A Lossless Watermarking Scheme for Halftone Image Authentication

Jeng-Shyang Pan[†], Hao Luo[††], and Zhe-Ming Lu[††,†††]

[†]Department of Electronic Engineering, National Kaohsiung University of Applied Sciences, Kaohsiung, Taiwan
[††]Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China
[†††]University of Freiburg, Freiburg, Germany

Summary
Nowadays, halftone images appear routinely in books, magazines, printer outputs, and fax documents. It is desirable to embed data in halftone images for copyright protection and content authentication. This paper proposes a novel watermarking scheme for halftone image authentication, exploiting image hash as a fragile watermark. After pixel blocking and ordering, a lookup table is constructed according to blocks' frequency of occurrence. Watermark embedding is to displace the original blocks with the corresponding similar blocks in the lookup table, and in the reverse process watermark is extracted. Some extra blocks are randomly selected with a secret key for the lookup table embedding, and the original data of these blocks are also inserted into the image. In image authentication, the lookup table is reconstructed first with the secret key, and then a simple table-look-up procedure is employed to extract the watermark hash, finally we only need to compare the watermark hash with the hash of recovered image: if they are equal, the original image suffers no alteration; otherwise it is changed. As a lossless technique, the original image can be perfectly recovered by performing the reverse process of the watermark embedding if the watermarked image is intact. It is necessary to keep the content of original host image unchanged in some specific applications, where content accuracy of the host image must be guaranteed, e.g. military maps, medical images, great works of art, etc. As a fragile watermarking, even one pixel toggling can be detected. Because of the small quantity of watermark, low quality distortion is introduced to the halftone image. Experiment results demonstrate the effectiveness of the scheme.

Key words:
Halftone image, Lossless watermarking, Hash sequence, Image authentication

1. Introduction

Digital halftoning is a technique to transform multi-tone images into two-tone images, e.g. 8-bit grayscale images into 1-bit binary images. The halftone images can resemble the original images when viewing from a distance by the low-pass filtering in the human visual system. Most popular halftoning methods can be divided into three categories: ordered dithering [1], error diffusion [2], and direct binary search [3]. Among these, error diffusion achieves a preferable tradeoff between good visual quality and reasonable computational complexity. With halftone images widely used, content authentication, changes localization and copyright protection for this kind of images are receiving an increasing interest among researchers with digital watermarking techniques. Many watermarking techniques are proposed for multi-tone images, and those for halftone images are developed in recent years. In contrast, quite a small number of authentication watermarking approaches are available for halftone images.

In the literature, most methods cannot perfectly restore the original image in watermark extraction or detection. Existing watermarking usually introduces irreversible degradation to the host medium. Although the degradation is slight, it cannot satisfy the requirement of some specific situations, where content accuracy of the host image must be guaranteed, e.g., military maps, medical images, great works of art, etc. Therefore, it is quite necessary to develop a lossless watermarking method for authenticating halftone images. However, till the present time, there has been little attention paid to the lossless watermarking techniques for halftone images.

This paper proposes a watermarking scheme for halftone images combining the above two characteristics, namely, lossless and for authentication purpose. In image authentication, we only need to compare two hash sequences: the extracted watermark hash and the hash of the restored image. If the two sequences are equal, the halftone image suffers no alteration; otherwise it is changed intentionally or unintentionally.

The rest of the paper is organized as follows. Section 2 reviews the previous work on halftone image watermarking, in particular for secure authentication. Section 3 extensively describes the proposed scheme including watermark embedding and extraction, and meanwhile the authentication process. In Section 4, experimental results are presented for the demonstration of its effectiveness. Section 5 concludes the paper.

2. Previous work

Manuscript revised January 2006.

