Bit Priority-Based Biometric Watermarking

Tuan Hoang, Dat Tran and Dharmendra Sharma
Faculty of Information Sciences and Engineering
University of Canberra
Canberra, Australia

***Abstract*— In remote biometric authentication systems, raw biometric data stored in centralized databases or being transferred in communication channels are normally encrypted for security purposes. However, encryption does not provide security once the data are decrypted. Biometric watermarking can overcome this problem. The decrypted biometric data are still embedded in an image container and are only retrieved if a secret key is provided. It has been observed that retrieval error is very high if the embedded biometric data are numeric. We proposed a new method based on amplitude modulation and bit priority to embed high priority bits at good positions to reduce the retrieval error when they are converted to numeric data. Experimental results show a significant error reduction for the proposed method.**

***Keywords:* biometric watermark, amplitude modulation, bit priority**

I. INTRODUCTION

User authentication (human-by-machine authentication) is the process of verifying the identity of a user: is this person really who he/she claims to be? User authentication has become more complicated and difficult with the onset of the computer age. User authentication systems can be categorized into three main types: knowledge-based authentication (what you know, e.g., passwords and PIN), Object-based authentication (what you have, e.g., physical keys), and ID-based authentication (who you are, e.g., biometric ID such as voiceprint and signature, and physical ID such as passport and credit card) [1].

Passwords are excellent authenticators, but they can be stolen if recorded or guessed. Physical keys or other physical devices have similar advantages and disadvantages. Biometrics are useful to establish authenticity and for non-repudiation of a transaction, wherein a user cannot reject or disclaim having participated in a transaction. There has been a significant surge in the use of biometrics for user authentication in recent years because of the threat of terrorism and the Web-enabled world [2]. However, biometrics can be copied or counterfeited, so they cannot ensure authenticity or offer a guaranteed defense against repudiation. Different types of authenticators should be combined to enhance security and performance [3].

In order to promote the wide spread utilization of biometric techniques, an increased security of the biometric data is necessary. Techniques based on steganography can be suitable for transferring critical biometric information from a client to a server and reduce the chances of illegal modification of the biometric data. Encryption can be applied to biometric models or templates after enrollment and will be decrypted during authentication. The encrypted templates are secured since they can be decrypted with a secret key. However, the problem is that encryption does not provide security once the data are decrypted. In order to enhance security for user authentication systems, biometric watermarking can be involved. Biometric data are still embedded into the host data which have been decrypted and will only be retrieved if a secret key is provided, therefore biometric watermarking can provide security after decryption.

Biometric watermark is an invisible digital watermark that is embedded in a primary image and is imperceptible to the human eye but easily recoverable by a computer program. The locations that the biometric data embedded in the primary image are determined by a secret key to prevent possible pirates from easily removing the biometric data. The invisible watermark should not be easily removed by some multimedia signal processing techniques and should be retrieved from an altered image. The invisible watermarking techniques need to be utilized in conjunction with encryption, site security and a proper legal framework [4].

A number of watermarking algorithms have been developed. In the discrete cosine transform (DCT) domain visible watermarking algorithm [5], the primary image is divided into different blocks which are classified by perceptual methods and whose DCT coefficients are modified. In the amplitude modulation method for color images [4, 6], the blue channel is used to embed information which will be retrieved in the decoding phase using the neighbor approximation technique. This method is used for invisible watermarking.

In biometric watermarking, biometrics such as fingerprint, voice, and iris data will be converted to a bit sequence and then be embedded to a primary image. Consider the following example, where the bit sequence to be embedded is 0010 0001 and two watermarking techniques are used. After encoding and decoding by the first watermarking technique, the retrieved bit sequence is 0100 0001 with an error on the second and third bits. Using the second technique, the retrieved bit sequence is 0010 0010 with an error on the last two bits. If the number of wrong bits is regarded as error, we can see that the two watermarking techniques provide the same error (two wrong bits). However, if these embedded bit sequences are converted to unsigned 8-bit integers, and the difference between two integers is considered as an error, then the first watermarking method provides higher error than the second one does (the above sequences 0010 0001, 0100 0001,

1-4244-2426-9/08/$20.00 ©2008 IEEE

and 0010 0010 are corresponding to 33, 65, and 34, respectively.)

