Authentication of Binary Document Images Based on Embedding the BCH Codes of Watermarks

DA-CHUN WU[1,*] AND MING-KAO HSU[2]
[1]*Department of Computer and Communication Engineering, National Kaohsiung First University of Science and Technology, Taiwan*
[2]*Department of Information Management, Ming Chuan University, Taiwan*

ABSTRACT

Many commercial documents are easily transmitted via FAX or Internet. This paper explores a novel technique for the authentication of binary document images. An authentication method which uses BCH error correction codes is proposed. Logos or secret information in the forms of BCH codes are embedded in document images as the authentication signals. Even-odd relationships of lengths of run pairs are used for embedding information in binary images. We slightly adjust the length of run to represent the embedding bit value without causing noticeable differences. A controlled threshold is also introduced, for considerations of human perception, to filter out all those runs with too small a length. An authenticated resulting image is created in the authentication process, the embedded Logos or secret information is also extracted in the same time. The authentication jobs can be carried out without referencing the original document images. Experimental results show the feasibility of the proposed method.

Key words: watermarking, authentication, binary image, BCH.

1. INTRODUCTION

Nowadays, commercial documents such as invoices and patent documents are frequently delivered by FAX or over the Internet. It is an important and imperative topic to add extra information to digitalized documents so that we can protect intellectual property rights and prevent these documents from being illegally copied, altered, or disseminated. In recent years, there have been many research topics on digital watermarking (Hsu & Wu, 1999; Lu & Liao, 2003; Li & Cox, 2007).

Colors in a binary image have a high contrast, therefore color changes are easily perceived by the human eye. Consequently, it is more difficult to hide data in 2-color images than gray-level images or true-color images. Wu & Lee (1998) proposed a block-based embedding method which embeds one bit in a block by, at most, changing one pixel in the block. Pan, Chen and Tseng (2000) proposed an improved method by utilizing a weight matrix to embed $\lfloor \log_2(m \cdot n + 1) \rfloor$ bits in a $m \times n$ block by changing only two bits. They (Tseng & Pan, 2002) also proposed a corrective technique to filter out unsuitable runs to improve image quality. Wu & Liu (2004) hid one bit in each image block via the enforcement of an odd–even relationship of black pixels by manipulating flappable pixels. A shuffling technique was used to achieve a large amount of data embedding in a binary image without

* Corresponding author. E-mail: dcwu@ccms.nkfust.edu.tw

causing noticeable artifacts. This paper will propose a novel authentication technique for binary document images, which can embed trademarks or messages about products into images without causing noticeable differences. The method can be used to ensure the identification of intellectual property rights of digitalized documents. This paper will also propose a technique which appropriately verifies whether a binary image has been tampered with, or not. The remainder of this paper is organized as follows. In section 2, the proposed data hiding method is presented and the process for extracting the embedded data is described. In Section 3, the proposed authentication techniques are illustrated. Several experimental results are shown in Section 4. Finally, concluding remarks are stated in Section 5.

2. DATA EMBEDDING BASED ON ADJUSTING LENGTHS OF RUNS

The RLE (Run Length Encoding) (Sayood, 2000) technique is one of the compression techniques that are commonly applied to binary images in fax transmissions. In the process of RLE, a binary image is scanned in a raster order. Runs are composed of continuous pixels with same color, i.e., black runs are composed of continuous black pixels and white ones are composed of continuous white pixels. The essential parameters of each run include color and length (the number of pixels). In this paper, a data hiding technique which adjusts the lengths of runs in run pairs within a binary image will be proposed. Each run-pair is composed of two adjacent runs. The run-pair may be composed by a black run followed by a white run or a white run followed by a black run. In Figure 1, we illustrate how to combine two adjacent runs into a run-pair from left to right.

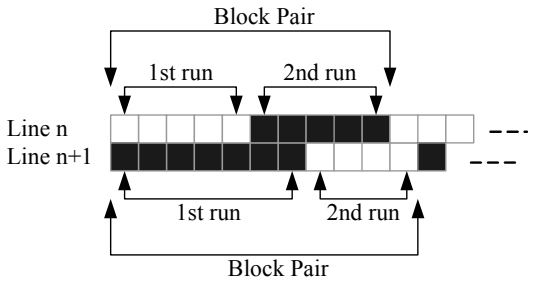


Figure 1. Run-pairs composed with RLE.

