. M. Rahman, and M. Iqbal, "Digital watermarking for image authentication based on combined DCT, DWT and SVD transformation", arXiv preprint arXiv:1307.6328, 2013.
- [9] Makbol, Nasrin, and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition", Digital Signal Processing 33, pp. 134-147, October, 2014.
- [10] S. Agarwal, Priyanka, and U. Pal, "Different types of attack in image watermarking including 2D, 3D images", International Journal of Scientific & Engineering Research, Vol. 6, No. 1, January, 2015.
- [11] N. Chawla and Mahendra Kumar Pandey, "Lifting scheme based non-blind hybrid image watermarking technique using low frequency band", 7th IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2017.
- [12] P. Gupta and G. Parmar, "Image watermarking using IWT-SVD and its comparative analysis with DWT-SVD", Proc. IEEE International Conference on Computer, Communications and Electronics (COMPTELIX-2017), pp. 527-531, Manipal University, Jaipur, July, 2017.
- [13] R.Tyagi and M. K. Pandey "An adaptive second level hybrid image Watermarking Technique using DWT-SVD in low frequency band" Published in IJARCCCE, Vol. 6, Issue 1, January 2017.
- [14] USC-SIPI image database
<http://sipi.usc.edu/database/database.php>