A Novel Intelligent Multiple Watermarking Schemes for the Protection of the Information Content of a Document Image

K.R. Chetan(✉) and S. Nirmala

Department of CSE, JNN College of Engineering, Shimoga, Karnataka, India
chetankr@jnnce.ac.in, nir_shiv_2002@yahoo.co.in

Abstract. Most of the past document image watermarking schemes focus on providing same level of integrity and copyright protection for information present in the source document image. However, in a document image the information contents possess various levels of sensitivity. Each level of sensitivity needs different type of protection and this demands multiple watermarking techniques. In this paper, a novel intelligent multiple watermarking techniques are proposed. The sensitivity of the information content of a block is based on the homogeneity and relative energy contribution parameters. Appropriate watermarking scheme is applied based on sensitivity classification of the block. Experiments are conducted exhaustively on documents. Experimental results reveal the accurate identification of the sensitivity of information content in the block. The results reveal that multiple watermarking schemes has reduced the amount of data to be embedded and consequently improved perceptual quality of the watermarked image.

Keywords: Multiple watermarking · Intelligent watermarking · Fragile watermarking · Robust watermarking · Integer wavelets · Contourlets · Gradient binarized blocks · GLCM

1 Introduction

Document images are used as proof for authentication and business transactions. Traditionally digital watermarking has been used as a primary technique for copyright protection and integrity management of document images [1–3]. The document image consists of information with various levels of sensitivity. For instance, in a cheque image, the signature and amount are dynamically changing information for each cheque and thus possess highest level of sensitivity. The bank name, logo, cheque number contain regeneratable information content and hence constitute lower level of sensitivity. There also exists many empty areas in a cheque which can be classified as insensitive areas. Each sensitivity level needs different type of protection. Therefore, there is a need to use multiple watermarking techniques on the different areas of the same document image. The multiple watermarking schemes have two fold objectives: improve the perceptual quality of the watermarked image by reducing embedding capacity; perform tamper detection and recovery with better accuracy.

S. Mukherjee et al. (Eds.): ICVGIP 2016, LNCS 10481, pp. 3–14, 2017.
https://doi.org/10.1007/978-3-319-68124-5_1

This paper is organized as follows: Sect. 2 provides a literature review of the existing works in intelligent and multiple watermarking schemes. The proposed model is explored in Sect. 3. Section 4 presents experimental results of the proposed multiple watermarking scheme. Conclusions of the proposed work are summarized in the last section.

2 Literature Review

Digital watermarking is classified as robust, fragile and semi-fragile based on the robustness to incidental and intentional attacks [4]. A detailed survey of the works on robust, fragile and semi-fragile watermarking techniques can be found in [5–10]. Most of the past efforts on watermarking schemes apply single type of watermarking technique on the entire document image. Houmansadr et al. [11] proposed a watermarking technique based on the entropy masking feature of the Human Visual System (HVS). Kankanhalli and Ramakrishnan [12] developed a watermarking technique by embedding just noticeable watermarks. Radharani et al. [13] designed a content based watermarking scheme in which watermark is generated using Independent Component Analysis (ICA) for each block of the input image. In [14–16], few works on the segmentation of the image into objects using image statistics and subsequently applying the robust watermarking schemes for each objects are described. Shieh et al. [17] proposed the use of genetic algorithm (GA) [18] to compute the optimal frequency bands for watermark embedding into a Discrete Cosine Transform (DCT) based watermarking system, which can simultaneously improve security, robustness, and image quality of the watermarked image. A novel idea was put forward in [19] to embed multiple watermarks with different compression domains into the same source. Lu et al. [19] developed an algorithm for embedding multiple watermarks into the Vector Quantization (VQ) domain, as well as for hiding the secret keys associated with the watermarks in the transform domain to enhance the robustness of the watermarked image. Sheppard et al. [20] discussed the different ways of multiple watermarking like rewatermarking, segmented watermarking and composite watermarking [20]. They explored different attack scenarios [21, 22] and level of robustness that could be provided by each category of multiple watermarking.

The literature reviews on the content based multiple watermarking techniques reveals that most of the existing works lack intelligent classification of information content of a document image based on sensitivity to the attacks. In the existing techniques, authors attempted to apply multiple watermarks of the same type to each block of the document image and it is not based on the appropriateness of the watermarking for the information content present in the block. In addition, the existing schemes also incur tradeoff between robustness and fragility of the watermarking multiple times. These issues motivate towards an intelligent classification of the different areas of a document image and application of different types of watermark schemes appropriate to the sensitivity requirement of each area of the document image. In this paper, a new model for intelligent multiple watermarking is designed that automatically computes desired type of watermarking for each block of the document image.

