Intelligent Multiple Watermarking Schemes for the Authentication and Tamper Recovery of Information in Document Image

K.R. Chetan and S. Nirmala

Abstract Existing works on document image watermarking provide same level of protection for information present in the source document image. However, in a document image the distribution of the information contents influences on the level of protection required. This necessitates application of multiple watermarking techniques on the source document image. In this paper, novel intelligent multiple watermarking techniques are proposed. The source document image is divided into blocks of the same dimension. For each block, appropriate type of watermarking is decided based on the type of block which is determined automatically using gradient binarized technique. The blocks with regeneratable information are protected using semi-fragile watermarking and blocks with non-regeneratable information are protected using fragile watermarking. Experimental results reveal the accurate identification of type of the block. The performance results reveal that multiple watermarking schemes have reduced the capacity of embedding and consequently improved perceptual quality of the watermarked image.

Keywords Multiple watermarking · Intelligent watermarking · Contourlet transforms · Curvelet transforms · Tamper detection · Tamper recovery · Document image

1 Introduction

Most of the document images are used as proof of authentication and copyright protection in the business transactions. "Digital watermarking technique has been used as a primary means for copyright protection and integrity management of

K.R. Chetan (✉) · S. Nirmala
Computer Science Department, Jawaharlal Nehru National College of Engineering, Shivamogga 577201, Karnataka, India
e-mail: chetankr@jnnce.ac.in

S. Nirmala
e-mail: nir_shiv_2002@yahoo.co.in

R.K. Choudhary et al. (eds.), *Advanced Computing and Communication Technologies*, Advances in Intelligent Systems and Computing 562, https://doi.org/10.1007/978-981-10-4603-2_18

document images [1–3].” The document image consists of information content which can be divided into regeneratable or non-regeneratable blocks. The regeneratable blocks contain minimal changing information content. The blocks having dynamically changing information content are categorized as “non-regeneratable” blocks. Further, there are many empty regions classified as “non-content blocks”. Each type of block requires different types of protection. Therefore, there is a need to use multiple watermarking techniques on the different areas of the same document image.

The rest of the paper is organized as follows. Section 2 provides literature review of the existing works. The proposed model is explored in Sect. 3. Experimental results of the proposed scheme are presented in Sect. 4. The performance analysis of the novel technique work is made in Sect. 5. Conclusions of the proposed work are summarized in Sect. 6.

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]. Houmansadr et al. [11] proposed a watermarking technique based on the entropy masking feature of the Human Visual System (HVS). Kankanhalli et al. [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 of the objects are described. Shieh et al. [17] used genetics [18] to compute the optimal frequency bands for watermark embedding. Lu et al. [19] developed an algorithm for embedding multiple watermarks into the Vector Quantization (VQ) domain. Sheppard et al. [20] discussed different ways of multiple watermarking like re-watermarking, segmented watermarking, and composite watermarking [20] using different attack scenarios [21, 22].

The literature reviews on the content-based multiple watermarking techniques reveal that most of the existing works lack intelligent application of appropriate watermarking scheme. The previous works on multiple watermarking schemes incur significant degradation in the perceptual quality of the watermarked image. The existing schemes also incur tradeoff between robustness and fragility of the

watermarking multiple times. In this paper, a novel intelligent multiple watermarking model is proposed that automatically computes desired type of watermarking for each block of the document image.

3 Proposed Model

In this work, a new multiple watermarking model is proposed. The novelty of this approach lies in identifying automatically the type of watermark required for different regions of source document image based on the information content present in that region. This in turn reduces the amount of watermarking to be done in comparison to a single watermarking technique for the entire document image. The proposed model consists of multiple watermarking embedding and extraction process. The input document image is decomposed into blocks of uniform size. To each block, either fragile or semi-fragile watermarking is applied, which is determined automatically. Semi-fragile watermarking is implemented using curvelet-based embedding [23] and fragile watermarking is accomplished using contourlet-based embedding [24]. Extraction process is carried on the blocks of the watermarked image.