From the above example, we can see that bits in different positions in a bit sequence will have different priorities for numerical information. The current amplitude modulation method for color images [4, 6] does not take into account this bit priority problem. In this paper, we propose a new digital watermarking method based on amplitude modulation and priority level of bits for biometrics watermarking. We propose that high priority bits should be embedded at good positions in the primary image to achieve low error rate when they are retrieved. We performed a number of experiments to evaluate the proposed method. Experimental results show a significant error reduction for the proposed method comparing with the current digital watermarking method based on amplitude modulation.

The paper is organized as follows. Section 1 reviews watermarking methods and introduce the problem of embedding numeric values. Section 2 summarizes the current digital watermarking method based on amplitude modulation. Section 3 presents the proposed method. Section 4 presents experiments to evaluate the proposed method and to compare with the current method. Finally, we conclude in Section 5.

II. Amplitude Modulation-Based Digital Watermarking

Let $I(m, n)$ be a color image of size $m \times n$. If the RGB color system is used, then $I(m, n) = \{R(m, n),\ G(m, n),\ B(m, n)\}$. Let $S = (s_1, s_2, \dots, s_k)$ be the bit sequence of size k to be embedded in the image I, and $I'(m, n) = \{R'(m, n),\ G'(m, n),\ B'(m, n)\}$ be the image obtained after embedding S into the image I. The amplitude modulation-based digital watermarking method embeds bits by modifying the blue channel in the color image I. Each bit in S will be embedded d times at different positions in the image I. The blue channel is chosen because human eyes are least sensitive to it comparing with the red or the green ones. Therefore

$$I'(m, n) = \{R(m, n),\ G(m, n),\ B'(m, n)\} \tag{1}$$

Encoding Process: A pseudo-random position sequence $p = (p_1, p_2, \dots, p_{d\times k})$, where $p_{(t-1)*d+h} = (i, j)$ representing row and column indices at which bit s_t is embedded the h-th time, is chosen to embed the bit sequence S. The sequence p is randomly generated by a pseudo-random generator based on a given secret key K, which is used as a seed to the generator. The t-th bit in the bit sequence S will be embedded in the blue channel of the image I at d positions $p_{(t-1)*d+h}$, …, p_{t*d} according to the following equation

$$B'_{i,j} = B_{i,j} + s_t q L_{i,j} \tag{2}$$

where $L_{i,j}$ is luminance at the position (i, j) and can be calculated as follows

$$L_{i,j} = 0.299R_{i,j} + 0.587G_{i,j} + 0.144B_{i,j} \tag{3}$$

and q is a tradeoff between robustness and invisibility.

Decoding Process: Using the same secret key K as used in the encoding process, the position sequence $p_{(t-1)*d+h}$, …, p_{t*d} is regenerated by the pseudo-random generator. If the original value $B_{i,j}$ is given, we can determine the value of the embedded bit s_t by checking the difference δ between the retrieved value and the original value of the pixel being taken $\delta_{i,j} = B'_{i,j} - B_{i,j}$. The sign of the difference determines the value of the embedded bit. However, unfortunately, we do not have $B_{i,j}$ at decoding process, so we try to estimate it, denoted as $B''_{i,j}$, by using linear combination approximation of neighbor pixels. If the 8 neighbor pixels of the pixel (i, j) are considered, the value $B''_{i,j}$ is calculated as follows

$$B''_{i,j} = \frac{1}{8}\left(\sum_{di=-1}^{1}\sum_{dj=-1}^{1} B'_{i+di,\,j+dj} - B'_{i,j}\right) \tag{4}$$

and the approximated difference now is calculated as

$$\delta_{i,j} = B'_{i,j} - B''_{i,j} \tag{5}$$

The single bit s_t is embedded at d positions $p_{(t-1)*d+1}$, …, p_{t*d}, therefore we use the arithmetic average method to calculate the value δ_t

$$\overline{\delta}_t = \frac{1}{d}\sum_{t=1}^{d}(B'_{p(t-1)d+i} - B''_{p(t-1)*d+i}) \tag{6}$$

The sign of $\overline{\delta}_t$ is the estimated bit s'_t of the embedded bit s_t. The larger the absolute value of $\overline{\delta}_t$ is, the higher confidence of the estimation is.

$$s'_t = sign(\overline{\delta}_t) \tag{7}$$

III. Amplitude Modulation and Bit Priority-Based Digital Watermarking

Let $I(m, n)$ be a color image of size $m \times n$. If the RGB color system is used, then $I(m, n) = \{R(m, n),\ G(m, n),\ B(m, n)\}$. Let $S = (s_1, s_2, \dots, s_k)$ be the bit sequence of size k to be embedded in the image I, and $I'(m, n) = \{R'(m, n),\ G'(m, n),\ B'(m, n)\}$ be the image obtained after embedding S into the image I. Let $Pri(s)$ be a bit priority function. The priority level of bit s_t is high if the value of $Pri(s_t)$ is large.

