Research Journal of

Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 3 (4): 229-236, 2011
ISSN 1815-7432 / DOI: 10.3923/rjit.2011.229.236

A High-capacity Lossless Algorithm for Watermarking Binary Images

Wei Liang, Jianbo Xu and Jing Long
School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China

Corresponding Author: Wei Liang, School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China Tel: 86-731-58290227 Fax: 86-781-58290194

ABSTRACT
In order to solve the low capacity and poor visual quality of binary image watermarking algorithm, a high-capacity lossless watermarking algorithm is presented. The proposed algorithm first encodes the original image and then determines parameter values of watermark locations according to image block characteristic coefficient of RS code. We randomly select cross-substitution process model blocks according to value of replace degree factor. Finally, binary image watermark is embedded through difference of replace methods in two modes. Experimental results show that the algorithm effectively enhances visual quality of watermark in secret image. The effective capacity of embedded watermark is obviously increased and the original image can be losslessly recovered in watermark extraction.

Key words: Binary image, watermark, replace mode, lossless recovery

INTRODUCTION
With social development and technology advancement, digital image, as mainstream media for information exchange (Tian, 2003; Fridrich *et al.*, 2001), has become a significant carrier of information hiding with the extensive application market of digital image, digital watermarking algorithm has also been concerned by more research institutions and scholars (Celik *et al.*, 2005; Fu and Au, 2002). In general, watermark embedding may alter pixel values of original image. The alteration can be ignored by human visual system; however, it cannot be tolerated in specific application fields such as medical image or remote sensing image. Since, the receiver need further analyze and process original image, therefore, the secret image need to be losslessly recovered after extracting watermark to get the original image with embedded watermark. It brings out higher demands for lossless watermark image (Wu and Liu, 2004; Yang and Kot, 2004, 2006).

The existing research of lossless digital watermarking technology primarily focused on grayscale or color continuous image (Pan *et al.*, 2006; Tzeng and Tsai, 2003; Yang and Kot, 2007; Robertson *et al.*, 1996; Lu *et al.*, 2002). Since the coefficient of these images has a large range, slight alteration will not result in obvious visual distortion. Binary image has two brightness level of black and white, vision sense of which is greatly different. Each pixel value represents specific meaning. Any slight alteration will leave distinct modification mark or change the expression of image information. In consequence, many lossless watermarking algorithm based on continuous images can not be used to binary images. The lossless watermarking algorithms which aim at binary images are less (Lu *et al.*, 2002). The related literature is few. Most existing algorithms embed watermark in image edge information to avoid visual distortion. The domestic and overseas related technologies have two categories: methods based on reversibility of embedding function. For instance, in literature (Tsai *et al*., 2005) constructed logic operation on each eligible pixel to embed watermark information. The lossless recovery of original image was implemented by inverse operation of the logic operation, without any auxiliary information. However, the secret image obtained by this algorithm has poor quality and less watermark capacity. Furthermore, how to accurately determine the altered pixel locations in lossless recovery has no much description. Another category is method based on replacing mode block of image. For example literature (Ho *et al*., 2009) selected two specific modes as a group and replaced the two modes mutually for watermark embedding. This method performed lossless recovery at location of mode block which appears with less frequency in original image. The characteristic of image block locations are without reasonable computation when selecting and replacing mode block. Therefore, the capacity is much limit and lossless recovery has poor visual quality.

In order to solve the low capacity and poor visual quality of binary image watermarking algorithm, a high-capacity lossless watermarking algorithm is presented. Fist, we encode the original image and compute characteristic of RS code and then determine the structure of replacing mode block according to coefficient of replace degree factor S of binary image. At last, high-capacity lossless algorithm for watermarking binary image is implemented by embedding strategy of coding sequence.

LOSSLESS WATERMARKING ALGORITHM BASED ON CROSS-SUBSTITUTION

The lossless watermarking methods by replacing mode blocks consist of two sub procedures: Encoding of original image and embedding of lossless watermark information. As seen from Fig. 1, we can firstly extract the edge information of image which is suitable for embedding watermark and compute characteristic value of image block locations. Finally, we determine various substitution modes for embedding watermark.