3 Proposed Model

The proposed model for the novel intelligent multiple watermarking system consists of two processes namely Embedding and Extraction. The Embedding process divides the input document image into blocks and intelligently determines the type of watermarking to be applied for each block. The watermarking algorithm depends on the information content of the image. This is primarily available through the energy component and hence luminance component in transformation is used. Further image is converted back to color after watermarking to produce watermarked image. The embedding technique depends on the type of watermarking. Robust watermarking is implemented using integer wavelet embedding [23] and fragile watermarking is accomplished using contourlet based embedding [24]. Extraction process is carried on the blocks of the watermarked image. The result of the watermark extraction depends on the type of the watermarking. The outcome of the robust watermark extraction on the block of the watermarked image is content authentication of the block. The outcome of fragile watermark extraction on the block of the watermarked image results in tamper detection and recovery of information content in the block. The following subsection explores the embedding process and extraction process in detail.

3.1 Multiple Watermark Embedding

The multiple watermark embedding process is shown in Fig. 1. It is an intelligent and adaptive embedding scheme which depends on the information content of the

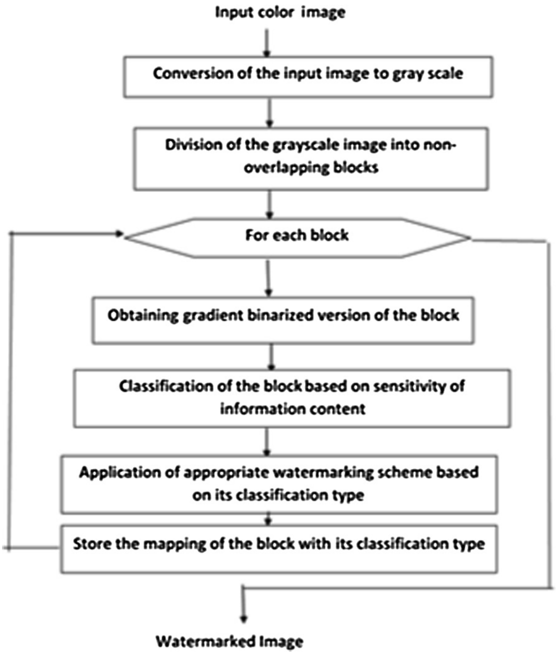
Input color image
Conversion of the input image to gray scale
Division of the grayscale image into non-overlapping blocks
For each block
Obtaining gradient binarized version of the block
Classification of the block based on sensitivity of information content
Application of appropriate watermarking scheme based on its classification type
Store the mapping of the block with its classification type
Watermarked Image

Fig. 1. Multiple watermark embedding process

document image. Experiments have been conducted on all document images corpus to analyze the effect of size of the block on accuracy in identification of the type of the block and processing time. For each block, gradient binarized version of the information content in the block is obtained. Further, the sensitivity level of each block and type of watermarking required is found automatically. Subsequently, appropriate watermark embedding algorithm is applied for each block.

The gradient binarized version of the information content in the block is computed using the following algorithm:

```
Algorithm : Gradient_Binarized_Block(B)
Input: An image block B of size 128X128 with pixel values containing gray levels (0-255)
Output: Gradient Binarized block of B
  1. for every pixel $p$ at location $(i, j)$ in the block,
  2.        do find its gradient value

                $g_p(i,j) = \sum_{x=-1}^{1} \sum_{y=-1}^{1} p(x+i, y+j)$        (1)

  3.        compute maximum gradient value in the block

                $g_{max} = max_{i=1}^{128X128} \left( g_p(i,j) \right)$        (2)

  4.        Set gradient threshold $g_{thresh}$ to $(g_{max})/2$
  5.        Convert all the pixel values from gray levels to binary using $g_{thresh}$. The
            values of the pixels having gray levels above $g_{thresh}$ is set to 1 and values of
            the rest of the pixels is set to 0.
  6.        Let $n1$ denote the total number of pixels having value 1 and $n0$ denote
            total number of pixels with value 0.
  7.        Compute new gradient threshold as

                $g_{thresh1} = round(n1 * w1 + n0 * w2)$        (3)

  8.        if $g_{thresh1} = g_{thresh}$
               then return
            else
               $g_{thresh} = g_{thresh1}$
  9.      return gradient_binarized_block of $B$
```