The locations where white runs adjoin black runs can be view as coarse boundaries within a binary image. If we make slight modifications to these locations, the changes are not so easily perceived. In this method, each run-pair can be used for embedding one bit of data by adjusting the lengths of the black run and

the white run. Assume L_B is the run-length of the black run in a given run-pair P, and L_W is the run-length of the white run of P. This technique uses the odd/even characteristic of the run-length of the black or white run in a given run-pair to represent the embedded bit. The choice of white run or black run is random and varies from run-pair to run-pair. At most, one pixel of the black and white run will be changed but the total number of pixels of the run-pair is not changed. This method only generates noise-like effects at the border between the white run and the black run within a run-pair. In this method, the new run-length of the black run after adjustment is L'_B, and its range will be in [L_B-1, L_B+1]. Let the new length of the white run be L'_w, its range will also be adjusted in [L_W-1, L_W+1] to match the condition $L_B + L_W = L'_B + L'_w$, i.e. the total length of a run-pair is keep unchanged. This technique uses the odd/even characteristic of L'_B or L'_w to represent the embedded data. For example, if L'_B or L'_w is even, the embedded data is 0. Otherwise, the embedded data is 1. Therefore, we can extract the embedded data only by calculating the number of black or white pixels in a run-pair. If the number of the pixels in the black or white run is even, the extracted data is 0. Otherwise, the extracted data is 1.

A run with a small length may have immense variation during the adjustment. For example, if the number of pixels in a run is originally 2, it may vary from 1 to 3 after the adjustment. As the result of a change in one half of the length, it might be easy to perceive a difference in the image and the quality of the image might be affected. Therefore, the method uses a controlled threshold T ($T > 0$) in the embedding process to filter out the runs with too small a length. If a run-pair does not meet the condition

$$L_B > L_W \geq T \text{ or } L_W > L_B \geq T \text{ or } (L_B = L_W \text{ and } L_B > T) \tag{1}$$

the run-pair will not be used for embedding data and so will not be modified. This method scans images in a raster scan order to find all run-pairs which meet the condition. Each run-pair which meets the condition will embedded one bit of information. Assume we want to embed a bit d in the black run within a given run-pair. The method of adjustment can be expressed as:

$$\begin{cases} L'_B = L_B + \text{sgn}(L_W - L_B) * \left| (L_B \bmod 2) - d \right|; \\ L'_W = L_W - \text{sgn}(L_W - L_B) * \left| (L_B \bmod 2) - d \right|, \end{cases} \quad \text{where } \text{sgn}(x) = \begin{cases} 1 & \text{if } x \geq 0; \\ -1 & \text{if } x < 0. \end{cases} \tag{2}$$

It never reduces the length of the smaller run, and the condition still holds after the adjustment.

In the process of extracting data, each run-pair P will be obtained as in the embedding steps. The length of the black run L''_B and that of the white run L''_W in P are then calculated. We can determine whether the run-pair has embedded data previously by checking L''_B and L''_W. Assume the extracted data is d' and was embedded in the black run previously. The condition for checking the existence of embedding data and the extracting method can be expressed as

$$\begin{aligned} &if\ (L''_B > L''_W \geq T\ or\ L''_W > L''_B \geq T)\ or\ (L''_B = L''_W\ and\ L''_B > T) \\ &\quad d' = L''_B \bmod 2. \end{aligned} \tag{3}$$

3. AUTHENTICATION TECHNIQUES OF BINARY DIGITAL IMAGE WITH BCH CODES

A method of authenticating binary images will be proposed. First, we transform embedding data into error correction codes by a coding rule. Then each bit of the codes is embedded in one run-pair of an image. In the process of authenticating, the extracted data is verified whether it satisfies the corresponding error correction coding rules or not. If it does not satisfy the rules, the run-pair will be treated as an altered region.