3.1 Embedding of Multiple Watermarks

The embedding process of multiple watermarks is shown in Fig. 1. Experiments have been conducted exhaustively on all the document images in the corpus to measure the impact of size of the block against accuracy in identifying type of the block. The average number of blocks expected for each type of the block, the number of blocks identified correctly, and processing time are recorded in Table 1. "It can be observed from values in Table 1 that the blocks of lesser size exhibits higher accuracy and consume more time than the blocks of higher dimensions." Considering these parameters size of the block is set to 128×128. For each block, gradient binarized version of the information content in the block is computed. The type of each block is classified based on the uniformity in distribution and amount of information content present in the block.

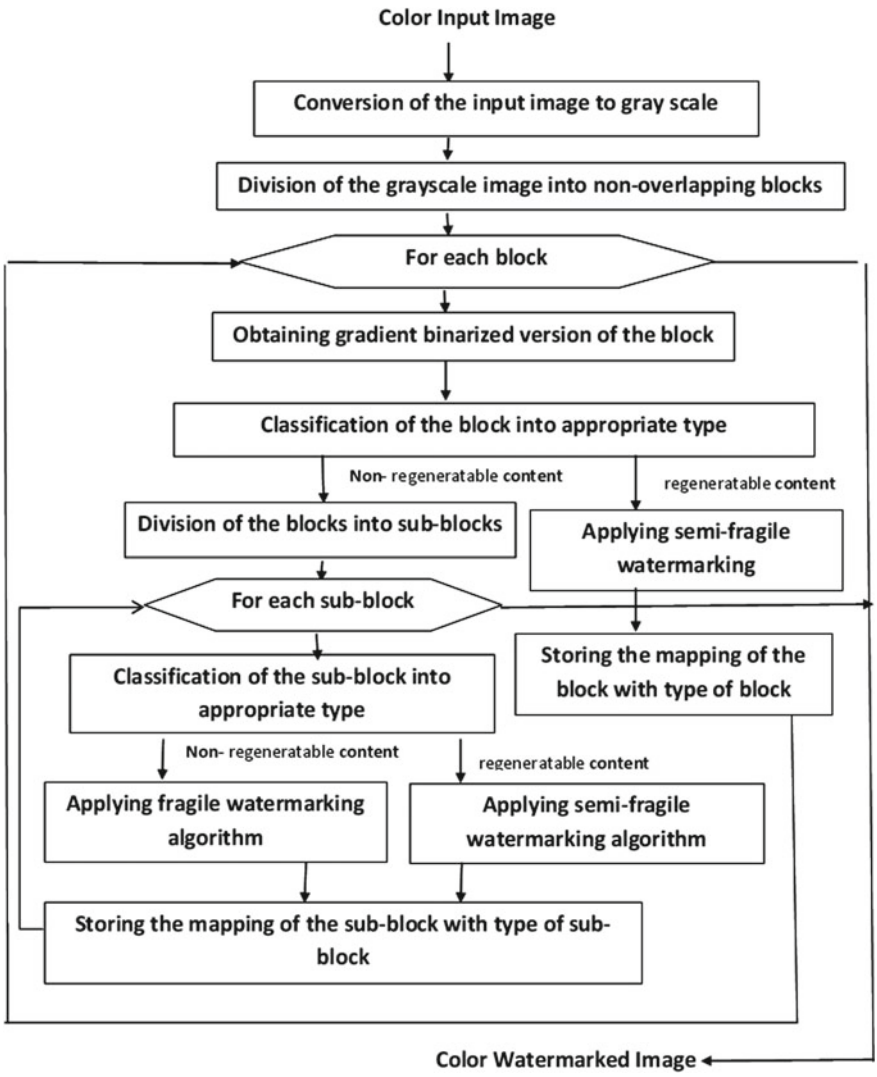

Fig. 1 Multiple watermark embedding process

Table 1 Average accuracy in identification of the block type and processing time for identification