Characteristic values of image block locations: For enhancing watermark security, the proposed algorithm will not embed original watermark information but image processed with RS code. We perform XOR operation on pixels of original image A (i, j) and binary sequence B with the same length generated by cipher. Coding image block $\bar{A}(i,j)$ is generated, that is:

$$\bar{A} = A \otimes B \tag{1}$$

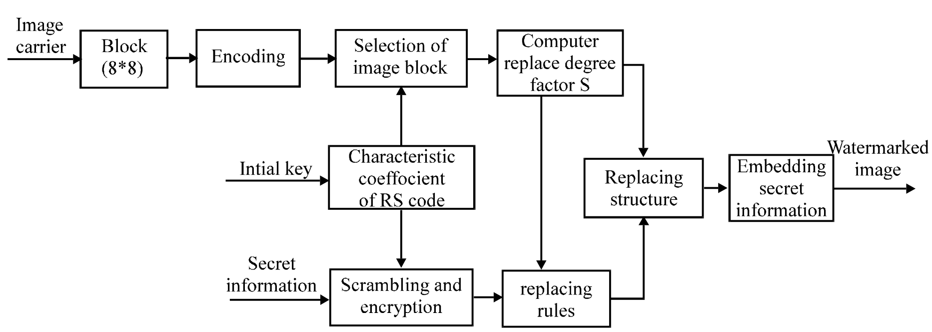


Fig. 1: The procedure of watermark embedding

Definition 1: One encoding symbol X_i ($0 \le i \le 35$) in RS encoding sequence can be defined as:

$$X_i = \bar{A} \otimes B \tag{2}$$

The definition of encoding symbol ensures numeric area of X_i ($0 \le i \le 35$) in [0,255] which meets that in GF (2^8) Galois field.

Definition 2: The corresponding value Sa_i ($0 \le i \le 35$) of encoding image block $\bar{A}$ is defined as standard deviation in this block:

$$SAi = \sqrt{\frac{\sum_{X=1}^{36} (S_x - S_a)^2}{36}} \tag{3}$$

Here, S_a denotes mean value of S_x ($0 \le x \le 35$) in Sa_i ($0 \le i \le 35$).

Theorem 1: For RS (38,36) code of image block $\bar{A}$ with size of 8×8 in GF (2^8) Galois field, if values lie in [0,255], the check symbols b_0 and b_1 could adaptively detect and correct any one of 38 encoding symbols.

Proof: With Definition 1 and 2, assuming encoding sequence RS (38, 36) is, we have the following two expressions:

$$S_0 = a_{35}+a_{34}+....a_0+b_1+b_0 = 0 \tag{4}$$

$$S_0 = a_{35}+a_{34}+....a_2+a_1d_1+a_0b_0 \tag{5}$$

By solving expressions 4 and 5, we get b_0 and b_1.

With above operations, check coefficients b_0 and b_1 are used in pixel characteristics of binary image for constructing RS code randomly. The computation of location characteristic of image blocks is according to that of check code.

Cross-substitution of mode blocks: In binary image, the similarity between two image blocks with size of 8×8 can be used to select mode blocks pair which is suitable for mutually replacing. A replace degree factor S is chose to measure the consistency of two adjacent image blocks. The expression is denoted as:

$$S = 2 \times \sum_{k=j}^{j+1} A(k,i) \oplus A(k,i+1) \tag{6}$$

Here, $\bar{A}(i,j)$ denotes pixel value at jth row and i th column in 8×8 image block. Since, human visual system is sensitive to alteration at horizontal and vertical direction, smaller value of replacing degree factor S means any alteration on image block will be perceptive, it is less suitable for alteration; conversely, more suitable.

Different substitution method of image blocks has direct relation with embedding effect of watermark information. By using cross substitution method, we can get more image blocks. The mode block which is suit to substitute occupies more probability.

In watermark embedding area, the selection algorithm of 8×8 image block A can be described as:

$$A^{w}_{n}(i,\ j) = \begin{cases} \lfloor a_n \times A_n(i,j) \rfloor, \text{if } S \geq 1 \\ A_n(i,j), \qquad \text{if } 0 \leq S \leq \end{cases} \tag{7}$$

Here, n denotes the number of 8×8 image blocks in original image. W is binary watermark. $A^{0}_{n}(i,\ j)$ represents pixel value of watermarked image after substitution operations. $A^{W}_{n}(i,\ j)$ and $A_n(i,\ j)$, respectively denotes (i,j) pixel value of nth 8×8 image block in watermarked image A before substitution and original carrier image A. S is adaptive smoothness factor corresponding to nth block of image A. Consequently, with formula 7, we get the cross substitution expression of image block in watermark embedding:

$$A^{0}_{n}(i,j) = A_n{}^{w}(i,j) + SA_n(i,j),\ 1 \leq i,\ j \leq 8, n \in \{1, 2, \ldots\ldots\ldots N\} \tag{8}$$