Encoding Process: Similar to the amplitude modulation-based watermarking method, a pseudo-random position sequence $p = (p_1, p_2, \dots, p_{d\times k})$, where $p_{(t-1)*d+h} = (i, j)$ is the position chosen to embed bit the h-th time. However, in our proposed method, we embed high priority bit at good positions so that we can retrieve that bit with a low error rate. It can be seen that if the difference between $B''_{i,j}$ and $B'_{i,j}$ is low, then the retrieved bit is good. Therefore we propose to use the Pewitt operator which calculates the gradient in a two-dimensional image to determine good positions. The lower the gradient at a position is, the better this position is.

–1	–1	–1
0	0	0
1	1	1

–1	0	1
–1	0	1
–1	0	1

Figure 1. The Pewitt operators *Px* for *Gx* (left) and *Py* for *Gy* (right).

The values *Gx* and *Gy* are calculated as follows

$$Gx_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,j+dj} Px_{di+2,dj+2} \right)$$

$$Gy_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} B_{i+di,j+dj} Py_{di+2,dj+2} \right)$$

$$G_{i,j} = \sqrt{Gx_{i,j}^2 + Gy_{i,j}^2} \tag{8}$$

If the difference between the pixels in a small neighbor block of the pixel is not significant, we can replace the blue channel with another channel for gradient calculation. In this paper, we choose the red channel.

$$Gx_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R_{i+di,j+dj} Px_{di+2,dj+2} \right)$$

$$Gy_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R_{i+di,j+dj} Py_{di+2,dj+2} \right)$$

$$G_{i,j} = \sqrt{Gx_{i,j}^2 + Gy_{i,j}^2} \tag{9}$$

The position sequence *p* will be rearranged according to the increase of gradient. The bits whose priority level is from high to low will be embedded sequentially.

Decoding Process: Based on the secret key *K*, the sequence *p* is regenerated as shown in the encoding process. However, the gradient at each position needs to be calculated and depending on these gradient values, the sequence *p* will be rearranged.

$$Gx'_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R'_{i+di,j+dj} \, Px_{di+2,dj+2} \right)$$

$$Gy'_{i,j} = \left(\sum_{di=-1}^{1} \sum_{dj=-1}^{1} R'_{i+di,j+dj} \, Py_{di+2,dj+2} \right)$$

$$G'_{i,j} = \sqrt{Gx'^2_{i,j} + Gy'^2_{i,j}} \tag{10}$$

As $R = R'$, we have $G'_{i,j} = G_{i,j}$ at all position (i, j) calculated. Therefore the sequence *p* after rearranging is the same in both the encoder and decoder processes. Further steps are conducted in the original method as shown in (4), (5), (6) and (7) to retrieve the embedded information.

IV. Experimental Results

We evaluated the proposed method on a database that contains integers to be embedded in a color image of Mona Lisa in JPEG format with size 384 × 300, which totally has 115200 pixels. The bit priority function for the *i*-th bit in the bit sequence *S* representing an integer will be of the form $Pri(s_i) = i$. We represent these integers as sequences of 4 bytes, i.e. 32 bits, therefore *i* will be from 1 to 32.

Figure 2. The color image of Mona Lisa used.

A 32-bit integer was selected to generate several arrays of different lengths. For example such an array of integer 100 would be 100, 100, …, 100. The 32-bit integer was repeated in those arrays *h* times, where $h \in \{100, 150, 200, \ldots, 400\}$. Therefore the length of corresponding bit sequences to be embedded in the Mona Lisa image was from 3200 to 12800 bits. Each bit was embedded at different *d* positions, where $d \in \{5, 10, 15\}$. Table 1 shows the ratios of embedded pixels over total pixels in the primary image for each experiment. Some of the ratios are greater than 100% because we also wanted to check if embedding a bit at several positions would enhance the quality of retrieval even the image size was small. As other experiments in amplitude modulation-based watermarking, the tradeoff *q* was set to 0.1.