In this algorithm, the values of the weights $w1$ and $w2$ is empirically set to 0.5. The number of iterations required for termination of this algorithm depends on the distribution of the information content in the block. The outcome of this algorithm is a binary version of the block that gives segmentation of foreground and background information contents in the block.

```
Algorithm: Classification_of_sensitivity_level(B)
Input: Gradient_binarized_block B
Output: Sensitivity_level of B
  1. Computation of the energy distribution of the block using median of the pixel values in gradient binarized block B
       $ED_b = median(g_b)$   (4)
  2. Computation of the relative energy distribution $RED_b$ of binarized block b using:
       $RED_b = \frac{ED_b}{max_{n=1}^{nb}(ED\ )}$   (5)
     where, $nb$ denotes the total number of blocks in the source document image.
  3. Computing gray level cooccurence matrix (GLCM) of gradient binarized block b and designate it as $GLCM_b$
  4. Compute value of homogeneity parameter $HM_b$
  5. Compute sensitivity levels of block as follows:
       $sensitivity\_levels = \begin{cases} 0, & HM_b < 0.5 \text{ and } RED_b > 0.7 \\ 1, & 0.5 \leq HM_b < 0.85 \text{ and } RED_b \geq 0.3 \\ 2, & otherwise \end{cases}$   (6)
  6. return sensitivity_level
```

Experiments have been conducted on the document image corpus to decide on the appropriate range to relative energy distribution and homogeneity values for determining the sensitivity levels of the blocks. The average RED_b and HM_b values for different types of information content in these document images is calculated and values are recorded in Table 1. It can be observed from the values in Table 1 that RED values for blocks of document image containing dynamically changing information content are in the range 0.7–0.85 and HM values lie between 0.29–0.50. Thus, sensitivity level of the block with HM less than 0.5 and RED above 0.7 is set to 0. Similarly, it can see in Table 1 that blocks of the document image containing preprinted information content has RED values above 0.3 and HM values in between 0.5 to 0.85. Therefore, sensitivity level of these blocks is set to 1. For all the other blocks, sensitivity level is set to 2.

The type of watermarking used depends on the sensitivity levels of the information content in the block. Highly sensitive blocks are protected using fragile watermarking technique. In this paper an effective fragile watermarking technique based on contourlets [24] is used. Partially sensitive blocks are protected using robust watermarking technique [23]. The size of the block is decided based on two factors: effectiveness in the identification of the sensitivity of the block and processing time for identification.

Table 1. Computation of *RED* and *HM* values for different classes of document images in the corpus

Document image class	Preprinted information		Dynamically changing information	
	RED	HM	RED	HM
Cheques	0.33	0.67	0.72	0.50
Bills	0.36	0.82	0.79	0.35
Identity cards	0.62	0.85	0.76	0.39
Marks cards	0.30	0.79	0.85	0.29
Certificates	0.54	0.51	0.70	0.36

Experiments have been conducted exhaustively on all the document images to measure the impact of size of the block against accuracy in identifying sensitivity level of the block. The average number of blocks expected for each sensitivity level and number of blocks being accurately identified is recorded in Table 2. It can be observed from average accuracy in identification values that the blocks of lesser size exhibits higher accuracy.

Table 2. Impact of size of the blocks of a document image on accuracy in identification of its sensitivity level and processing time for identification

Block size	Type-0		Type-1		Type-2		IA (in %)	Processing time (in secs)
	EB	IB	EB	IB	EB	IB		
32 × 32	348	339	210	204	466	466	98.53	102.12
64 × 364	83	75	57	52	116	116	94.92	78.7
128 × 3128	22	20	17	15	25	25	93.75	32.11
256 × 3256	5	4	4	3	7	7	87.50	21.16

Where, EB-Expected no. of blocks evaluated manually by an expert, IB-Identified No. of blocks from the proposed approach, IA-Identification Accuracy of a block, which is calculated as the ratio of sum of IB of all block types over sum of EB of all the block types. Considering the values of the accuracy in identification of sensitivity level of a block and processing time incurred for identification, size of the block is set to 128 × 128.