Block size	Non-content		Uniform content		Nonuniform content		Avg IA (in %)	Processing time (in s)
	EB	IB	EB	IB	EB	IB		
32 × 32	466	466	210	204	153	150	98.97	89.12
64 × 64	116	116	57	52	33	29	96.94	41.7
128 × 128	25	25	17	15	9	8	95.75	23.11
256 × 256	7	7	4	3	2	2	89.61	18.16

where, *EB* Expected number of blocks evaluated manually by an expert, *IB* Identified number of blocks from the proposed approach, and *IA* Identification accuracy of a block

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

Algorithm to compute gradient binarized version an image:
Input: Image I of size M X N containing gray scale values (0-255)
Output: Binarized Image of I
Step 1: Decompose I into blocks of size 128 X 128
Step 2: For every pixel p at location (i,j) in the block, find its gradient value from immediate neighbours i.e.

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

Step 3: Compute maximum gradient value in the block

$$g_{max} = \max(g_p) \tag{2}$$

Step 4: Set gradient threshold g_{thresh} to $(g_{max})/2$
Step 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.
Step 6: Let $n1$- number of pixels with pixel value 1 and $n0$ - with value 0.
Step 5: Compute new gradient threshold as $g_{thresh1} = round(n1 * w1 + n0 * w2)$
Step 6: If $g_{thresh1} = g_{thresh}$, Stop
Otherwise, Set $g_{thresh} = g_{thresh1}$, Go to Step 4

IA is computed using the equation below:

$$\mathrm{IA} = \frac{\sum_{\mathrm{block\_type}} \mathrm{IB}}{\sum_{\mathrm{block\_type}} \mathrm{EB}}. \tag{3}$$

Experiments are conducted on exhaustive doc-corpus to find the appropriate values of weights w_1 and w_2. From experimental calculations, it was found setting $w_1 = 0.4$ and $w_2 = 0.6$ leads to a higher degree of accuracy in identification of the

type of the block with less amount of time. Hence, the values of weights w_1 and w_2 are set to 0.4 and 0.6, respectively. The gradient binarized block is classified into an appropriate type using the following algorithm:

Algorithm to classify gradient binarized block into various block types
Input: Gradient binarized block
Output: Type of the block
Step 1: Computation of the information content of the block by computing percentage of pixels in the block with intensity value 1

$$IC_b = \frac{\sum_{i=1}^{128X128} g_b}{128X128} \tag{4}$$

Step 2: Classifying blocks into content and non-content blocks

$$block\_type = \begin{cases} content, & IC_b > 0.1 \\ non-content, & otherwise \end{cases} \tag{5}$$

Step 3: For the blocks of type "content", the cluster density of rows and columns in the block is computed.
To find row clusters:

```
For i = 1 : rows
  For j = 1: cols
      if (g_b(i,j) = g_b(i,j+1) then
            continue
      Else
            row_clusters = row_clusters + 1
      End-if
  End-for
End-for
```

Interchanging indices i and j in the above loops will yield $column\_clusters$
Step 4: $avg\_clusters=(row\_clusters+column\_clusters)/2$
Step 5: $group\_density = {}^{avg\_clusters}/_{128\ X\ 128}$
Step 6: If $group\_density$ exceeds a threshold 0.4, blocks are sub-divided of same dimension. Steps 3-5 should be repeated for each subblock. Otherwise, type of the block is determined using Equation (6).
Step 7: For each content subblock, further classification into regenerable or non-regenerable content is performed using following equation:

$$block\_content\_type = \begin{cases} regeneratable, & group\_density \le 0.4 \\ non-\text{regeneratable}, & otherwise \end{cases} \tag{6}$$

The setting of thresholds (0.1 for information content and 0.4 for group density) is based on the experimental evaluation of the identification accuracy. These thresholds exhibit an accuracy of more than 95% in identification of the type of block. Non-regeneratable blocks are protected using fragile watermarking technique. In this paper an effective fragile watermarking technique based on contourlets [24] is used. Regeneratable blocks are protected using semi-fragile watermarking technique. In this work, semi-fragile watermarking is implemented using Discrete Curvelets Transform (DCLT) [23].

