A New Curvelet Based Blind Semi-fragile Watermarking Scheme for Authentication and Tamper Detection of Digital Images

S. Nirmala and K.R. Chetan

Abstract A novel blind semi-fragile watermarking scheme for authentication and tamper detection of digital images is proposed in this paper. This watermarking scheme is based on Discrete Curvelet Transform (DCLT), which captures the information content of the image in few coefficients compared to other transforms. The novelty of the approach is that the first level coarse DCLT coefficients of the input image are quantized into 4 bits which is used as watermark and embedded into the pseudo randomly determined coefficients. At the receiver side, the extracted and generated first level coarse DCLT coefficients of the watermarked image are divided into blocks of uniform size. The difference in the energy between each block of extracted and generated coefficients is compared and if the difference exceeds threshold, the block is marked as tampered. This scheme exhibits higher Normalization Correlation Coefficient (NCC) values for various incidental attacks and is thus more robust than existing scheme [1]. The proposed scheme outperforms in localizing tampered regions compared to method [1].

Keywords Discrete curvelet transforms · Semi-fragile watermarking · Normalized correlation coefficient · Tamper detection · Incidental attacks · Intentional attacks

1 Introduction

Digital watermarking schemes protect the integrity and authenticity of the digital images. The watermarking schemes are broadly categorized as robust, fragile and semi-fragile. Robust watermarks are designed to resist attempts to remove or destroy the watermark. The fragile watermarks are designed to be easily destroyed

S. Nirmala (✉) · K.R. Chetan
Department of CSE, JNN College of Engineering, Shimoga, India
e-mail: nir_shiv_2002@yahoo.co.in

K.R. Chetan
e-mail: krc_555@yahoo.co.in

S.C. Satapathy et al. (eds.), *Information Systems Design and Intelligent Applications*, Advances in Intelligent Systems and Computing 434,
DOI 10.1007/978-81-322-2752-6_2

for the minor manipulation on the watermarked image. A semi-fragile watermark combines the properties of fragile and robust watermarks [2]. The semi-fragile watermarks are robust against most of the incidental attacks and fragile to the intentional attacks. Many efforts on semi-fragile watermarking schemes were found in literature. Chang et al. [3] proposed a semi-fragile watermarking technique to improve the tamper detection sensitivity by analyzing and observing the impact of various image manipulations on the wavelet transformed coefficients. In [4–6], semi-fragile watermarking schemes based on the Computer Generated Hologram coding techniques were described. Maeno et al. [7] presented a semi-fragile watermarking scheme for extracting content-based image features from the approximation sub-band in the wavelet domain, to generate two complementary watermarks. A blind semi-fragile watermarking scheme for medical images was discussed in [8]. Wu et al. [9] proposed a semi-fragile watermarking scheme through parameterized Integer Wavelet transform.

A new watermarking approach based on Discrete Curvelet Transforms (DCLT) [10] was developed in [1]. In this method, a logo watermark is embedded into first level DCLT coefficients using an additive embedding scheme controlled by visibility parameter. The existing method [1] has many limitations. The Normalized Correlation Coefficient (NCC) values drops after a variance of 0.05 for the noise attacks. The existing method [1] is not completely blind as the first level coarse DCLT coefficients and visibility factor needs to be communicated to the receiver. In this paper, a blind semi-fragile watermarking is proposed that addresses all the afore-mentioned limitations. The authentication is performed based on the fact that incidental attacks do not change information content and the average energy in a block substantially. The rest of the paper is organized as follows: The proposed methodology is explained in Sect. 2. Section 3 presents the experimental results and comparative analysis. Discussions are carried out in Sect. 4. The conclusions are summarized in Sect. 5.