3.1 BCH Coding Method

The error correction coding method used in this paper is the BCH (Bose Chaudhuri-Hocquenghem) code (Lin & Costello, 1983). The algorithm is commonly applied to CCIR 584-1. It is a kind of cyclic code which is capable of random error correction. The BCH method used in this paper codes each 4-bit data to a 7-bit data stream. Therefore, we can call it BCH (7, 4). Assume the authenticating data *a* is coded to *c* by using BCH (7, 4). When *c* has a 1-bit error we can also convert it back to original *a*. When *c* has a 2-bit error we can not restore it but can detect the existence of the error. This method provides a method that is not only capable of authentication but also can restore tampered authenticating data to its original from. A cyclic code possesses a good mathematical structure which includes the mechanism of automatic synchronization. This mechanism is provided by a linear feedback shift register. If data is not correct during decoding, it can rapidly return to the state of regular decoding from the error state. This property is fairly robust for extracting data from a data stream that contains errors. We can achieve the purpose of authenticating images with this advantage.

3.2 The Authenticating Method by Adjusting Length of Runs

This paper proposes a method which mainly authenticates a binary image's authenticity. It includes two procedures: the embedding authenticating data process and the examining authenticating data process. The authenticating data can be secret words or copyright signals. In this paper the original authenticating data is a logo image. It is coded with BCH (7, 4) firstly and then each bit of the coded bits is embedded in a run-pair of an image by the method mentioned above. When examining the authenticating data, we can not only determine the integrity of the extracted data with BCH coding structure itself but can also observe the extracted images with the human eye to prove the copyright.

Before embedding the original authenticating data, we first code the data to error correction form. Each 4-bit data d is encoded to 7-bit error-corrected bit stream e. The method encodes each four bits of the original authenticating data, $d_1d_2d_3d_4$ to 7-bit error-corrected code $e_1e_2e_3e_4e_5e_6e_7$. Table 1 shows parts of the possible 4-bit data which were transformed into the corresponding 7-bit error-corrected code.

Table 1. *Parts of BCH (7,4) coding reference table*

Original data	Encoded data
0000	0000000
0001	0001011
0010	0010110
…	…
1101	1101001
1110	1110100
1111	1111111

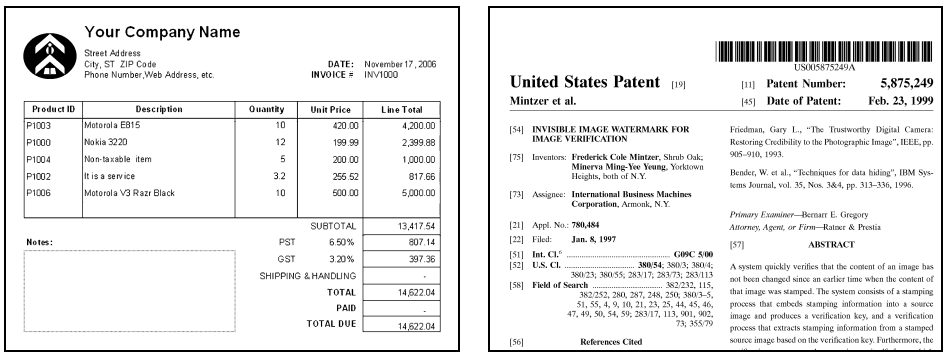
For example, if the original authenticating data is 110001100101. First, we divide it into three parts of four bits each. These three parts in order are 1100, 0110, and 0101. By using Table 1, we can obtain the corresponding error correction data stream 1100010, 0110001, and 0101100, respectively. Then, we use the method proposed in the previous section to embed one bit in each run-pair of an image. The authenticating data will be used repeatedly to embed in a whole image in raster order.

The extracting procedure is achieved by using Equation (3), which was mentioned in the previous section. The extracted data are then examined. Every 7-bit bit-stream is compared with each code word in Table 1. The comparisons determine whether the bit-stream conforms to the rules of BCH (7, 4) coding. If it matches, the correspondingly 4-bit authenticating data can be returned. Otherwise, we view the first bit of this 7-bit data as error data, discard it and label the run as an error run. Next, the remaining six bits of the bit-stream are shifted to the left and the next extracted bit appended to their end to form a new 7-bit bit-stream. The above procedure is repeated until all runs of an image are processed.

