International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 14 • Issue 1 pp. 22-27 Jan - June 2022 www.csjournals.com

Digital Watermarking Approach for Grayscale Lossy Image Authentication using Frequency Domain

Hiral A. Patel
Sutex Bank College of Comp. Applications & Science,VNSGU, Surat, Gujarat, India

Abstract:
The JPG image is the main source of data transmission through communication channel. The authentication of this type of Lossy formatted image is a crucial task. This paper mainly focuses on this issue. Digital Image Watermarking approach is used for authentication of lossy typed image. The watermark is generated as per the feature of image using SVD technique and with average of image block. The embedment of watermark is done using Quantization Technique and using Integer Wavelet Transformation. The watermark is extracted from the original image using De-quantization technique. The performance of simulated system is measured using PSNR which is achieved up to 33.9368dB. The proposed system is tested for JPEG Compression also. It will work satisfactory with the same. The comparison of the proposed system is also done with two other techniques and the proposed system is also give better outcomes as compare to other systems.

Keywords: Digital Watermarking, Authentication, IWT, QIM, Image Security

Introduction:
As the use of internet increases day by day, the use of digital documents like image, audio, video etc. are also increased. There is a need to develop electronic security system which protect as well as provides authenticity to the digital documents. This paper focuses on digital images only. There are two different types of formats available to store images: Lossy (.jpg) and lossless (.png, .tiff etc.). The researchers here focus on digital grayscale images with lossy format which is stored as ".jpg". The image which is stored as '.jpg', internally compressed in such a way that the image looks as similar as original image but with loss of some un-noticeable detail.

The digital watermarking is one of the techniques using which the security can be given to the images. The watermark is embedded within the original image which helps in authentication process at receiving side. Watermark is an individual file or feature extracted file [1-10]. Watermark is generated based on the feature of the original image then it is easily extracted and again generated from the watermarked image at the receiving side [1-5]. In this paper, the watermark is generated from the original image using Singular Value Decomposition method and by calculating average of individual blocks.

The generated watermark can be embedded within the original image using various methods like LSB, MSB, DFT, DCT, DWT etc [11-13]. The embedment using DWT is better than all other methods [12]. DWT divides the image into 4 sub-bands. The values of these sub-bands are in form of float values which may be rounded during further process which may create error. The Integer Wavelet Transform performs the same task but the results are in form of integer values [14]. In this paper, IWT is used to embed the watermark in place of DWT. Quantization Index Method (QIM) is highly robust against the JPEG Compression when it is applied within frequency transform [15-20]. [16] Suggested QIM method which divided the Step size into four sub intervals. If the watermark bit set to 1 then pixel value is modified as C_1 whereas with watermark bit it is modified as C_0. The imperceptibility of watermarked image is less and also the pixel value is modified either with C_0 or C_1 so more quantization error is generated. To reduce the noticeable perceptual quantization error, [15] suggested QIM technique in which fixed scaling parameter (α) is used. Researcher divides the step size into six sub-intervals. The sub-interval within which pixel value lies and corresponding to watermark bit, the pixel value is modified. Except this change QIM Watermark embedment and extraction Processes are same. The imperceptibility of watermarked image is improved as compare to [16]. Within [16] when watermark bit is 0 and pixel value lies within any sub-interval then respective modification criteria is specified properly but when watermark bit is 1 then no criteria were specified for the interval upper half interval. Now if no modification is applied to the pixel value, then during extraction Watermark becomes 0 which gives wrong output. Some criteria must be specified for this interval. The respective modifications in interval are suggested in previous published paper [14]. The same QIM technique is applied for embedment of watermark in this paper.

Proposed Watermarking System:

The proposed watermarking system is divided into sub-processes. The algorithm for each process is discussed below:

a. Watermark Generation Process

The feature of original image is extracted from image and this feature is used as watermark.

Input: Original Gray Scale Image of size 512 X 512 (IM)

Output: Watermark (WM).

1. Apply Integer Wavelet Transform and decompose the IM into LL1, LH1, HL1 and HH1 sub-bands of size 256X256.
2. Select LL1 sub-band and divide the image into 4X4 blocks (i.e. A11, A12,…). Calculate the average of each block(AVG_{4X4}).
3. Decompose each 4X4 block into 2x2 blocks (i.e. A11_1, A11_2, A11_3, A11_4). Calculate average (i.e. AVG_{2X2}) and SVD (S_1 and S_2) for each sub-blocks.
4. The watermark is calculated as per the following criteria for 2X2 block:
   If S_1>256 then wm bit=1 otherwise wm bit=0
   If $AVG_{2X2} > AVG_{4X4}$ then wm bit=1 otherwise wm bit=0
5. To represent one 2X2 block 2 bits are used so to represent one 4X4 block 8 bits are used which are demonstrated in Fig. __.