3.2 Extraction of Multiple Watermarks

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/subblock extracted and generated is compared and if there is a mismatch, the corresponding block/subblock 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. If the block contains non-regeneratable content, then fragile watermark extraction is performed using contourlets [24]. If the block contains regeneratable content, semi-fragile watermark extraction is performed using DCLT coefficients [23].

4 Results

Document images are scanned and a sophisticated corpus is built with different classes like Cheques, Bills, Identity Cards, Marks cards, and Certificates, and each class consists of 30 images. We have tested the accuracy of the identification for all the classes of document images in the corpus. The accuracy values in Table 1 suggest that average accuracy of identification of type of blocks for all classes of document images is more than 95%. Hence, proposed multiple watermarking system exhibits highly accurate identification of type of the block and thus supports for application of intelligent multiple watermarking. Figure 2 depicts that watermarked image is perceptually similar to source document image in the corpus. An example of insertion attack on a regeneratable block and modification attack on a non-regenerable block of the watermarked image is illustrated in Fig. 2. Semi-fragile watermarking extraction results reveal that there is a great degree of accuracy in tamper detection. Further, accurate tamper recovery of the nonuniform content block is also observable in Fig. 2.

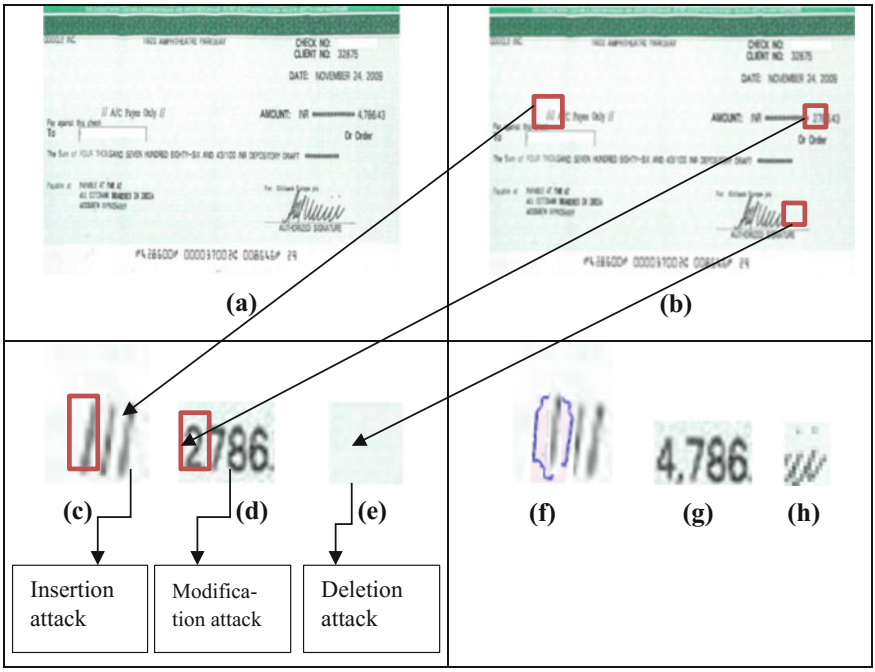

Fig. 2 Results of proposed multiple watermarking system **a** source document image, **b** watermarked image, **c** zoomed up uniform content block tampered with insertion attack, **d** zoomed up nonuniform content block containing preprinted information content with modification attack, **e** zoomed up nonuniform content block containing handwritten information content with deletion attack, **f** tamper detection results of uniform content block, **g** and **h** tamper recovery results of nonuniform content blocks

5 Analysis

The proposed watermarking system is measured for performance in terms of the following parameters: (i) Fidelity analysis using Peak Signal-to-Noise Ratio (PSNR), (ii) Accuracy of Tamper detection, and (iii) Accuracy of Tamper recovery.