3.2 Multiple Watermark Extraction

Multiple watermark extraction process has two fold objectives based on the of watermark extraction process involved. Robust watermark extraction aims at content authentication of the block. This is implemented using robust watermarking scheme [23]. Fragile watermark extraction involves tamper detection and recovery of the information content of a document image. The fragile watermark extraction is performed using contourlets [24]. Multiple watermark extraction has similar steps as in multiple watermark embedding process discussed in Sect. 3.1 until the identification of the type of the gradient binarized block. Subsequently, the type of the block extracted and generated is compared and if there is a mismatch, the corresponding block of the document image is declared "inauthentic". However, if there is a match, then watermark extraction is carried out based on the type of the block. The extracted and generated watermarks are compared for similarity using Feature Similarity Index [24] and based on the comparison, the tamper detection of the block is decided. If the block is tampered, recovery of information content is made by extracting watermark embedded at robust locations [24]. During robust watermark extraction, the watermark is extracted from the LL-band of the integer wavelet transformation performed on the block of a document image. The extracted watermark is decoded using binary block coding technique [23]. The decoded watermark is compared with original watermark and decision of content authentication of the block is performed [23].

4 Results

We have created a corpus of document images. All the images in the corpus are scanned document images. The classes of document image corpus considered are Cheques, Bills, Identity Cards, Marks cards and Certificates. Each class of document image consists of 30 images. The results of the identification of type of the blocks of a sample document image in the corpus are shown in Fig. 2.

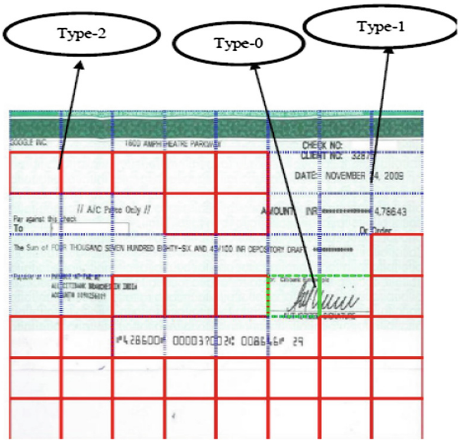

Fig. 2. Results of identification of the type of the block of a sample Cheque image

It can be observed in Fig. 2, that there are three types of blocks in the sample Cheque image. The blocks with dashed border are Type-0 blocks. They are highly sensitive blocks containing large variations in the information content and distribution of the information. The blocks with dotted border are Type-1 blocks i.e. partially sensitive blocks which contain preprinted information. They have moderate homogeneity in distribution of the information content. Remaining type of blocks in the document image are the insensitive blocks (Type-2) which contain less energy and higher homogeneity of information. We have tested the accuracy of the identification for all the classes of document images in the corpus.

Once the blocks are identified, appropriate type of watermarking has been applied based on the type of the block to obtain watermarked image. Subsequently multiple watermark extraction has been applied on the watermarked image and incidental and intentional attacks have been applied on the watermarked image. The results of multiple watermark embedding and extraction are shown in Fig. 3. Figure 3 shows that watermarked image is perceptually similar to source document image in the corpus. An example of incidental attack on partially sensitive block and intentional attack on a highly sensitive block of the watermarked image is demonstrated in Fig. 3. Further, one could also observe there is great degree of accuracy in tamper detection and recovery of the highly sensitive block.

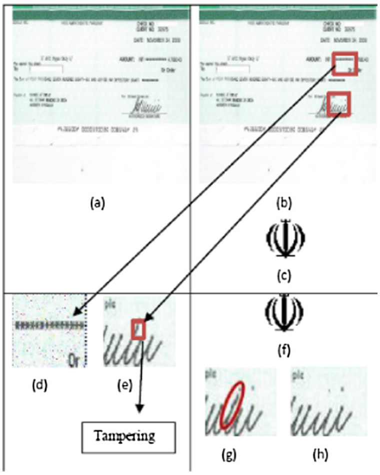

Fig. 3. Results of proposed multiple watermarking system (a) source document image (b) watermarked image (c) original watermark for robust watermarking (d) zoomed up Partially sensitive block with salt and pepper noise attack (e) zoomed up Highly sensitive tampered block (f) extracted robust watermark (g) tamper detection results (h) tamper recovery result

5 Analysis

The performance of the proposed watermarking system is measured in terms of the following parameters: (i) Performance analysis using Peak Signal to Noise Ratio (PSNR) (ii) Robustness Analysis using Normalized Correlation Coefficient (NCC) (iii) Fragility Analysis using accuracy of Tamper detection and recovery.

