IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 6, Ver. I (Nov.- Dec. 2017), PP 07-11
www.iosrjournals.org

An Invisible, Robust and Secure DWT-SVD Based Digital Image Watermarking Technique with Improved Noise Immunity

Monika Yadav[1], Neeraj Jain[2]

Electronics & Communication Department, Modern Institute of Technology and Research Centre, India[1]yadavmonika4381.mjy@gmail.com
Electronics & Communication Department, Modern Institute of Technology and Research Centre, India
[2]njain741@yahoo.co.in

Abstract : *The chances of copyright violation and privacy have been increased due to growth of networking and technology. Digital watermark is useful to verify the integrity of the content and for authenticity of an owner. A digital watermark is a digital signal or pattern inserted into a digital document (text, graphics and multimedia presentations). Watermarking is one of the promising solutions for ownership authentication, tamper detection and protection of digital content. The watermark inserted into the image should be invisible so that it may not be forged by clever attackers; reversible so that at the receiving end there is exact recovery of the watermark and the host image. However, the exact recovery of the watermark is not possible when the image is attacked by noise, cropped, rotated, median filtered, low or high pass filtered and many more such alterations or attacks. Digital images are commonly pre-processed by JPEG before being sent through internet. Attacks cause degradation of the image and it may result in alterations in the pixel values of the image. Such alterations in the image data are harmful for detection of watermark payload and host image. Encryption is used for adding the security to the watermark image embedded to the host image. Arnold transform is used for encrypting the watermark image. The watermark is embedded into the host image in the frequency domain. DWT is used to convert the host image into the frequency domain. Singular values of the 8x8 blocks LL band coefficients are calculated. This further adds to the robustness and embedding capacity of the watermarking algorithm*

Keywords –*Discrete Wavelet Transform (DWT), Joint Photographic Expert Group (JPEG)*

Date of Submission: 30-10-2017 Date of acceptance: 16-11-2017

I. Introduction

The rapid development of internet and communication technologies is making the multimedia data to be easily copied, distributed, accessed and used illegally. For this purpose, the security of the multimedia data is most important now-a-days. So to provide the security to our digital information or multimedia data basically we use three technologies such as cryptography, steganography and digital image watermarking.

Digital watermarks can be embedded into images through the spatial domain technique or the frequency domain technique. The spatial domain generally uses simple algorithms to embed the watermark by altering the pixel values of the original image. In the frequency domain, pixel values are transformed to the coefficients. These coefficients changed to embed watermarks in the original images. Therefore, watermarks embedded by the technique of the transform domain have more robustness than watermarks which are embedded by spatial domain.

In digital image watermarking, digital watermarking techniques (DWT) are hierarchical and close to the human visual system. Besides, DWT helps watermarks to prevent from attacks. In recent times, SVD technique is combined with DWT technique as a new multiple transform domain (DWT-SVD) to improve the robustness and keeps the imperceptibility for digital watermarking. In addition, we also intend a technique to create keys based on the changed positions of the original and orthogonal matrices of the watermarks, which improves security of the watermarks for the digital watermarking.

II. Watermarking Process

The basic idea behind watermarking an image with some information is to modify the pixel values of the host image in such a way so that it seems to be modulated by that information. There must be some pre-defined set of rules to modify or adjust the pixel values in order to retrieve the watermark payload at the receiving end. It should also be assured that there is no harm to the perceptibility of the watermarked image.
Figure 1 shows the basic watermarking procedure and figure 2 shows the watermark retrieval procedure