TABLE I. Ratios (%) of embedded pixels over total pixels for each experiment

Number of integers	**Number of positions for embedding**		
	5	**10**	**15**
100	13.89%	27.78%	41.67%
150	20.83%	41.67%	62.50%
200	27.78%	55.56%	83.33%
250	34.72%	69.44%	104.17%
300	41.67%	83.33%	125.00%
350	48.61%	97.22%	145.83%
400	55.56%	111.11%	166.67%

It is seen from Figure 3 that the error obtained from the proposed method (shortened as priority) is very low but the error from the current amplitude modulation-based watermarking method (shortened as non-priority) is increasing when the array sizes increase.

Since the error in each experiment was dependent on the sequence of random positions, we embedded the array 5 times in 5 different random sequences of positions in the image and then calculated the average error. The error is calculated as follows

$$AbsoluteError = \sum \left| RA_i - OA_i \right| \tag{11}$$

where RA is the retrieved array and OA is the original array (embedded array), respectively, and *h* is the number of occurrences of the integer in the integer array.

It can be seen from Figure 3 that the proposed priority method provides very low errors. The errors from the proposed method is not significantly different from the current method for the arrays whose sizes are less than 200, but it tends to be much better when the array sizes increase.

TABLE II. ERRORS FOR THE PROPOSED PRIORITY METHOD

Number of integers	Number of positions for embedding each integer		
	5	10	15
100	0.00067	0.00000	0.00000
150	0.00005	0.00000	0.00000
200	0.00131	0.00000	0.00000
250	0.00054	0.00000	0.00103
300	0.00003	0.00000	0.00086
350	0.00093	0.00241	0.18821
400	0.00031	0.00000	0.02239

Table II shows average errors for the proposed priority method. Comparing with Table I, it is seen that the error is not significant if the ratio of embedded pixels and total pixels in the primary image is less than 100%. If the ratio is greater than 100%, the average error is unpredictable because bits are embedded in the same positions resulting to information loss. A larger size image should be used to avoid this problem. Moreover, if bits are embedded 10 or 15 times, the average error is nearly 0.

Table 3 shows average errors for the current non-priority method to compare with the errors in the proposed priority method. Figure 3 presents the error values in Table II and Table III in 3 diagrams. The numbers of wrong bits in both the methods are not different but the positions of wrong bits are different so integers obtained from converting retrieved bit sequences will be significantly different as seen in Table III.

TABLE III. ERRORS FOR THE CURRENT NON-PRIORITY METHOD

Number of integers	Number of positions for embedding each integer		
	5	10	15
100	8.32	0.02	0.01
150	6.29	5.74	8.21
200	23.88	23.74	59.16
250	32.71	65.97	175.58
300	80.89	141.00	396.13
350	110.37	250.94	598.53
400	163.33	377.96	939.12

V. CONCLUSION

We have proposed a new biometric watermarking method based on amplitude modulation and bit priority level. While inheriting security characteristics such as anti-attack from the original method, the proposed method is very useful in biometrics applications, where numeric feature or model values of fingerprint, voice, or iris need to be embedded to an image. The proposed method has been evaluated and compared with the current digital watermarking method based on amplitude modulation. Since the errors are nearly zero in the proposed method, no changes have been affected to biometric authentication systems.