1	2	3	4	5	6	7	8
S11 bit	AVG1 bit	S12 bit	AVG2 bit	S13 bit	AVG3 bit	S14 bit	AVG4 bit

6. LL1 image is divided into 4096 blocks and 4096 X 8 = 32768 bits are used as watermark (WM).

b. Watermark Embedment Process

The embedment watermarking process is discussed below:

Input: Original Gray Scale Image of size 512 X 512 (IM)

Output: Watermarked Image (WMD).

1. Apply Integer Wavelet Transform and decompose the IM into LL1, LH1, HL1 and HH1 sub-bands of size 256X256.
2. Select LL1 sub-band and divide the image into 4X4 blocks (i.e. A11, A12,…).
3. The watermark bit is embedded using QIM embedding technique which is discussed earlier at specific position within block which is shown in Fig. ___. The embedded image is considered as i_LL1 image.

	1^{st} bit		3^{rd} bit
2^{nd} bit		4^{th} bit	
	5^{th} bit		7^{th} bit
6^{th} bit		8^{th} bit	

4. Apply inverse IWT to i_LL1, LH1, HL1 and HH1 to get watermarked image (WMD).

c. Watermark Extraction Process

The watermark extraction process is discussed below:

Input: Watermarked Image (WMD)

Output: Extracted Watermark (EWM)

1. Apply Integer Wavelet Transform and decompose the WMD into LL1, LH1, HL1 and HH1 sub-bands of size 256X256.
2. Select LL1 sub-band and divide the image into 4X4 blocks (i.e. A11, A12,…).

International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 14 • Issue 1 pp. 22-27 Jan - June 2022 www.csjournals.com

3. To extract the watermark bits from each block, apply QIM extracting technique at the positions shown in Fig. ___.
4. Watermark bits of blocks are considered as Extracted watermark (EWM).

d. Authentication Process

This watermark helps in the process of authenticating image. If the extracted watermark and extracted generated watermark bits are nearly matched then the image is considered as Authentic otherwise it is declared as unauthentic image.

Input: Watermarked Image (WMD)

Output: Extracted Generated watermark (EGWM)

1. Apply the generating watermark steps on WMD to extract the features of it.
   Consider this watermark as Extracted Generated Watermark (EGWM).
2. Compare EGWM and EWM with each other for authenticating image. If both are near to equal, the image is considered as Authentic.

Performance Evaluation:

Peak Signal Noise Ratio (PSNR) is the distortion measurement standard which is used to test the imperceptibility of watermarked image. It is defined in Eq. __. As the value of PSNR increase, the watermarked image is more similar to original image.

$$PSNR=10\times\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (\_\_)$$

Here $$MSE=\frac{1}{M\times N}\sum_{i=1}^{m}\sum_{j=1}^{n}\left[I(i,j)-r(i,j)\right]^2$$

Experimental Results:

The algorithm is simulated using MATLAB R2017a. Grayscale JPG images which are shown in Fig. 1 are used to test the efficiency of algorithm.

Fig-1 Original Image

Watermarked images are demonstrated in Fig. 2.

Fig-2 Watermarked Image

The Simulated system is also tested using Method[15] and Method[16] method. Table1 shows the PSNR results.

Table-1 PSNR Comparison

Image	PSNR [15]	PSNR [16]	PSNR Proposed
Lena	31.6223	32.8922	32.8922
Pepper	31.9482	33.486	33.6860
Sunflower	33.2687	34.3046	34.7246
Camera man	32.6908	33.7602	34.7602
Woman	31.4557	32.6205	33.6205
Average	32.1971	33.4127	**33.9367**

As per tabular outcomes, it is clear that the proposed method is more imperceptible as compare to other two suggested algorithms.

The original generated watermark is compared with the generated watermark from watermarked image for all these systems and the results are shown in form of total numbers of matched bits in Table 2.

Table-2 Bit Matching Comparison

Image	Matched Bits (out of 32768)		
	Method[15]	Method[16]	Proposed
Lena	32301	32329	32375
Pepper	32373	32377	32437
Sunflower	32351	32351	32397
Camera man	32204	32186	32255
Woman	32241	32218	32332
Average	32294	32292	32359
Matching Percentage	98.55%	98.55%	**98.75%**

As per the Table2, it is clear that the Proposed method, give improved result as compare to other two methods. Average matching in form of percentage is 98.55%, 98.55% and 98.75%. The bit matching with proposed system is high as compare to other two methods.

To test the robustness of the system, the JPEG compression attack is applied to all the systems and the outcomes are compared as compare to two other methods. Related matched bits calculations are shown in Table 3.

Table-3 After JPEG Compression attack Comparison

Image	Matched Bits (out of 32768)		
	Method[15]	Method[16]	Proposed
Lena	32272	32294	32330
Pepper	32347	32338	32395
Sunflower	32079	31982	32043
Camera man	31834	31844	31898
Woman	32236	32209	32315
Average	32154	32133	32196
Matching Percentage	98.12%	98.06%	**98.25%**

As per the results, the proposed system performs well with JPEG Compression attack also. Average matching after attack is 98.12%, 98.06% and 98.25%. The bit matching with proposed system is high as compare to other two methods.