2 Proposed Semi-fragile Watermarking Scheme

Curvelet transform has been developed to overcome the limitations of wavelet and Gabor filters [11]. To achieve a complete coverage of the spectral domain and to capture more orientation details, curvelet transform has been developed [12]. The Digital Curvelet Transform (DCLT) is usually implemented in the frequency domain for higher efficiency reasons [13]. The implementation of DCLT is performed either using wrapping or unequally spaced fast Fourier transform (USFFT) algorithms [14]. In this paper, a novel method for semi-fragile watermarking using DCLT for authentication and tamper detection of digital images is presented.

2.1 Watermark Embedding

The process of generating and embedding watermark is depicted in Fig. 1. The input image is a gray scale image and is transformed using DCLT. The watermark is generated from the first level coarse DCLT coefficients.

These coefficients are quantized into four bits and embedded into the first level coarse DCLT coefficients at the locations determined using pseudo random method [15]. Subsequently, inverse DCLT is applied to get watermarked image. Suppose the size of the input image is $N \times N$, then the number of scales used in DCLT is varied from $2 \text{ to } \log_2(N)$. The perceptual quality of the watermarked image is measured using Peak Signal to Noise Ratio (PSNR) [16]. The average PSNR values of all the images in the corpus for different dimensions of the input image at different scales used in DCLT are shown in Table 1. It is observed from the values shown in Table 1 that, if the number of scales is less than or equal to $(\log_2(N) - 3)$, there is a significant increase in PSNR values.

The coarse coefficients of first level DCLT are extracted. The coefficients are quantized into 4 bits. The number of Least Significant Bits (LSBs) to be used is a tradeoff between accuracy of tamper detection and imperceptibility of the watermarked image. The accuracy of tamper detection is evaluated using the following equation:

$$Accuracy\ of\ Tamper\ Detection = \frac{Average\ Number\ of\ bits\ identified\ as\ tampered}{Average\ Number\ of\ bits\ actually\ tampered} \tag{1}$$

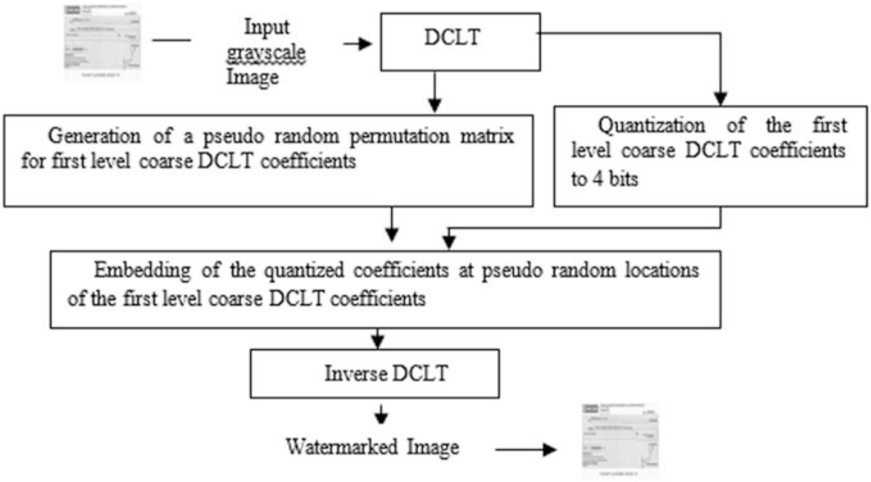
Input
grayscale
Image
DCLT
Generation of a pseudo random permutation matrix for first level coarse DCLT coefficients
Quantization of the first level coarse DCLT coefficients to 4 bits
Embedding of the quantized coefficients at pseudo random locations of the first level coarse DCLT coefficients
Inverse DCLT
Watermarked Image

Fig. 1 Semi-fragile watermark embedding process

Table 1 PSNR values of the watermarked image at different scales of DCLT

Size of the input image $N \times N$	Range of the scale (2 to $\log_2(N)$)								
	2	3	4	5	6	7	8	9	10
128 × 128	28.45	35.56	44.61	44.78	44.89	45.01			
256 × 256	28.49	35.56	44.50	52.84	52.91	52.94	53.07		
512 × 512	29.02	36.61	45.01	52.91	53.70	53.91	54.01	54.1	
1024 × 1024	29.35	35.62	44.79	52.92	53.61	53.84	54.05	54.2	54.3