Different from grayscale or color images, there are mainly three challenges to embed data in halftone images. The first one is less information redundancy for each pixel value has only one bit. Consequently many watermarking approaches cannot be directly transplanted to halftone images. Another challenge is visual quality degradation. To insert data in halftone images, change of the pixel value is either from black to white or from white to black. Usually, human visual system is sensitive to the abrupt change, e.g. the white cross and the black cross. The third challenge is lower embedding capacity. High capacity is one of the key factors to evaluate the performance of watermarking techniques. Actually, for halftone images, this challenge is closely related to the former two challenges. It is expected that a large quantity of data cannot be embedded into halftone images considering visual quality degradation, for less information redundancy can be explored.

Available data hiding methods for halftone images can be divided into three classes: (1) Pixel-based: this kind of methods is to change the values of individual pixels, usually randomly selected [4] [5]. (2) Block-based: these methods divide the host image into blocks and modify characteristic of some blocks [6] [7]. (3) Hybrid-based: they insert data by combining the characteristics of pixel-based and block-based [8].

Kim and Afif introduce an authentication watermark AWST (authentication watermarking by self toggling) for halftone images in [9]. It consists of following steps: choosing a set of pseudo-random pixels in the image, clearing them, computing the message authentication code (MAC) or the digital signature (DS) of the random-pixels-cleared image, and inserting the resulting code into the selected random pixels. One disadvantage of the AWST is it cannot obtain the original image in watermark extraction and image authentication when the host image is not changed, because it clears some pixels randomly selected and never can be recovered. However, our scheme overcomes this problem: the host image can be perfectly restored as long as it suffers no alteration, otherwise even a single pixel change can be detected. The scheme can only simply detect the change without spatially locating them.

3. Proposed scheme

Existing watermarking techniques [10] can be classified into three categories: robust, fragile and semi-fragile. Among them, fragile watermarks are easily corrupted by image processing operations, and thus often used for checking image integrity and authentication. Authentication watermark is a hidden data inserted into an image that can be applied to detect any unauthorized change of the image. Our scheme is a block-based method.

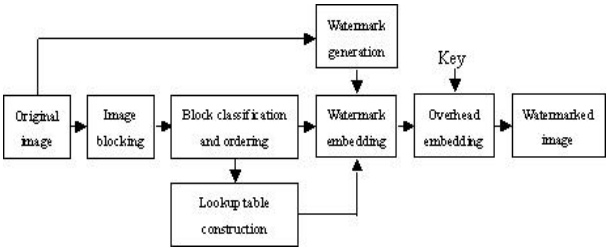

Fig. 1 Block diagram of watermark embedding.

3.1 Watermark embedding

The block diagram of watermark embedding is as shown in Fig. 1, and each step is detailed described below.

Watermark generation Our scheme exploits image hash as a fragile watermark. Image hashing is known as the problem of mapping an image to a short binary string. Image hash function has the properties that perceptually identical images have the same hash value with high probability, while perceptually different images have independent hash values. In addition, the hash function is secure, so that an attacker cannot predict the hash value of a known image. Image hashing is one-way, collision-free and relatively easy to compute for any given image. Hence, the watermark can be viewed as adaptive for its sensitivity to change of the image.

Our scheme generates the watermark hash W_H of the original image using hash functions. Suppose W_H is an L-bit "0-1" sequence, thus we need L blocks to embed data for each block can be inserted into 1-bit data.

Image blocking The scheme starts with dividing the halftone image into disjoint pixel blocks. Suppose the size of the halftone image I and a block B are M×N and m×n respectively, and I is segmented into b blocks $B_1, B_2, \ldots B_b$. Since each pixel is either black or white, an m×n block has totally $2^{m\times n}$ different patterns. Some patterns never occur in I, while some occur many times.

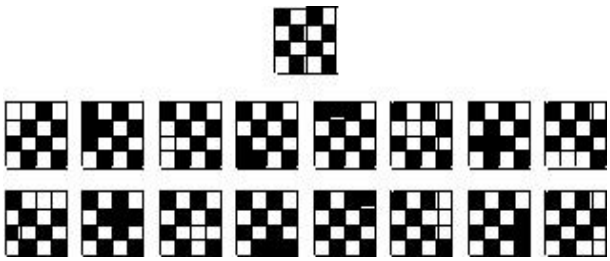

Fig. 2 An example of an original block and its similar blocks.