5.1 Fidelity Analysis

The fidelity of the proposed multiple watermarking scheme is evaluated in terms of PSNR [25]. A plot of PSNR values is shown in Fig. 3 for different classes of the document images. The graph shown in Fig. 3 reveals that PSNR values of the multiple watermarking schemes are better than semi-fragile and fragile watermarking schemes when applied separately. The amount of watermarking performed

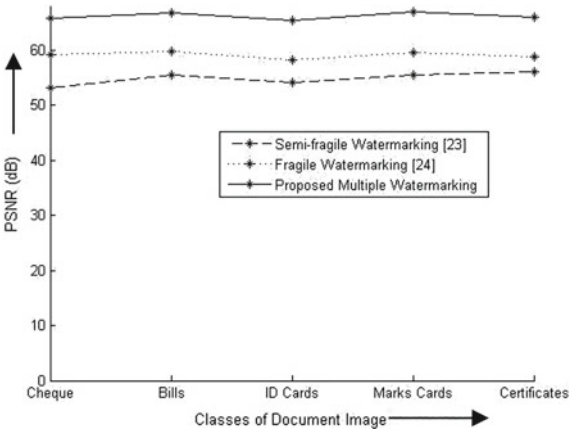

Fig. 3 PSNR values of different classes of document images in the corpus

Table 2 Average TDA and TRA values for different intentional attacks

Intentional attacks	Existing semi-fragile watermarking scheme [23]	Existing fragile watermarking scheme [24]	Proposed multiple watermarking scheme	
	TDA	TRA	TDA	TRA
Insertion	0.9	0.87	0.94	0.92
Deletion	0.92	0.91	0.95	0.94
Modification	0.87	0.87	0.94	0.92

depends on the type of the block. Hence, the noise induced due to watermarking is reduced and this contributes for the better fidelity of the watermarked image.

5.2 *Effectiveness Analysis of Detection and Correction Operations*

The effectiveness in detecting and correcting tamper of an attacked block of the proposed multiple watermarking schemes is evaluated in terms of accuracy of tamper detection and tamper recovery parameters. Accuracy of tamper detection and recovery is evaluated as follows:

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

where n—total number of bits in the fragile watermarked blocks, ta—tampered bit, and 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 multiple watermarking scheme and existing semi-fragile [23] and fragile

watermarking [24] schemes separately. These values are tabulated in Table 2. It can be observed that proposed multiple watermarking scheme exhibits better performance in both detection and correction operations on the tampered information content of document image.

6 Conclusions

A novel watermarking technique for protection of document images using multiple watermarking schemes on the same image is proposed in this paper. The blocks of a document image have been automatically classified into various types with greater accuracy. The performance analysis of the proposed approach reveals significant improvement in the fidelity of the watermarked image. The proposed scheme also outperforms the existing methods [23, 24] with better tamper detection and recovery capabilities. Improvement on the accuracy of identification of the type of block is the task of further enhancement.

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.: Multimedia watermarking techniques. Proc. IEEE **87**(7), 1079–1107 (2002)
4. Potdar, V.M., Han, S., Chang, E.A.: 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. Lect. Notes Comput. Sci. **5097**, 839–849 (2008)
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 European Symposium on Optics/Photonics in Security & Defence, pp. 173–182 London (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 Workshop on Image Analysis for Multimedia Interactive Services (2001)
15. Kim, M., Lee, W.: A content-based fragile watermarking scheme for image authentication. Lect. Notes Comput. Sci. Content Comput. **0302**, 258–265 (2004)
16. Habib, M., Sarhan, S., Rajab, L.: A robust fragile dual watermarking system in the dct domain. Lect. Notes Comput. Sci. Knowl.-Based Intell. Inf. Eng. Syst. **3682**, 548–553 (2005)
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, MA (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. Zhang, X., Wang, S.: Watermarking scheme capable of resisting sensitivity attack. IEEE Sign. 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. Sec. 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 Sign. Process. Lett. (Communicated)
25. Aggarwal, D.: An efficient watermarking algorithm to improve payload and robustness without affecting image perceptual quality, J. Comput. **2**(4) (2010). ISSN 2151-9617