Table 2 Accuracy of the tamper detection and PSNR of the watermarked image

No. of least significant bits used	Accuracy of tamper detection (%)	PSNR values (dB)
2	78.65	66.62
3	87.50	59.61
4	94.27	53.15
5	95.57	36.24
6	96.88	26.58

It can be observed from the values shown in Table 2 that the accuracy of tamper detection values is more than 90 % for the number of bits used for quantization is above 3. It can also be inferred from the computed PSNR values that imperceptibility of the image and high accuracy of tamper detection decreases in large amount after 4 bits.

Each of the first level coarse DCLT coefficient is quantized to 4 bits and embedded into a coarse coefficient, whose location is decided by a pseudo random permutation [15]. The embedding of the watermark is done according to the Eq. (2) as follows:

$$D_{l_k}(m,n) = D^q_{l_k}(i,j)\, k = 1\ldots4 \tag{2}$$

where, $D_{l_k}(m,n)$—kth LSB of the coarse first level DCLT coefficient at (m, n), $D^q_{l_k}(i,j)$—kth LSB of the quantized coarse first level DCLT coefficient at (i, j).

2.2 Watermark Extraction

The watermarked image may be subjected to incidental or intentional attacks during transmission. Checking the integrity and authenticity of the watermarked image are carried out during watermark extraction process. The process of watermark extraction is shown in Fig. 2. The watermarked image is transformed using first level DCLT.

The watermark is extracted from four LSBs of each first level DCLT coarse coefficient. It is inversely permuted and dequantized. At the receiver, tamper

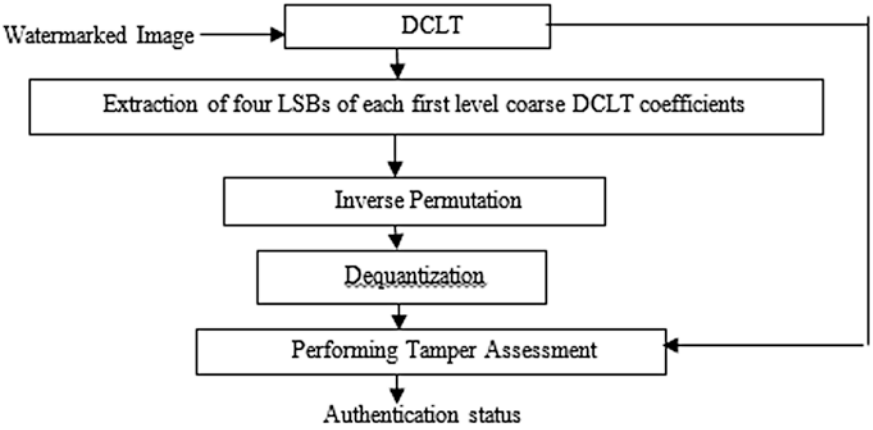
Watermarked Image
DCLT
Extraction of four LSBs of each first level coarse DCLT coefficients
Inverse Permutation
Dequantization
Performing Tamper Assessment
Authentication status

Fig. 2 Semi-fragile watermark extraction process

assessment is carried out by dividing the dequantized and generated first level coarse DCLT coefficients into blocks of uniform size. We have conducted experiments to determine the appropriate size of block for tamper assessment. The average accuracy and processing time required for tamper detection for all the images in the corpus is shown in Table 3. It can be observed from the values in Table 3 that, the tamper detection accuracy and processing time decreases with increase in the size of the block. We have arrived to the decision that the size of the block is set to 3 × 3 which is enough to achieve better (94 %) tamper assessment with reasonable processing time.