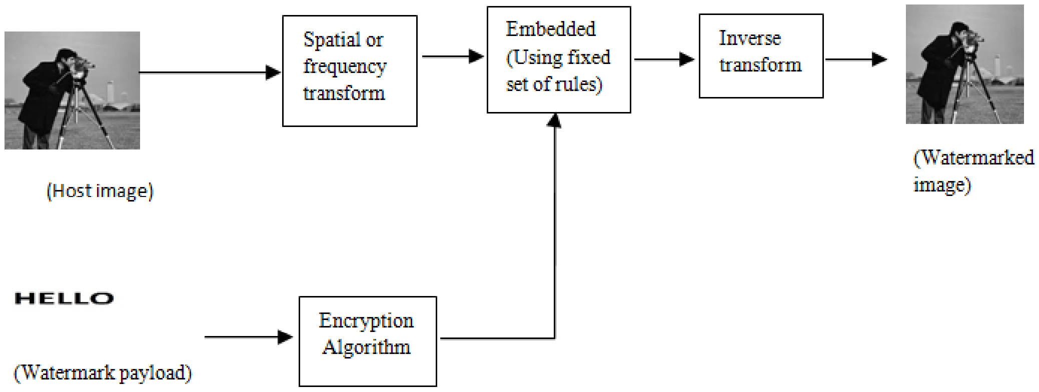

Figure 1: Basic images watermarking embedding process.

The authenticity and validity of the received watermarked image is tested. For the purpose of authentication, the payload data is encrypted using a private key of the sender. For validating the host image, normal correlation of the retrieved and the original watermark is calculated. If it is found in the tolerable limit then the host image is valid otherwise not.

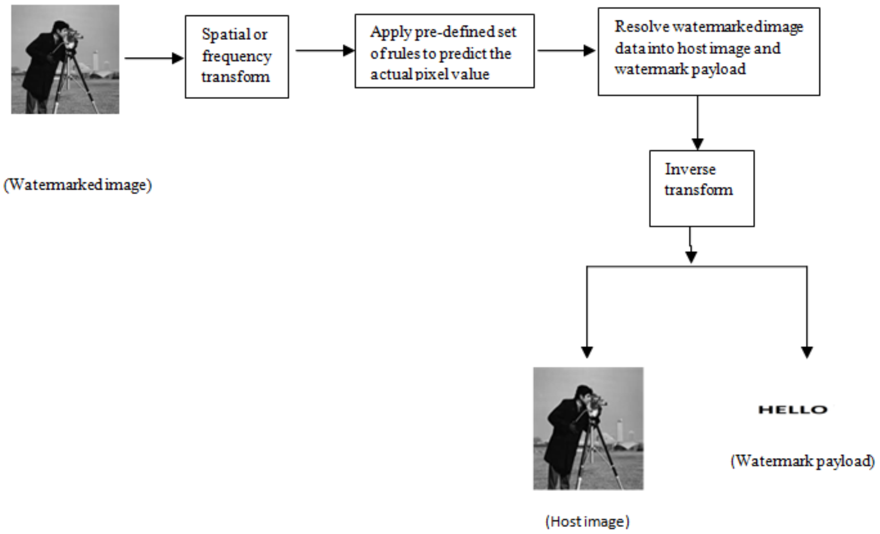
Spatial or frequency transform
Apply pre-defined set of rules to predict the actual pixel value
Resolve watermarked image data into host image and watermark payload
(Watermarked image)
Inverse transform
HELLO
(Watermark payload)
(Host image)

Figure 2: Basic image watermark retrieval process.

III. Discrete Wavelet Transform

The discrete wavelet transform is mainly similar to the Fourier transform (or mostly to the windowed Fourier transform) but they have almost different merit function. The main comparison is this: Fourier transform divide or decomposes the signal into sine and cosine, i.e. the functions defined in the Fourier space; but discrete wavelet transform takes functions that are localized or defined in both the real space and Fourier space

The discrete wavelet transform (DWT) is a classification of the wavelet transform using a discrete set of scales and the wavelet translations. In other words, this transform divide or decomposes the signal into the mutually orthogonal set of wavelets, which is the exact difference from the continuous wavelet transform (CWT), or sometimes its execution or implementation for the discrete time series is called discrete-time continuous wavelet transform (DT-CWT).

In functional analysis and numerical analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are sampled discretely. For any other wavelet transforms, it also has an advantageover Fourier transforms that is in temporal resolution; discrete wavelet transform captures both the frequencyinformation (location in time). The discrete wavelet transform has a large number of applications in engineering, mathematics, science, and computer science. Most useful, signal coding is used to show a more redundant form of discrete signal and also as a preconditioning for data compression.