Block classification and ordering This step aims to select appropriate blocks to embed data. To all blocks in I, we count their occurrence respectively, and then rank the frequency of occurrence. Sorted in descending order, suppose $t_1, t_2, \ldots t_j$ ($j \le 2^{m\times n}$) denotes the occurrence times

of block pattern p_1, p_2, …p_j, respectively. It is clear that Formula (1) is satisfied.

$$\sum_{l=1}^{j} t_l = b \tag{1}$$

Lookup table construction A lookup table T is made up of original blocks O_1, O_2, …O_u, similar blocks S_1, S_2, …S_u, and frequency of occurrence of O_1, O_2, …O_u. S_j $(1 \le j \le u)$ is the corresponding similar block of O_j. Similar blocks that never occur in the image are used to displace original blocks for watermark embedding. In the context, two blocks with the same size are considered similar if the Hamming distance between them is 1, namely, only one pixel value is different. Therefore each block has $2^{m\times n}$ similar blocks. As an example a 4×4 block and its 16 similar blocks are shown in Fig. 2.

According to the frequency of occurrence, we select k block patterns with highest k occurrence t_1, t_2, …t_k as a candidate block set.

To a block in the set, if all of its similar ones occur at least once in I, then the block is discarded from the candidate set. If one or more similar blocks do not occur, we randomly select one as its similar block. All candidate blocks are investigated like this, and original blocks and corresponding similar blocks are recorded in T. Besides this, we need to record the frequency of occurrence for computing embedding capacity. So far a lookup table is constructed. It is essential that each similar block in T must be different from any other blocks. More details of the lookup table construction can be seen in [11].

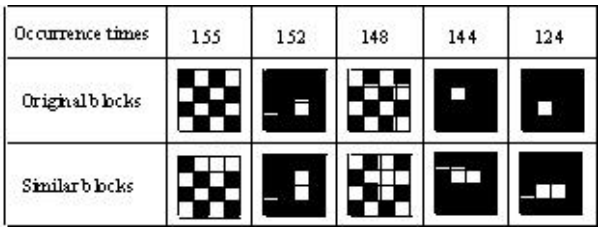

Fig. 3 An example of a lookup table.

As an example shown in Fig. 3, the lookup table is constructed on the halftone Lena image, with the size of the Lena and a block 512×512 and 4×4 pixels, respectively. Only 5 blocks with highest frequency of occurrence and their similar blocks are given.

Watermark embedding To embed data, we compare the block B_i $(1 \le i \le b)$ with O_1, O_2, …O_u one by one. If B_i is the same as O_j, 1-bit data can be inserted with the rule: If "0" is to be embedded, we do not change B_i, if "1" is to be embedded, we displace B_i with S_j. The operation as shown in Formula (2) is repeated for all blocks B_1, B_2, …B_b.

$$\begin{cases} B_i = O_j & \text{if} \quad W_H = 0 \\ B_i = S_j & \text{if} \quad W_H = 1 \end{cases} \tag{2}$$

Overhead information embedding In [11], the lookup table needs extra storage space for watermark embedding and extraction. Since different image has different lookup table, no universal table is suitable for all images. Besides, the lookup table is also need to be protected. Our scheme overcomes the disadvantage successfully by embedding the lookup table in the host image as overhead information.

The overhead information is embedded as follows.

(i) Use a pseudo-random number generator with a secret key K to choose a set of non-repeating blocks G in I. Note these blocks must not coincide with the watermarked blocks.

(ii) Embed G in I. An m×n block of G is rearranged to a "0-1" string and embedded as the same way of watermark embedding. The process is repeated for all blocks in G. Since a block displacement can embed one bit, Formula (3) must be satisfied. In Formula (3), $2umn$ is the total bits of the lookup table T.

$$\sum_{l=1}^{k} t_l \ge W_H + 2umn \quad (1 \le k \le j) \tag{3}$$

(iii) Displace blocks in G with blocks in T directly.