The energy of the dequantized and first level coarse DCLT coefficients are computed using the Eqs. (3) and (4) as follows:

$$E_1 = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} |D(i,j)| \tag{3}$$

$$E_2 = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} |D_e(i,j)| \tag{4}$$

Table 3 Accuracy of tamper detection and processing time for varying size of the blocks

Block size	Tamper detection accuracy (%)	Processing time (s)
2 × 2	96.35	5.1892
3 × 3	94.27	3.1121
4 × 4	83.85	2.1602
5 × 5	75.26	1.5123
6 × 6	60.16	1.0992

where, $N = 3$, size of each block, E_1—energy of each block of the first level DCLT coarse coefficients of the watermarked image, E_2—corresponding energy from the watermarked image, $D(i, j)$—generated first level DCLT coarse coefficient at (i, j) from the watermarked image, and $D_e(i, j)$—extracted first level DCLT coarse coefficient at location (i, j) from the watermarked image. The tamper assessment is performed using the Eqs. (5) and (6) as below:

$$T = \frac{|E_1 - E_2|}{\mathrm{MAX}_E} \tag{5}$$

$$a(i) = \begin{cases} \text{tampered}, & T > 0.4 \\ \text{``not tampered''}, & \textit{otherwise} \end{cases} \tag{6}$$

where, MAX_E—Maximum energy possible in first level coarse DCLT coefficient and T- tamper value and $a(i)$—Authentication status of each block i.

3 Experimental Results

We have created a corpus of different types of images for testing the proposed semi-fragile watermarking system. The corpus consist of various categories of images like Cheque, ID cards, Bills, Certificates, Marks cards and few images taken from the standard image database USC-SIPI [17]. The existing method [1] and the proposed method has been tested for tamper detection of all the images in the corpus. The results of tamper detection for the two sample cases which involves tampering of text and image respectively is shown in Fig. 3. It is evident from the

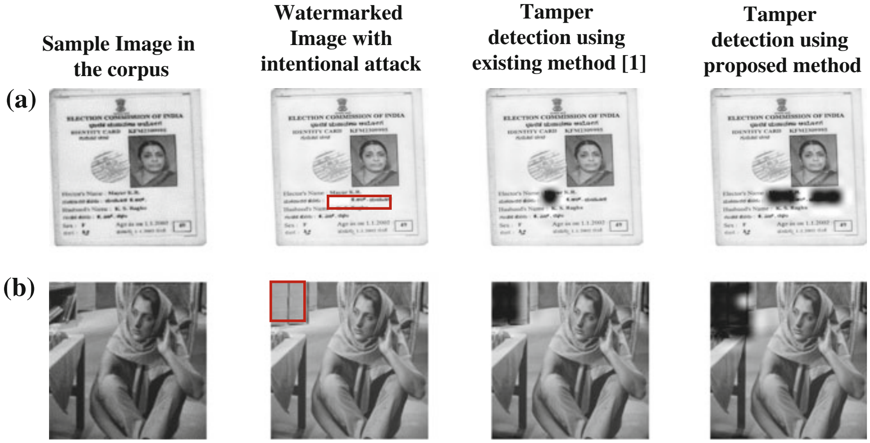
Sample Image in the corpus
Watermarked Image with intentional attack
Tamper detection using existing method [1]
Tamper detection using proposed method
(a)
(b)

Fig. 3 Results of tamper detection. **a** Text tampering. **b** Image tampering

visual inspection of results shown in Fig. 3 that the detection of tampered locations is more accurate in the case of proposed method.

4 Discussions

A comparative analysis of fragility and robustness of the existing [1] and proposed method are performed and are discussed in detail in the following subsections.