4. EXPERIMENTAL RESULTS

Two 2000 x 1500 binary images “Invoice” and “Patent” are shown in Figure 2 as the cover images. A 78 x 28 binary logo image “NKFUST” (Figure 3) acts as the authenticating data in our experiments and will be used repeatedly in the embedding steps. Figure 4 shows the embedding capacity vs. the controlled threshold T which filters out the runs with too small a length in the embedding process. In Figure 5, the magnified cover image “Invoice,” the resulting images after embedding authenticating data in “Invoice” by using two successive threshold values 4 and 5, and the differences between the cover image and the resulting images are shown.

Figure 6 shows the magnified resulting images after embedding authenticating data by setting threshold T to 2, and the authenticating data extracted from the images of the embedding results. The magnified altered images are shown in Figure 7. Some numerals and the company name are tempered. The resulting images of authentication from the altered images and the authenticating data which are extracted from the altered images are shown in Figure 8.



Your Company Name

Street Address
City, ST ZIP Code
Phone Number,Web Address, etc.

DATE: November 17, 2006
INVOICE # INV1000

Product ID	Description	Quantity	Unit Price	Line Total
P1003	Motorola E815	10	420.00	4,200.00
P1000	Nokia 3220	12	199.99	2,399.88
P1004	Non-taxable item	5	200.00	1,000.00
P1002	It is a service	3.2	255.52	817.66
P1006	Motorola V3 Razr Black	10	500.00	5,000.00

	SUBTOTAL	13,417.54
PST	6.50%	807.14
GST	3.20%	397.36
SHIPPING & HANDLING		-
	TOTAL	14,622.04
	PAID	-
	TOTAL DUE	14,622.04

Notes:

US005875249A

United States Patent [19]
Mintzer et al.

[11] **Patent Number: 5,875,249**
[45] **Date of Patent: Feb. 23, 1999**

[54] **INVISIBLE IMAGE WATERMARK FOR IMAGE VERIFICATION**

[75] Inventors: **Frederick Cole Mintzer**, Shrub Oak; **Minerva Ming-Yee Yeung**, Yorktown Heights, both of N.Y.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **780,484**

[22] Filed: **Jan. 8, 1997**

[51] **Int. Cl.**[6] **G09C 5/00**

[52] **U.S. Cl.** **380/54**; 380/3; 380/4; 380/23; 380/55; 283/17; 283/73; 283/113

[58] **Field of Search** 382/232, 115, 382/252, 280, 287, 248, 250; 380/3–5, 51, 55, 4, 9, 10, 21, 23, 25, 44, 45, 46, 47, 49, 50, 54, 59; 283/17, 113, 901, 902, 73; 355/79

[56] **References Cited**

Friedman, Gary L., "The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image", IEEE, pp. 905–910, 1993.

Bender, W. et al., "Techniques for data hiding", IBM Systems Journal, vol. 35, Nos. 3&4, pp. 313–336, 1996.

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—Ratner & Prestia

[57] **ABSTRACT**

A system quickly verifies that the content of an image has not been changed since an earlier time when the content of that image was stamped. The system consists of a stamping process that embeds stamping information into a source image and produces a verification key, and a verification process that extracts stamping information from a stamped source image based on the verification key. Furthermore, the

(a) (b)

Figure 2. Cover Images. (a) Invoice. (b) Patent.

Figure 3. The authenticating image data "NKFUST."

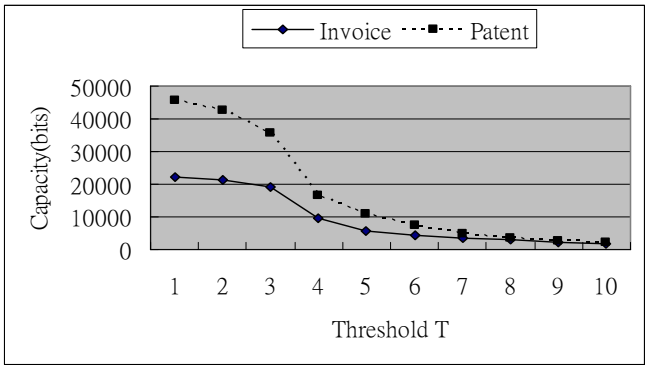


Figure 4. Embedding capacity vs. controlled thresholds.