3.2 Watermark extraction and image authentication

The block diagram of watermark extraction and image authentication is as shown in Fig. 4.

Lookup table reconstruction The watermarked image I' is segmented into m×n blocks B_i' $(0 \le i \le b)$. Before watermark extraction, the lookup table must be reconstructed first. We use the same key K to find out the blocks G', and thus T' can be recovered by extracting G' directly.

Watermark extraction Let W_H' denotes the information extracted. According to the lookup table T' the watermark is extracted as shown in Formula (4). We compare the block B_i' $(1 \le i \le b)$ with blocks in T'. If B_i' is the same as O_j' $(1 \le j \le u)$, "0" is extracted; if B_i' is the same as S_j' $(1 \le j \le u)$, "1" is extracted.

$$\begin{cases} W_H' = 0 & \text{if} \quad B_i' = O_j' \\ W_H' = 1 & \text{if} \quad B_i' = S_j' \end{cases} \tag{4}$$

The extracted information W'_H consists of the extracted watermark H_1 and the original data of G'. If "0" extracted, we do not change the block; if "1" extracted, we displace S'_j with B'_i. After we recover G', the restored image R is obtained.

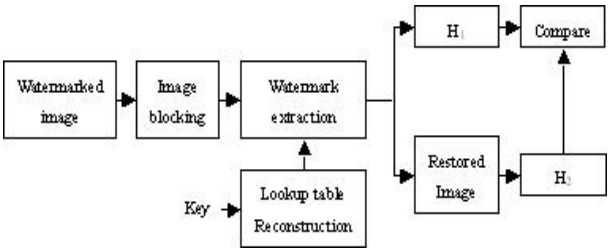

Fig. 4 Block diagram of watermark extraction and image authentication.

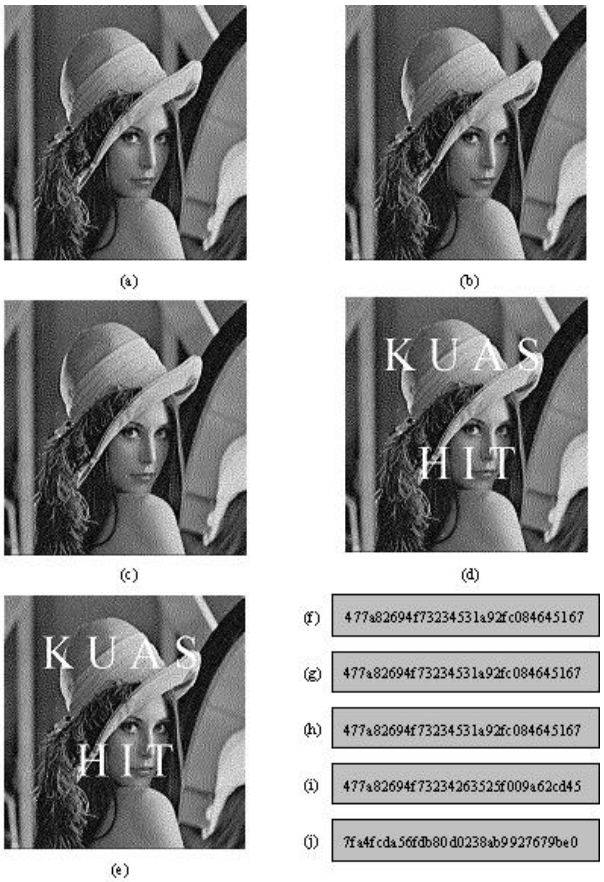

Fig. 5 Experimental results on halftone Lena Image. (a) Original Lena, (b) Watermarked Lena without alteration, (c) Restored Lena of (b), (d) Watermarked Lena with alteration, (e) Restored Lena of (d), (f) Original watermark, (g) Watermark extracted from (b), (h) hash of (c), (i) Watermark extracted from (d), (j) hash of (e).