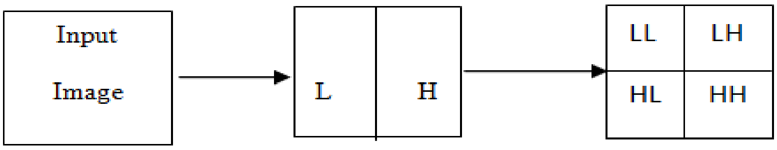

Figure 3: Block diagram of DWT first level decomposition

IV. Embedding & Retrieval

The proposed algorithm follows the method given for embedding the watermark in host image. First, we read host image and watermark payload then we will resize the images to embed the useful information in the host image. Now apply 2-dimentional discrete wavelet transform to the host image to get the specified low frequency band that have LL band. After the extraction of LL band of DWT transformed image. To apply the singular value decomposition to the LL band first we divide the LL band into 8x8 blocks then calculate the SVD of each 8x8 blocks of LL band.

Now Arnold transform used to provide the encryption to the watermark payload. Arnold transform is used to provide the robustness to the watermarked image.Every 8x8 SVD transformed LL band coefficients modified with Arnold transformed watermark payload using embedding algorithm that will explain below.

Now we get watermarked image and to check the robustness watermarked image and host image, apply the inverse SVD transform to calculate the LL band coefficients using modified singular values. To get watermark host image apply inverse DWT to the modified coefficients. Then compare the MSE and PSNR between host image and watermarked image to check the robustness of watermarked image.

Embedding Algorithm:
I: host image of size (X, Y)
LL: LL band of DWT of host image I
W: watermark image of size (K, L)
WS: pixels of watermark image in a single row array
WS_EN: encrypted watermark series (WS)
B_{ij}: N x N blocks of LL band before embedding of watermark, where N x N is the size of the block and 1<i<X/N, 1<j<Y/N
B'_{ij}: N x N blocks of LL band after embedding of watermark, where N x N is the size of the block and 1<i<X/N, 1<j<Y/N
S: singular values of SVD transformed blocks B_{ij}
Ψ: quality factor
J: watermarked image

Host image I and watermark image W is read in MATLAB environment. 2D-Discrete Wavelet Transform of host image I is calculated. Embedding of watermark is done in LL band of DWT transformed host image I. The watermark image W is converted into a single row array of pixels WS. For the purpose of adding more security, WS is encrypted to WS_EN using Arnold transform. Singular values, S, of N x N blocks B_{ij} is calculated using SVD transform. The encrypted watermark pixels WS_EN is embedded into the singular values S by modifying the value of S (1, 1). The quality factor ψ controls the depth of modification, hence controls the quality of the watermarked image. The quality factor ψ is responsible for the performance of the watermarking algorithm in terms of MSE and PSNR. Modified singular values and the singular matrices are used to reconstruct the watermarked LL band coefficients. B'_{ij} is reconstructed LL band after watermark embedding. Inverse 2D-Discrete Wavelet Transform is calculated to reconstruct the watermarked image, J

Retrieval Algorithm:
BW_{ij}: NxN blocks of LL band of noisy watermarked image, where NxN is the size of the block and 1<i<X/N, 1<j<Y/N
SW: singular values of SVD transformed blocks BW_{ij}
WR= retrieved watermark image
The watermarked image, J, is read in MATLAB. 2D-Discrete Wavelet Transform of J is calculated. The LL band of DWT transformed image is divided into blocks of NxN. Singular values, S_w, of each NxN block of LL band is calculated. Apply equation (6.1) to calculate the retrieved watermark pixels.

$$WR(i,j) = \frac{SW(i,j)-S(i,j)}{\psi}$$

The retrieved watermark pixels are decrypted using inverse Arnold Transform to get the original watermark image, WR.

V. Simulation & Results

In order to test the robustness of the proposed algorithm, two assessment metrics for the watermark logo has been used. Normalized Correlation (NC) metric is given by equation (1).

$$\text{NC} = \frac{\sum_{i=1}^{N} W*W'}{\sum_{i=1}^{N} W^2}(1)$$

Where w is the original watermark and w' is the retrieved watermark. N is the size of the watermark. For two identical images, the value of NC is equal to one. The value of NC is less than one if the two images have some amount of dissimilarity. However, the two images are said to be identical if NC is greater than or equal to 0.80. For two completely different images, NC is zero.