4.1 Robustness Analysis

The robustness is evaluated using the parameter Normalization Correlation Coefficient (NCC) [15] between the extracted and received first level DCLT coarse coefficients. The NCC values are computed for both existing method [1] and proposed method by varying the variance parameter of the noise. The graph is plotted for NCC values for each type of noise and is shown in Fig. 4. It is evident from Fig. 4 that the NCC values drop substantially for the existing method [1] for variance greater than 5. The watermarked image is also subjected to JPEG compression by varying the amount of compression. A plot depicting the robustness performance of the existing [1] and proposed schemes in terms of NCC values is shown in Fig. 5. It is observed from Fig. 5 that for quality factors from 15 to 5 %, NCC values are better for proposed scheme than the existing scheme [1].

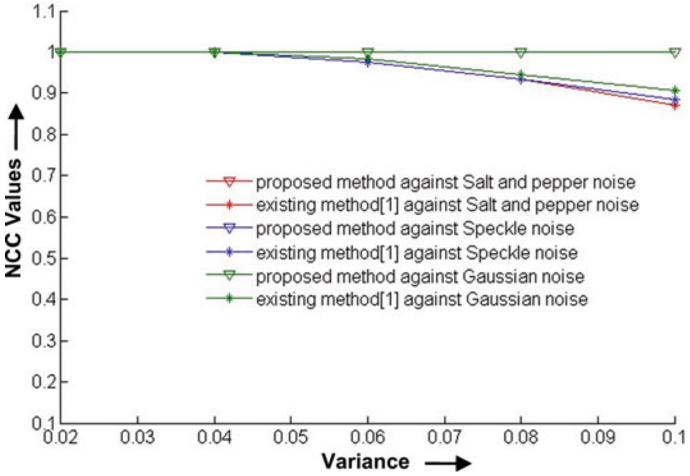

Fig. 4 Robustness under noise attacks

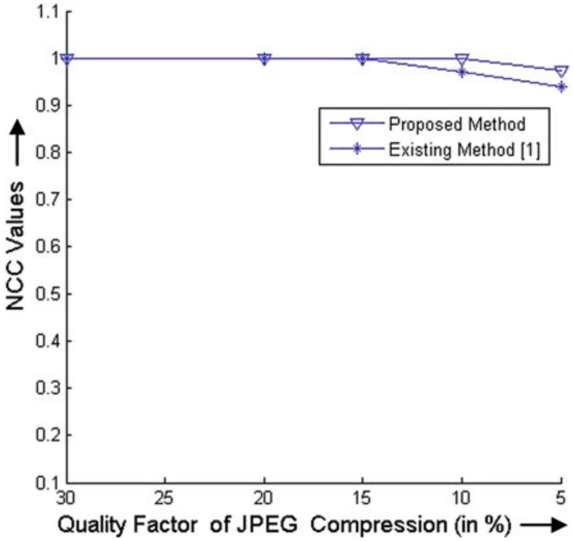

Fig. 5 Robustness against JPEG compression

4.2 *Fragility Analysis*

The fragility is decided based on the tamper assessment capabilities of a semi-fragile watermarking scheme. We have tested all the images in the corpus for different types of tampering namely (i) inserting a new content (ii) deleting the existing content (iii) modifying an existing content and (iv) performing multiple attacks in the same image.

The performance of detection of tampered regions for both existing method [1] and proposed method is measured in terms of parameter accuracy of tamper detection using Eq. (3). The tamper detection values in Table 4 reveals that, the proposed method results in better accuracy than the existing method [1]. The average accuracy of tamper detection is around 94 % and at least 10 % more than existing method [1]. However, there is a failure of around 6 % in accurate detection and localization of tamper.

Table 4 Analysis of tamper detection against various intentional attacks

Attack	Accuracy of tamper detection	
	Existing method [1] (%)	Proposed method (%)
Insertion	82.69	93.27
Deletion	79.17	92.19
Modification	80.99	94.37
Multiple attacks	77.88	91.35

5 Discussions

A blind semi-fragile watermarking scheme based on DCLT has been proposed in this paper. From the results, it is inferred that this method exhibits higher NCC values and thus, more robust than the existing method [1]. The proposed approach leads to significant improvement in detection of tampered regions in the watermarked image compared to the existing method [1]. The proposed work can be further enhanced by using more sophisticated measures for evaluating tamper detection in an image. By embedding into selected curvelet coefficients, it could be possible to improve the accuracy of tamper detection and at the same time the embedding process could be made inexpensive. The selection of curvelet coefficients is considered as future work of the current study.