Watermark embedding: Figure 1 shows the watermark embedding procedure. For a given original image A, the preprocessed image is A. We divide binary image into several 8×8 blocks. The watermark is separately embedded and extracted in each block. Since image blocks with all 1 (white) and all zero (black) are absolutely white or black smooth image blocks. It is perceptive to alter this type of image blocks. Therefore, these image blocks cannot be used to hide information while other blocks can do. The embedding type has two categories: Type-1 and Type-2. The substitution between blocks of the same type represents embedding watermark 0 while between blocks of different type, watermark is 1. In this embedding method with fixed length, each substitution of mode blocks can only embed one bit watermark information. Each type of mode blocks has only used 2/3 embedding capacity. Therefore, we perform cross substitution to specific type of mode blocks TYPE-1 and TYPE-2 which will increase number of mode blocks, thus increase the amount of embedded watermark information. The watermark embedding is described as follows:

Step 1: Given 8×8 image block A, the preprocessed 8×8 image block is A. The secret processed image m is scrambled with key key1, m is generated. In this way, the security of watermark embedding is enhanced. For embedding image watermark, it also improves the robustness

Step 2: By solving expression (3) and (4), the check code b_0 and b_1 of RS (38, 36) encoding sequence is computed. We use b_0 and b_1 to construct structure of RS encoding sequence and select 36 image block with size of 8×8, with the first 16 pixels of which as watermark embedding locations

Step 3: Since binary image only has two color tone of black and white, we compute replace degree factor S on the basis of keeping better connectivity of pixels

Step 4: With the coefficient of replace degree factor S, we randomly select a block by controlling of. Through the embedding strategy, we divide encoding sequence into two different substitution modes: (1) substitution between blocks of the same type denotes watermark 0; (2) substitution between blocks of different type denotes watermark 1

Step 5: In embedding strategy of encoding sequence, if capacity of encoding sequence is limit, we could combine encoding sequence adaptively and perform cross substitution by selecting two different substitution modes for reducing embedding overhead. The procedure repeat through step 3 and step 5, until all watermark information are embedded

Watermark extraction: In the presented algorithm, watermark extraction will divide secret image into blocks, same as embedding. All blocks which are possible to hide secret information will be orderly found under control of key. Finally, the hidden information is extracted in these blocks. The extraction procedure is very simple, in which all 1 or all 0 represents no hidden information in block. If there are two "0" in mode blocks with the same substitution, the pixels at bottom left and top right are the extracted information. Zero or four 0 in the block represents no hidden information. The algorithm to extract hidden information in mode blocks is as follows:

Step 1: With the encoding sequence and embedding strategy of mode blocks substitution, the watermarked binary image is divided into 8×8 blocks as that in embedding procedure. Under control of, we get block m which probably carries watermark information

Step 2: With key 1, we compute check code b_0 and b_1 of encoding sequence RS (38, 36) for each image block probably carrying watermark information

Step 3: By using decoding principle of mode block, the first 16 pixels of 8×8 image blocks can be obtained. Meanwhile, the watermarked locations could be known

Step 4: We combine the digital bit in the watermarked locations to get the embedded binary watermark information

EXPERIMENTAL RESULTS AND ANALYSIS

The presented algorithm is evaluated in Visual C++ 6.0 environment. Three binary images with different texture information are used as test images. We use our algorithm respectively on these three images and the experimental results are shown in Fig. 2.

By embedding the same number of watermarks in the test sample, whatever non-text or text, our method has good secrecy.