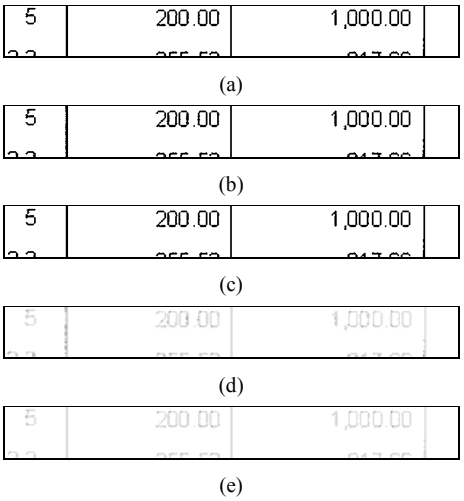


Figure 5. Magnified "Invoice." (a) Original cover image. (b) The resulting image after embedding authenticating data in Figure 5(a) by setting the control threshold to 4. (c) The resulting image after embedding authenticating data in Figure 5(a) by setting the control threshold to 5. (d) The difference between Figure 5(a) and Figure 5(b) (dark pixels). (e) The difference between Figure 5(a) and Figure 5(c) (dark pixels).

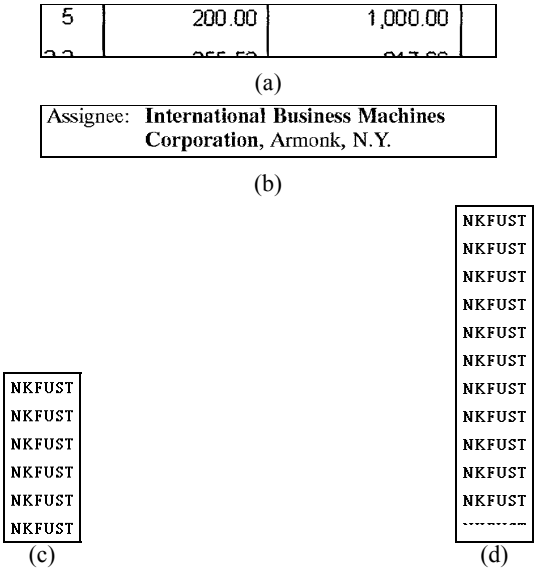
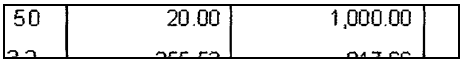


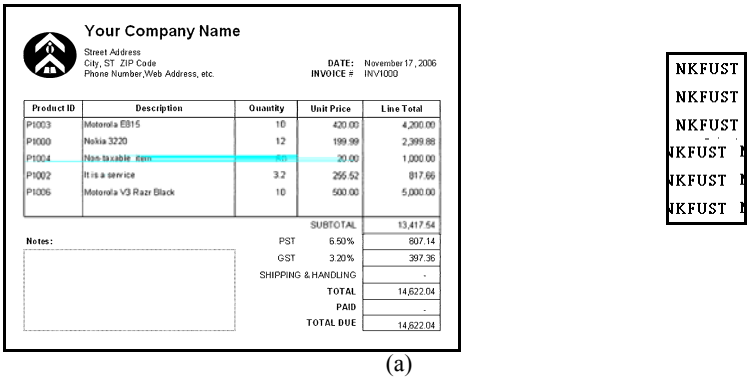
Figure 6. The magnified resulting images by setting threshold T to 2, and the authenticating data which was extracted from the resulting images. (a) Invoice. (b) Patent. (c) Authenticating data of Figure 6(a). (d) Authenticating data of Figure 6(b).