Conclusion:

The proposed system is used for authentication of grayscale image. The watermark is generated from the original image so extra cover image is not required. The algorithm doesn't require original image at the time of extracting watermark. The imperceptibility of watermarked image is measured in form of PSNR which is 33.9368dB. The watermark is embedded within the original image using Integer Wavelet Transform and Quantization Index Method. Different QIM methods are applied to the algorithm to test the performance of the QIM methods. The average watermark bit matching within proposed system is 98.75% which is acceptable than other two QIM methods. The proposed system is also robust against JPEG Compression attack. The average watermark bit matching within proposed system is 98.25% after JPEG Compression attack which is also acceptable as compare to other two QIM Methods. The algorithm is implemented with only the grayscale images so in future; authors will try to develop the authentication system for color image.

References:

1. Li Chunlei, et al. "Semi-fragile self-recoverable watermarking scheme for face image protection." *Computers & Electrical Engineering* on Elsevier (2016).
2. Dadkhah, Sajjad, et al. "An effective SVD-based image tampering detection and self-recovery using active watermarking." *Signal Processing: Image Communication*29.10 (2014): 1197-1210.
3. Kim, Cheonshik, Dongkyoo Shin, and Ching-Nung Yang. "Self-embedding fragile watermarking scheme to restoration of a tampered image using AMBTC." *Personal and Ubiquitous Computing* 22.1 (2018): 11-22.
4. Lin, Phen Lan, Chung-Kai Hsieh, and Po-Whei Huang. "A hierarchical digital watermarking method for image tamper detection and recovery." *Pattern recognition* 38.12 (2005): 2519-2529.
5. Rhayma, Hanen, et al. "Semi fragile watermarking scheme for image recovery in wavelet domain." *2018 4th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*. IEEE, 2018.
6. Pongsomboon, Paween, Toshiaki Kondo, and Yoshiyuki Kamakura. "An image tamper detection and recovery method using multiple watermarks." *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2016 13th International Conference on*. IEEE, 2016.
7. Haghighi, Behrouz Bolourian, Amir Hossein Taherinia, and Ahad Harati. "TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique." *Journal of Visual Communication and Image Representation* (2017).
8. Bravo-Solorio, Sergio, et al. "Fast fragile watermark embedding and iterative mechanism with high self-restoration performance." *Digital Signal Processing* 73 (2018): 83-92.
9. Kiatpapan, Sawiya, and Toshiaki Kondo. "An image tamper detection and recovery method based on self-embedding dual watermarking." *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 2015 12th International Conference on*. IEEE, 2015.
10. Wang, Na, and Chung-Hwa Kim. "Tamper detection and self-recovery algorithm of color image based on robust embedding of dual visual watermarks using DWT-SVD." *Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on*. IEEE, 2009.
11. LV LINTAO, et al. "A semi-fragile watermarking scheme for image tamper localization and recovery." *Journal of Theoretical and Applied Information Technology* 42.2 (2012): 287-291.
12. Kommini Chaitanya, Kamalesh Ellanti, and E. Harshavardhan Chowdary. "Semi-Fragile Watermarking Scheme based on Feature in DWT Domain."*International Journal of Computer Applications* 28.3 (2011): 42-46.
13. Ramos, Clara Cruz, et al. "Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Domain." *Discrete Wavelet Transforms-Algorithms and Applications*. InTech, 2011.
14. Patel, Hiral A., and Dipti B. Shah. "Digital watermarking system performance using QIM techniques and wavelet transforms." *Proceedings of Second International Conference on Smart Energy and Communication: ICSEC 2020*. Springer Singapore, 2021.

15. Meerwald, P.: Quantization watermarking in the JPEG2000 coding pipeline. In: Proceedings of the IFIP TC6/TC11 International Conferenve on Communications and Multimedia Security, Darmstadt, Germany, May 2001, vol. 192, pp. 69–79 (2001)
16. Zaid, A. Ouled, et al. "Improved QIM-based watermarking integrated to JPEG2000 coding scheme." *Signal, image and video processing* 3.3 (2009): 197-207.
17. Molina-García, Javier, et al. "Watermarking algorithm for authentication and self-recovery of tampered images using DWT." *Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW), 2016 9th International Kharkiv Symposium on*. IEEE, (2016).
18. Chetan, K. R., and S. Nirmala. "Intelligent Multiple Watermarking Schemes for the Authentication and Tamper Recovery of Information in Document Image." *Advanced Computing and Communication Technologies*. Springer, Singapore, 2018. 183-193.
19. Rhayma, Hanen, et al. "Semi fragile watermarking scheme for image recovery in wavelet domain." 2018 4th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP). IEEE, 2018.
20. Rosales-Roldan, Luis, et al. "Watermarking-based image authentication with recovery capability using halftoning technique." Signal Processing: Image Communication 28.1 (2013): 69-83.