The amount of distortion in the host image caused by the watermarking process is given by Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). MSE is defined by equation (2). PSNR for an eight bit gray scale image is given by equation (3).

$$\text{MSE} = \frac{1}{J*K}[\sum_{x=1}^{J}\sum_{y=1}^{K}(f(x,y) - f'(x,y))^2] \qquad (2)$$

$$\text{PSNR (dB)} = 20log_{10}\frac{255}{MSE}(3)$$

Where JxK is the size of the host image, f(x, y) is the original image pixel value and $f'(x,y)$ is the watermarked image pixel value. The value of PSNR above or equal to 40 dB ensures good quality of the image.

For testing the algorithm, images of Lena, Baboon, Cameraman and Peppers are used. Figure 4 shows the host images and figure 5 shows the watermark images.

(a) Cameraman image (b) Baboon Image (c) Peppers Image (d) Lena Image

Figure 4: Host images

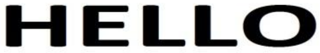

Figure 5: Watermark image

TABLE 1 MSE AND PSNR FOR THE 512x512 HOST IMAGE AND THE WATERMARKED IMAGE

Host Image	MSE	PSNR
Cameraman Image	4.8447e-004	81.2782
Peppers Image	4.8447e-004	81.2782
Lena Image	4.8447e-004	81.2782
Baboon Image	4.8447e-004	81.2782

Table 2 NC And PSNR For The Original Watermark Image And The Retrived Watermark Image

Host Image	NC	PSNR
Cameraman Image	1	54.1684
Peppers Image	1	54.1684
Lena Image	1	54.1684
Baboon Image	1	54.1684

To test the robustness of the proposed algorithm, the various attacks are considered which include Median Filtering (3x3), Gaussian noise (mean = 0, variance = 0.001), salt and pepper noise (density = 0.01) and Rotation (Anti clock wise 1 degree).

Table 3 shows the simulated results. The value of NC is greater than 0.8 for every channel attack except rotation attack. The proposed method shows the outstanding performance in retrieval of the watermark. The proposed algorithm is tested in MATLAB environment and proved its worth to be a robust and invisible watermarking algorithm.

Table3 Robustness Of Proposed Algorithm Againest Various Attack

Attack	NC	PSNR
Salt & Pepper Noise	0.80	54.0164dB
Median Filtering	0.98	52.7892dB
Gaussian Noise	0.94	51.4345dB
Rotation (1 degree)	0.5	26.2937dB

The proposed algorithm is compared and validated with the previous work done in this field. For the purpose of comparison Chinmayee et al. [16] is considered. Table 4 gives the comparison results of the proposed algorithm with Chinmayee et al. [16]. It is clear from the results that the proposed algorithm is giving comparable results for salt & pepper noise attack and improved results for rest of the attacks.

Table4 comparision Of Nc Values Of The Proposed Algorithm With The Previous Work

Attack	**Proposed algorithm**	**Chinmayee et al. [16]**	**Percentage Improvement (%)**
Median Filtering (3x3)	**0.98**	0.91	7.69%
Gaussian noise (mean = 0, variance = 0.001)	**0.94**	0.88	6.81%
salt and pepper noise (density = 0.01)	0.80	0.81	-1.25%

VI. Conclusion

The proposed method for watermarking digital images using DWT-SVD based frequency domain method is intensively studied. The algorithm is proposed to embed a reversible and invisible watermark in a gray scale image. It is also proposed to detect the watermark embedded in the host image even if the watermarked image undergoes some image processing attacks such as median filtering, rotation and channel noise. The watermark payload is a binary image. The watermark image is converted into bit stream and encrypted using Arnold Transform. Encryption increases the security in the watermarking algorithm.