References

1. Ghofrani, S. et.al., Image content authentication and tamper localization based on semi fragile watermarking by using the Curvelet transform, TENCON 2012—2012 IEEE Region 10 Conference, Cebu, pp. 1–6, (2012).
2. Prabhishek Singh et.al., A Survey of Digital Watermarking Techniques, Applications and Attacks, International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, No. 9, pp. 165–175 (2013).
3. W.H. Chang and L.W. Chang, Semi-Fragile Watermarking for Image Authentication, Localization, and Recovery Using Tchebichef Moments, International Symposium on Communications and Information Technologies (ISCIT), pp. 749–754. (2010).
4. G. Schirripa, C. Simonetti and L. Cozzella, Fragile Digital Watermarking by Synthetic Holograms, Proc. of European Symposium on Optics/Fotonics in security & Defence, London, UK, pp. 173–182. (2004).
5. J. Dittmann, L. Croce Ferri and C. Vielhauer, Hologram Watermarks for Document Authentications, Proceedings of IEEE International Conference on Information Technology, Las Vegas, pp. 60–64 (2001).
6. Y. Aoki, Watermarking Technique Using Computer-Generated Holograms, Electronics and Communications in Japan, Part 3, Vol. 84, No. 1, pp. 21–31. (2001).
7. K. Maeno, Q. Sun, S. Chang and M. Suto, New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization, IEEE Trans. Multimedia, Vol. 8, No. 1, pp. 32–45. (2006).
8. L. Xin and L. Xiaoqi and W. Wing, A semi-fragile digital watermarking algorithm based on integer Wavelet matrix norm quantization for medical images, IEEE International conference on bioinformatics and biomedical engineering, pp. 776–779, (2008).
9. X. Wu and J. Huang and J. Hu and Y. Shi, Secure semi-fragile watermarking for Image authentication based on parameterized integer Wavelet, Journal of Computers, Vol. 17, No. 2, pp. 27–36, (2006).
10. D. L. Donoho and M. R. Duncan, Digital Curvelet transform: Strategy, implementation and experiments, Proc. Society optics and photonics, Vol. 4056, pp. 12–29, (2000).
11. L. Chen, G. Lu, and D. S. Zhang, Effects of Different Gabor Filter Parameters on Image Retrieval by Texture, in Proc. of IEEE 10th International Conference on Multi-Media Modelling, Australia, pp. 273–278. (2004).
12. E. J. Candès, L. Demanet, D. L. Donoho, and L. Ying, Fast Discrete Curvelet Transforms, Multiscale Modeling and Simulation, Vol. 5, pp. 861–899 (2005).

13. J.-L. Starck and M.J. Fadili, Numerical Issues When using Wavelets, in Encyclopedia of Complexity and Systems Science, Meyers, Robert (Ed.), Springer New York, Vol 14, pp 6352–6368, (2009).
14. E. Candes and D. Donoho, New tight frames of Curvelets and optimal representations of objects with C2 singularities Comm. Pure Appl. Mathematics, Vol. 57, No. 2, pp. 219–266, (2004).
15. Jaejin Lee, Chee Sun Won, A Watermarking Sequence Using Parities of Error Control Coding For Image Authentication And Correction, Consumer Electronics, IEEE Transactions, Vol. 46, No. 2, pp. 313–317 (2000).
16. Yevgeniy Dodis et.al., Threshold and proactive pseudo-random permutations, TCC'06 Proceedings of the Third conference on Theory of Cryptography, Verlag Berlin, Heidelberg, pp. 542–560, (2006).
17. http://sipi.usc.edu/database/.