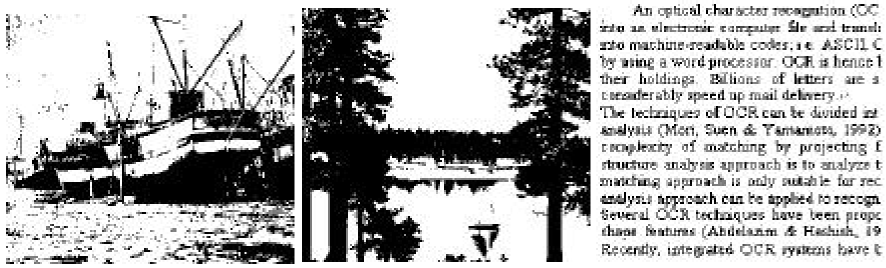
Evaluation of visual quality: In order to quantize invisibility and robustness, Peak Signal to Noise Ratio (PSNR) is used to describe difference between original image and watermarked image. Quality related function NC is to evaluate the quality of extracted secret information:

$$\mathrm{PSNR} = 10\log_{10}\frac{255}{\mathrm{RMSE}} \tag{9}$$

Here, RMSE denotes root mean square error of pixel gray value:

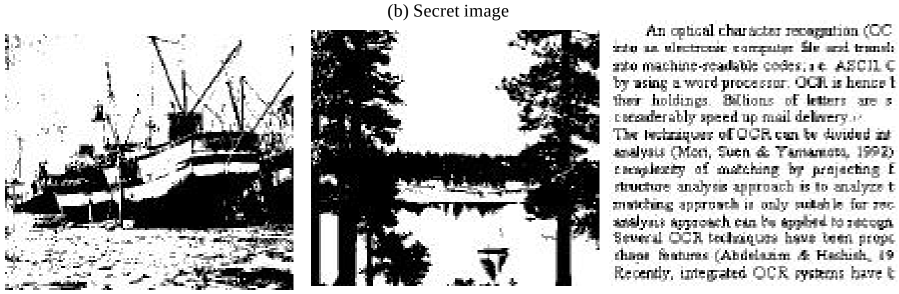
$$\mathrm{RMSE} = \sqrt{\sum_i \sum_j (X_{ij} - X^s_{ij} / MN} \tag{10}$$

M and N is length and width of original image. If the corresponding location has larger PSNR after embedding watermark, the watermarked image is more similar to the original:



(a) Original image

(b) Secret image



(c) Watermarked image

Fig. 2: The experimental results of presented algorithm

$$NC = \frac{\sum_i \sum_j s(i,j)s'(i,j)}{\sum_i \sum_j [s(i,j)]^2} \tag{11}$$

We compare present method with method of Tsai *et al.* (2005) and Ho *et al.* (2009) for evaluating the advantages. The experimental results are shown in Fig. 3. For methods in literatures (Tsai *et al.*, 2005; Ho *et al.*, 2009), the obtained PSNRs are increasing successively. By using the proposed method in above test sample figures, our method increases PSNR by 24.2%. Consequently, the mean embedding capacity mainly depends on texture information complexity of binary image carrier.

As seen in Fig. 3, PSNR using the proposed algorithm is higher than that of other methods. Meanwhile, in some cases, the reduction of embedded secret information may not improve visual quality of secret image. It has some relations with texture information of binary image itself.

Security analysis: We have performed copy attack, JPEG compression attack and noise attack on the watermarked image for evaluating the security. The experimental results in Fig. 4 show that