Image authentication The same hash function is used to compute the hash sequence H2 of R. Thus image authentication is reduced to a task of comparing H1 and H2. On one hand, if the host image I suffers no alteration, H1 is equal to H2, otherwise different. On the other hand, I suffers no alteration if H1 is equal to H2. In a word, if H1 is different from H2, I is changed, at least a single pixel.

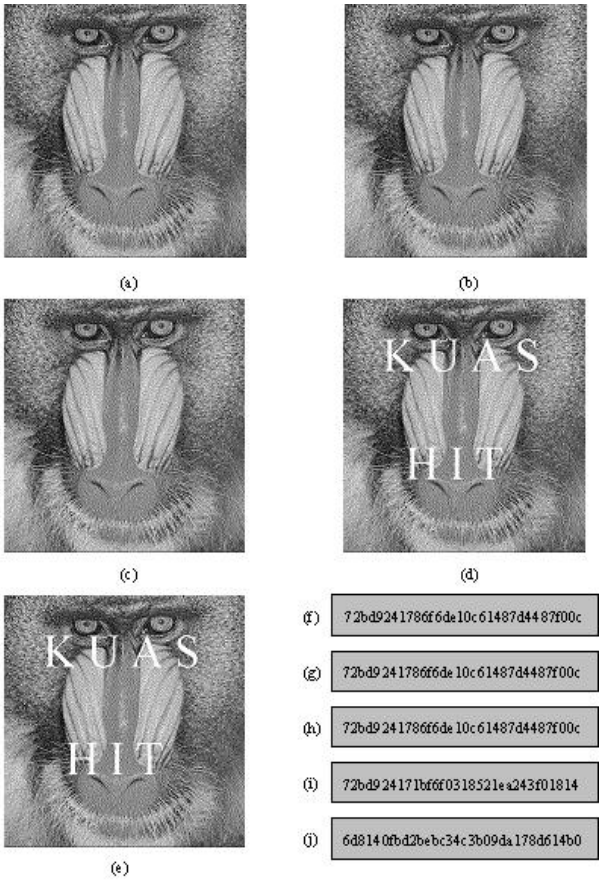

Fig. 6 Experimental results on halftone Baboon Image. (a) Original Baboon, (b) Watermarked Baboon without alteration, (c) Restored Baboon of (b), (d) Watermarked Baboon with alteration, (e) Restored Baboon of (d), (f) Original watermark, (g) Watermark extracted from (b), (h) hash of (c), (i) Watermark extracted from (d), (j) hash of (e).

4. Experimental results

In the experiment, 512×512 halftone Lena image and Baboon image are selected to test the effectiveness of the method. As shown in Fig. 5(a), the halftone Lena image is divided into 4×4 blocks. The original watermark, i.e. the hash sequence of Lena, is computed by the MD5 hash function. After translating the string into "0-1" sequence, 128-bit digest is obtained.

In authentication, we compare the watermark extracted from the watermarked image, and the hash sequence computed from the restored image. When the two

sequences are equal, as shown in Fig. 5(g) and Fig. 5(h), we can confirm the watermarked Lena suffers no alteration. Both of them are equal to the original watermark, as shown in Fig. 5(e). While if the watermarked Lena is tampered by a mark "KUAS HIT" (Fig. 5(d)), the two sequences are different, as shown in Fig. 5(i) and Fig. 5(j). Therefore, we can make a judgment by virtue of the two sequences are equal or not: if equal, the image suffers no alteration; otherwise changed.

The Baboon image is also divided into 4×4 blocks. As shown in Fig. 6, experimental results also verify effectiveness of the scheme.

4. Conclusion

This paper presents a lossless watermarking scheme for halftone image authentication. The hash sequence of the image is embedded as an adaptive fragile watermark. To judge weather the original image is changed or not, we only need to compare the extracted watermark and the hash sequence of the restored image. If they are exactly the same, the image suffers no alteration; otherwise it is changed. As long as the watermarked image is not unauthorized changed, the original image can be perfected recovered. Besides, no information needs to be saved except a secret key.