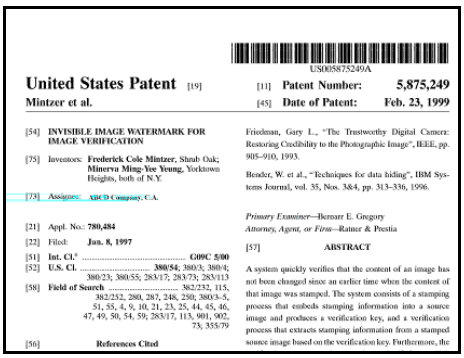
(a)

(b)

Figure 7. The magnified altered images. (a) Invoice. (b) Patent.



(a)



(b)

Figure 8. The resulting images of authentication and the extracted authenticating data from the altered images of Figure 6. (a) Invoice. (b) Patent.

5. CONCLUSIONS

In this paper, we have proposed a novel data hiding technique for binary images. We introduced a controlled threshold for considerations of human perception. We proposed a technique which authenticates the truthfulness of a

binary image. This technique can be used to protect the intellectual property rights of electronic documents in binary image form and check whether the image has been altered or not. In addition, the original image is not needed when we extract data or authenticate the truthfulness.

REFERENCES

Hsu, C. T. & Wu, J. L. (1999). Hidden digital watermarks in images. *IEEE Transactions on Image Processing*, *31*(2), 26-34.

Li, Q., & Cox, I. J. (2007). Using Perceptual Models to Improve Fidelity and Provide Resistance to Volumetric Scaling for Quantization Index Modulation Watermarking. *IEEE Transactions on Information Forensics and Security*, *2*(2), 127-139.

Lu, C. S., & Liao, H. Y. M. (2003). Structural digital signature for image authentication: an incidental distortion resistant scheme. *IEEE Transactions on Multimedia*, *5*(2), 131-173.

Lin, S., & Costello, D. J. (1983). *Error Control Coding*. Englewood Cliffs, New Jersey, USA: Prentice-Hall.

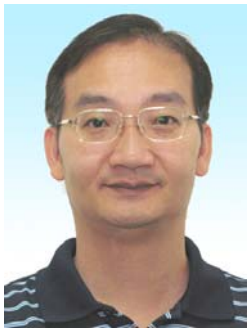
Pan, H. K., Chen, Y. Y., & Tseng, Y. C. (2000). A Secure Data Hiding Scheme for Two-Color Images. *Proceedings of 2000 IEEE Symposium on Computers and Communications*, 750-755. Antibes, France.

Sayood, K. (2000). *Introduction to Data Compression*. San Francisco, California, USA: Morgan Kaufmann.

Tseng, Y. C., & Pan, H. K. (2002). Data Hiding in 2-Color Images. *IEEE Transactions on Computer*, *51*(7), 873-879.

Wu, M., & Liu, B. (2004). Data Hiding in Binary Image for Authentication and Annotation. *IEEE Transactions on Multimedia*, *6*(4), 528-538.

Wu, M. Y., & Lee, J. H. (1998). A Novel Data Embedding Method for Two-Color Facsimile Images. *Proceedings of International Symposium on Multimedia Information Processing*. Chung-Li, Taiwan, ROC.



Da-Chun Wu was born in Taiwan, Republic of China in 1959. He received a B. S. degree from the Department of Computer Science from Tamkang University, Taiwan in 1983, an M. S. degree from the Institute of Information Engineering from Tamkang University in 1985, and a Ph. D. in Computer Science from National Chiao Tung University in Taiwan in 1999. He has devoted to teaching since 1987, started as an instructor in Ming Chuan University, Taiwan. He is currently an Associate Professor in the Department of Computer and Communication Engineering, National

Kaohsiung First University of Science and Technology in Taiwan. His major research interests include data hiding, watermarking, digital rights management, multimedia security and forensics.

Ming-Kao Hsu received an M. S. degree from the Department of Information Management at Ming Chuan University, Taipei, Taiwan in 2002. Mr. Hsu has served at EBN Technology Corp. in Taipei, Taiwan as a director of the System Information Business Department since July 2005. His major interests include data hiding and e-commerce.