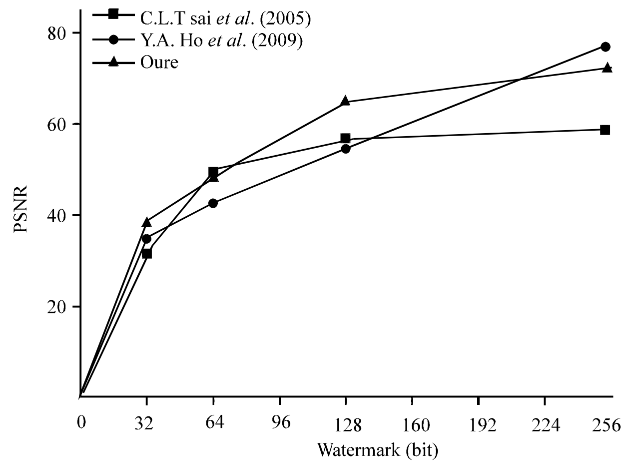


Fig. 3: PSNR comparison of three methods by using test figure Boat

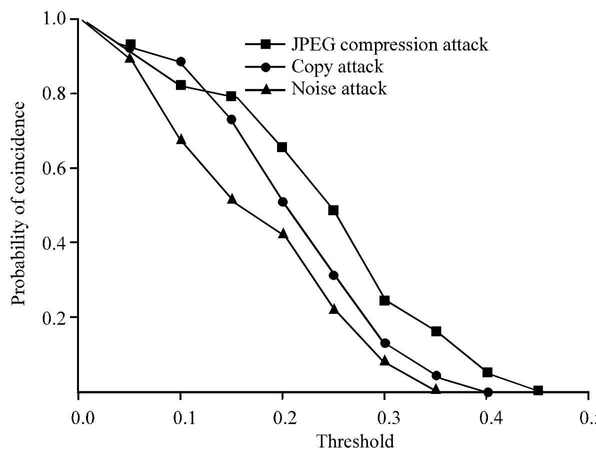


Fig. 4: Probability of coincidence

out method has lower probability of coincidence within a certain threshold which proves the above analysis. The algorithm has stronger resistance to common attacks.

CONCLUSION

A high-capacity lossless algorithm based on cross substitution is presented for watermarking image blocks. The algorithm divides image into blocks, embeds watermarks with different length and substitutes mode blocks with suitable size. The watermark capacity is greatly extended. Considering human visual system, we present connectivity factor and smooth factor of adjacent pixels. The suitable mode blocks are selected for substitution according to edge characteristic of binary image, thus embedding watermark. By comparing with related algorithm, the proposed algorithm has better superiority in terms of watermark capacity and visual quality which can be widely applied in fields of medical science, military and law.

ACKNOWLEDGMENT

This study is supported by the Scientific Research Fund of Hunan Provincial Education Department (Grant Nos. 09A027, 09C403), Natural Science Foundation of Xiangtan United Fund of Hunan Province (Grant No. 09JJ9006£¬11JJ9014), the Planned Science and Technology Project of Hunan Province, China (Grant No.2011GK3156) and Innovation Fund Project for Graduate Student of Hunan University of Science and Technology (S100119).

REFERENCES

Celik, M.U., G. Sharma, A.M. Tekalp and E. Saber, 2005. Lossless generalized-LSB data embedding. IEEE Trans. Image Process., 14: 253-266.

Fridrich, J., M. Goljan and R. Du, 2001. Invertible authentication watermark for JPEG images. Proceedings of the International Conference on Information Technology: Coding and Computing, April 2-4, 2001, Las Vegas, NV., USA., pp: 223-227.

Fu, M.S. and O.C. Au, 2002. Data hiding watermarking for halftone images. IEEE Trans. Image Process., 11: 477-484.

Ho, Y.A., Y.K. Chan, H.C. Wu and Y.P. Chu, 2009. High-capacity reversible data hiding in binary images using pattern substitution. Comput. Stand. Interfaces, 31: 787-794.

Lu, H., J. Wang, A.C. Kot and Y.Q. Shi, 2002. An objective distortion measure for binary document images based on human visual perception. Proc. Int. Conf. Pattern Recognit., 4: 239-242.

Pan, J.S., H. Luo and Z.M. Lu, 2006. A lossless watermarking scheme for halftone image authentication. Int. J. Comput. Sci. Network Secur., 6: 147-151.

Robertson, G.R., M.F. Aburdene, R.J. Kozick and R.F. Harris, 1996. Differential block coding of bi-level images. IEEE Trans. Image Process., 38: 1368-1370.

Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circ. Syst. Video Technol., 13: 890-896.

Tsai, C.L., H.F. Chiang, K.C. Fan and C.D. Chung, 2005. Reversible data hiding and lossless reconstruction of binary images using pair-wise logical computation mechanism. Pattern Recognit., 38: 1993-2006.

Tzeng, C.H. and W.H. Tsai, 2003. A new approach to authentication of binary images for multimedia communication with distortion reduction and security enhancement. Commun. Lett., 7: 443-445.

Wu, M. and B. Liu, 2004. Data hiding in binary image for authentication and annotation. IEEE Trans. Multimedia, 6: 528-538.

Yang, H. and A.C. Kot, 2004. Data hiding for bi-level documents using smoothing technique. Proc. Int. Symp. Circuits Syst., 5: 692-695.

Yang, H. and A.C. Kot, 2006. Binary image authentication with tampering localization by embedding cryptographic signature and block identifier. IEEE Sign. Proc. Lett., 13: 741-744.

Yang, H. and A.C. Kot, 2007. Pattern-based data hiding for binary image authentication by connectivity-preserving. IEEE Trans. Multimedia, 9: 475-486.