Acknowledgment

The authors would like to express their thanks to Dr. Bian Yang for his valuable advice.

References

[1] R. A. Ulichney, "Digital Halftoning," Cambridge, MA: MIT Press, 1987.
[2] R. W. Floyd and L. Steinberg, "An adaptive algorithm for spatial gray scale," Proc. SID 75 Digest. Society for information Display, pp. 36-37, 1975.
[3] D. Lieberman and J. Allebach, "Digital halftoning using direct binary search," Proc. of 1996 1st IEEE Int. Conf. on High technology, pp. 114-124, September 1996
[4] M.S. Fu, and O.C. Au, "Data Hiding by Smart Pair Toggling for Halftone Images," IEEE Int Conf Acoustics Speech and Signal Processing, vol. 4, pp. 2318-2321, 2000
[5] M.S. Fu, and O.C. Au, "Data Hiding Watermarking for Halftone Images," IEEE Trans Image Processing, pp. 477- 484. 2002
[6] Z. Baharav, and D. Shaked, "Watermarking of Dither Halftone Images," Hewlett-Packard Labs Tech Rep, HPL-98-32, 1998.
[7] H. Z. Hel-Or, "Watermarking and Copyright Labeling of Printed Images," Journal of Electronic Imaging, pp. 794-803. 2001
[8] S.C. Pei, and J.M. Guo, "Hybrid Pixel-Based Data Hiding and Block-Based Watermarking for Error-Diffused Halftone Images," IEEE Trans Circuits and Systems for Video Technology, pp. 867-884, 2003
[9] H.Y. Kim, and A. Afif, "Secure Authentication Watermarking for Binary Images," Proc Brazilian Symp on Computer Graphics and Image Processing, pp. 199-206, 2003
[10] J. S. Pan, H. C. Huang and L. C. Jain, "Intelligent Watermarking Techniques," World Scientific, 2004.
[11] P. S. Liao, J. S. Pan, Y. H. Chen and B. Y. Liao, "A Lossless Watermarking Technique for Halftone Image," International Workshop on Intelligent Information Hiding and Multimedia Signal Processing, Melbourne, Australia, May 15, 2005.

Jeng-Shyang Pan received the B. S. degree in Electronic Engineering from the National Taiwan University of Science and Technology, Taiwan in 1986, the M. S. degree in Communication Engineering from the National Chiao Tung University, Taiwan in 1988, and the Ph.D. degree in Electrical Engineering from the University of Edinburgh, U.K. in 1996. Currently, he is a Professor in the Department of Electronic Engineering, National Kaohsiung University of Applied Sciences, Taiwan. Professor Pan has published more than 50 journal papers and 120 conference papers. He joints the editorial board for LNCS Transactions on Data Hiding and Multimedia Security, Springer, International Journal of Knowledge-Based Intelligent Engineering Systems, IOS Press, and International Journal of Hybrid Intelligent System, Advanced Knowledge International. He is the Co-Editors-in-Chief for International Journal of Innovative Computing, Information and Control. His current research interests include data mining, information security and image processing.

Hao Luo received the B. S. degree and the M. S. degree from Harbin Institute of Technology (HIT), Harbin, China in 2002 and 2004, respectively. He is a Ph.D candidate in the School of Electronic Engineering in HIT. His research interests are mainly in information security and mesh retrieval.

Zhe-Ming Lu received the B.S., M.S. and Ph. D. degrees in Electrical Engineering from Harbin Institute of Technology in 1995, 1997 and 2001, respectively. He was the Alexander von Humboldt Research Fellow in University of Freiburg in Germany, from Oct., 2004 to Jan. 2006. He has published more than 110 papers and four books. He has been program committee members in several international conferences. He is now the Professor and Director of the Visual Information Analysis and Processing Research Center, Harbin Institute of Technology Shenzhen Graduate School. His research interests are image processing, pattern recognition, information hiding and visual information retrieval.