5.1 Performance Analysis

The performance of the proposed multiple watermarking scheme is evaluated in terms of PSNR. The perceptual quality of the watermarked image of size *NXN* is measured using Peak Signal to Noise Ratio (PSNR) [25]. A graph of PSNR values is depicted in Fig. 4 for different classes of the document images. The graph shown in Fig. 4 reveals that PSNR values of the multiple watermarking schemes are better than robust and fragile watermarking schemes when applied separately. This increase in PSNR and subsequently the perceptual quality of the watermarked image is due to the fact that all the blocks of the document image are not watermarked. The quantity of the watermark to be embedded depends on the type of the block. Hence, the noise induced due to watermarking is reduced to some extent and this result in the better fidelity of the watermarked image.

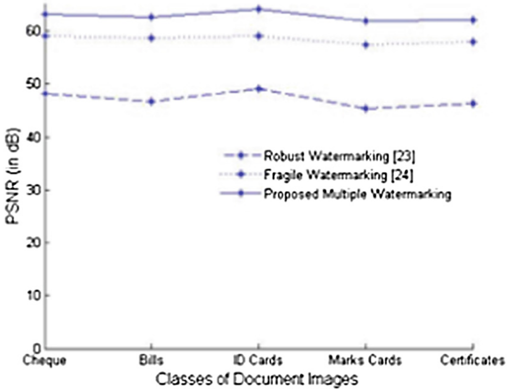

Fig. 4. Effect of watermarking schemes on PSNR values of different classes of document images in the corpus

5.2 Robustness Analysis

The robustness of the proposed multiple watermarking scheme is tested by applying various attacks such as horizontal cropping, vertical cropping, resizing, noise and JPEG compression on all the document images in the corpus. The degree of robustness obtained is evaluated in terms of NCC: [26]. The NCC values obtained by the application of proposed watermarking scheme only on partially sensitive blocks and robust watermarking scheme applied on the entire document image is recorded in Table 3. The NCC values in Table 3 show that there is a slight improvement in the robustness of the watermarked image. The increase in robustness is due to the localization of robustness to the blocks that are partially sensitive.

Table 3. Average NCC values for different incidental attacks

Incidental attack	Existing Robust watermarking scheme [23]	Proposed multiple watermarking scheme
Salt and pepper noise	0.93	0.96
Cropping	0.97	0.97
Resizing	0.94	0.95
JPEG compression	0.94	0.96

5.3 Fragility Analysis

The fragility capability of any watermarking scheme is evaluated in terms of accuracy of tamper detection and tamper recovery parameters. Accuracy of tamper detection is evaluated as follows:

$$TDA = 1 - \frac{\sum_{i=1}^{n} (ta_i \oplus td_i)}{n} \tag{7}$$

where, n – total number of bits in the fragile watermarked blocks, ta – tampered bit, td – tamper detection bit. The average values of TDA and TRA are computed for all document images in the corpus under different intentional attacks for proposed fragile watermarking scheme and contourlet based scheme [24] separately. These values are tabulated in Table 4. It can be observed that proposed multiple watermarking schemes has a slight improvement capability in detection and recovering from tampering of information content of document image.

Table 4. Average TDA and TRA values for different intentional attacks

Intentional attacks	Existing Fragile water marking scheme [24]		Proposed multiple watermarking scheme	
	TDA	TRA	TDA	TRA
Insertion	0.9	0.87	0.91	0.90
Deletion	0.92	0.91	0.92	0.92
Modification	0.87	0.87	0.90	0.89

6 Conclusions

A novel intelligent multiple watermarking schemes are proposed in this paper. The blocks of a document image have been automatically classified into various sensitivity levels with greater accuracy. The performance analysis of the proposed approach reveals improvement in the perceptual quality of the watermarked image. The proposed scheme also outperforms the existing methods [23, 24] in providing robustness, tamper detection and recovery capabilities. Improvement on the accuracy of identification of type of block is taken up as future work of the current study.

References

1. Wu, M., Liu, B.: Watermarking for image authentication. In: Proceedings of the IEEE International Conference on Image Processing, pp. 437–441 (1998)
2. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking And Steganography. Morgan Kaufmann Publishers Inc., San Francisco (2007)
3. Hartung, F., Kutter, M.: Mutimedia Watermarking Techniques. Proc. IEEE **87**(7), 1079–1107 (2002)