The thesis work focuses on robust image watermarking the performance of the algorithm is verified against various image processing attacks which are shown in table 3. The performance of the algorithm is measured in terms of MSE, PSNR and NC, which is shown in table 1&2. The improvement in the performance of the proposed algorithm in terms of NC is verified by table 4.

References

[1]. Tri H. Nguyen, Duc M. Duong and Duc A. Duong, “Robust and high capacity watermarking for image based on DWT-SVD”, The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF), pp. 83-89, 2015.

[2]. Zhaofeng Ma, “Digital Rights Management: Model, Technology and Application”, China communications, pp. 156-168, June 2017.

[3]. RajidiSatish Chandra Reddy, Srinivas Reddy Gopu, “Enterprise Digital Rights Management for Document Protection”, 31st International Conference on Advanced Information Networking and Applications Workshops, pp. 321-327, 2017.

[4]. HishamAbdalla, Xiong Hu, AbubakerWahaballa, Ahmed Abdalla, Mohammed Ramadan, Qin Zhiguang, “Digital Rights Management - Current Status And Future Trends”, 3rd International Conference on Information Science and Control Engineering, pp. 338-343, 2016.

[5]. Md. Asikuzzaman, Md. Jahangir Alam, Andrew J. Lambert, and Mark Richard Pickering, “Imperceptible and Robust Blind Video Watermarking Using Chrominance Embedding: A Set of Approaches in the DT CWT Domain”, IEEE Transactions on Information Forensics and Security, Vol. 9, No. 9, pp. 1502-1517, 2014.

[6]. Qing Liu & Jun Ying, “Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis”, IEEE Symposium on Electrical & Electronics Engineering, pp. 618-621, 2012.

[7]. Nasrin M. Makbol& Bee EeKhoo, “ A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition”, Digital Signal Processing, Vol. 33, pp. 134-147, 2014.

[8]. Musrrat Ali & Chang WookAhn, “Comments on ‘‘Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm’’”, Experts System with Applications, Vol. 42, pp. 2392-2394, 2015.

[9]. J. Feng, I. Lin, C. Tsai, Y. Chu, “Reversible watermarking: current status and key issues”, Int. Journal, Vol. 2, No. 3, pp. 161–170, 2006.

[10]. S.P. Mohanty, E. Kougianos and N. Ranganathan, “VLSI architecture and chip for combined invisible robust and fragile watermarking”, IET Information Security, Vol. 7, No. 4, pp. 600-611, 2007.

[11]. Amit M Joshi, AnandDarji and Vivekanand Mishra, “Design and Implementation of Real-Time Image Watermarking”, proc. of ICSPCC, pp. 1-5, 2011.

[12]. M. Kamran, Sabah Suhail and MuddassarFarooq, “A Robust, Distortion Minimizing Technique for Watermarking Relational Databases Using Once-for-All Usability Constraints”, IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 12, pp. 2694-2705, 2013.

[13]. Xinshan Zhu, Jie Ding, Honghui Dong, Kongfa Hu and Xiaobin Zhang, “Normalized Correlation-Based Quantization Modulation for Robust Watermarking”, IEEE Transactions on Multimedia, Vol. 16, No. 7, pp. 1888-1904, 2014.

[14]. AfafTareef and Ahmed Al-Ani, “A highly secure oblivious sparse coding-based watermarking system for ownership verification”, Journal of Expert Systems with Applications, Vol. 42, pp. 2224-2233, 2014.

[15]. E. P. Kumar, R. E. Philip, P. S. Kumar & M. G. Sumithra, “DWT-SVD based reversible watermarking algorithm for embedding the secret data in medical images”, Proc. of 4th International Conference on Computing, Communication and Networking Technologies, pp. 1-7, 2013.

[16]. Chinmayee Das, SwetalinaPanigrahi, Vijay K. Sharma & K.K. Mahapatra, “A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation”, International Journal of Electronics and Communications, Vol. 68, pp. 244-253, 2014.

IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) is UGC approved Journal with Sl. No. 5016, Journal no. 49082.

Monika Yadav An Invisible, Robust and Secure DWT-SVD Based Digital Image Watermarking Technique with Improved Noise Immunity.” IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), vol. 12, no. 6, 2017, pp. 07-11.