4. Potdar, V.M., Han, S., Chang, E.: A survey of digital image watermarking techniques. In: 3rd IEEE International Conference on Industrial Informatics, pp. 709–716 (2005). doi:10.1109/Indin.2005.1560462
5. Mirza, H., Thai, H., Nakao, Z.: Color image watermarking and self-recovery based on independent component analysis. In: Rutkowski, L., Tadeusiewicz, R., Zadeh, L.A., Zurada, J.M. (eds.) ICAISC 2008. LNCS, vol. 5097, pp. 839–849. Springer, Heidelberg (2008). doi:10.1007/978-3-540-69731-2_80
6. Wang, M.S., Chen, W.C.: A majority-voting based watermarking scheme for color image tamper detection and recovery. Comput. Stand. Interfaces **29**, 561–571 (2007)
7. Bas, P., Chassery, J.M., Macq, B.: Geometrically invariant watermarking using feature points. IEEE Trans. Image Process. **11**(9), 1014–1028 (2002)
8. Qi, W., Li, X., Yang, B., Cheng, D.: Document watermarking scheme for information tracking. J. Commun. **29**(10), 183–190 (2008)
9. Dawei, Z., Guanrong, C., Wenbo, L.: A chaos-based robust wavelet-domain watermarking algorithm. Chaos, Solitons Fractals **22**(1), 47–54 (2004)
10. Schirripa, G., Simonetti, C., Cozzella, L.: Fragile digital watermarking by synthetic holograms. In: Proceedings of the European Symposium on Optics/Fotonics in Security & Defence, London, pp. 173–182 (2004)
11. Houmansadr, A., et al.: Robust content-based video watermarking exploiting motion entropy masking effect. In: Proceedings of the International Conference on Signal Processing and Multimedia Applications, pp. 252–259 (2006)
12. Kankanhalli, M.S., Ramakrishnan, K.R.: Adaptive visible watermarking of images. In: IEEE International Conference on Multimedia Computing and Systems, vol. 1, pp. 568–573 (1999)
13. Radharani, S., et al.: A study on watermarking schemes for image authentication. Int. J. Comput. Appl. (0975 – 8887) **2**(4), 24–32 (2010)
14. Kay, S., Izquierdo, E.: Robust content based image watermarking. In: Proceedings of the Workshop on Image Analysis for Multimedia Interactive Services (2001)
15. Kim, M.-A., Lee, W.-H.: A content-based fragile watermarking scheme for image authentication. In: Chi, C.-H., Lam, K.-Y. (eds.) AWCC 2004. LNCS, vol. 3309, pp. 258–265. Springer, Heidelberg (2004). doi:10.1007/978-3-540-30483-8_31
16. Habib, M., Sarhan, S., Rajab, L.: A Robust-Fragile dual watermarking system in the DCT domain. In: Khosla, R., Howlett, R.J., Jain, L.C. (eds.) KES 2005. LNCS, vol. 3682, pp. 548–553. Springer, Heidelberg (2005). doi:10.1007/11552451_74
17. Shieh, C.-S., et al.: Genetic watermarking based on transform-domain techniques. J. Pattern Recogn. **37**, 555–565 (2004)
18. Goldberg, D.E.: Genetic Algorithms in Search Optimization and Machine Learning. Addison-Wesley, Reading (1992)
19. Lu, Z.-M., Xu, D.-G., Sun, S.-H.: Multipurpose image watermarking algorithm based on multistage vector quantization. IEEE Trans. Image Process. **14**(6), 822–831 (2005). doi:10.1109/Tip.2005.847324
20. Sheppard, N.P., Safavi-Naini, R., Ogunbona, P.: On multiple watermarking. In: Dittmann, J., Nahrstedt, K., Wohlmacher, D. (eds.) Multimedia and Security: New Challenges Workshop, p. 38871 (2001)
21. Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J.J., Su, J.K.: Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. IEEE Commun. Mag. **39**(8), 118–126 (2001)
22. Wang, S., Zhang, X.: Watermarking scheme capable of resisting sensitivity attack. IEEE Signal Process. Lett. **14**(2), 125–128 (2007)

23. Chetan, K.R., Nirmala, S.: An efficient and secure robust watermarking scheme for document images using integer wavelets and block coding of binary watermarks. J. Inf. Secur. Appl. **24–25**, 13–24 (2015)
24. Chetan, K.R., Nirmala, S.: A novel fragile watermarking scheme based on contourlets for effective tamper detection, localization and recovery of handwritten document images. IEEE Signal Process. Lett. (Communicated)
25. Aggarwal, E.D.: An efficient watermarking algorithm to improve payload and robustness without affecting image perceptual quality. J. Comput. **2**(4) (2010). ISSN 2151-9617
26. Zhu, X., et al.: Normalized correlation-based quantization modulation for robust watermarking. IEEE Trans. Multimed. **16**(7), 1888–1904 (2014)