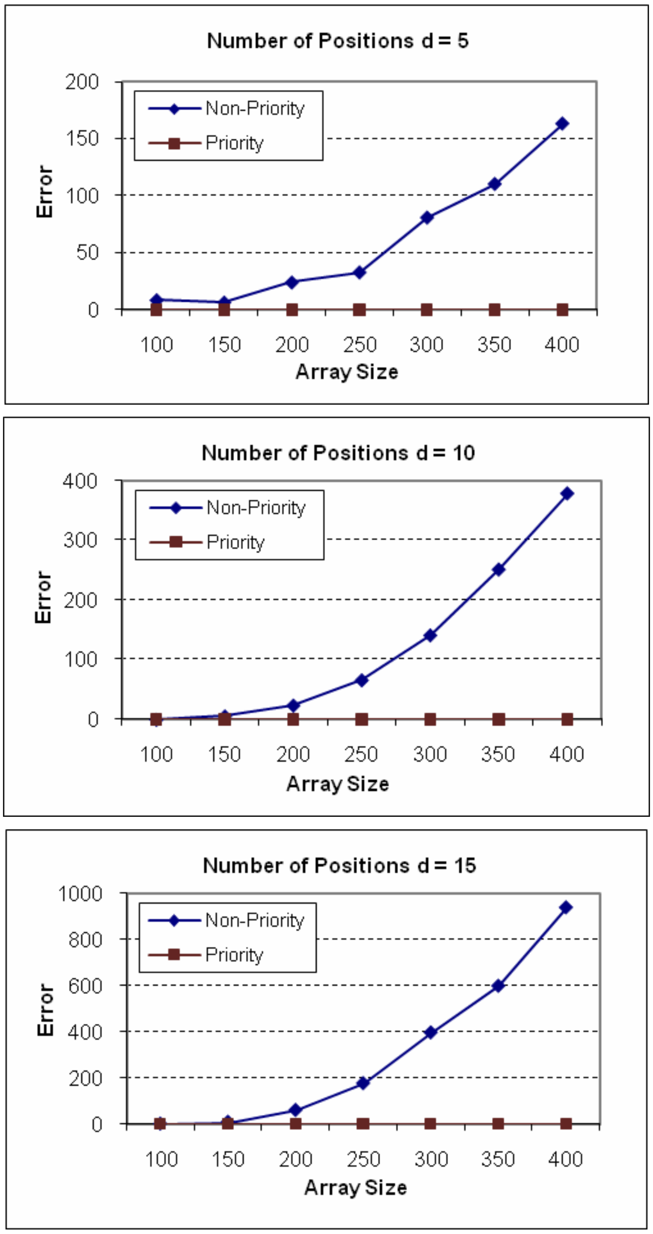

Figure 3. Errors for the original (non-priority) method and the proposed (priority) method.

REFERENCES

[1] L. O'Gorman. Comparing Passwords, Tokens, and Biometrics for User Authentication. Proceedings of the IEEE, vol. 91, no. 12, pp. 2021-2040, 2003

[2] R.M. Bolle, J. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior. Biometrics 101. IBM Research Report, IBM T. J. Hawthorne, New York, 2002

[3] A.M. Namboodiri and A.K. Jain, "On-line Handwritten Script Recognition" IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.26, no. 1, pp. 124-130, 2004

[4] M. Kutter, F. Jordan, and F. Bossen, "Digital Watermarking of Color Images Using Amplitude Modulation", Journal of Electronic Imaging, vol. 7, no. 2, pp. 326 – 332, 1998

[5] S.P. Mohanty, "Digital Watermarking: A Tutorial Review" Report, Dept. of Electrical Engineering, Indian Institute of Science, Bangalore, India, 1999

[6] T. Amornraksa and K. Janthawongwilai, "Enhanced images watermarking based on amplitude modulation", Image and Vision Computing, vol. 24, no. 2, pp. 111 – 119, 2006

[7] Kankanhalli, M.S., Rajmohan, Ramakrishnan, K.R.: Adaptive visible watermarking of images, IEEE Multimedia Computing and Systems, vol. 1, pp. 568 – 573, 1999

[8] H. Yongjian, S. Kwong, "An image fusion based visible watermarking algorithm", in Proceedings of the 2003 International Symposium on Circuits and Systems, vol. 3, pp. 794 – 797, 2003

[9] S.P. Mohanty, K.R. Ramakrishnan, M.S. Kankanhalli, "A DCT domain visible watermarking technique for images", in Proceedings of Multimedia and Expo IEEE International Conference, vol. 2, pp. 1029 – 1032, 2000

[10] I.J. Cox et al., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. on Image Processing, vol. 6, no. 12, pp. 1673 – 1687, 1997

[11] R. G. Wolfgang, and E. J. Delp, "A Watermark for Digital Images", Proc. IEEE Intl. Conf. on Image Processing, ICIP-96, vol. 3, pp. 219 – 222, 1996

[12] W. Zhu et al., "Multiresolution Watermarking for Images and Video: A Unified Approach", Proc. IEEE International Conf. on Image Processing, vol. 1, pp. 465 – 468, 1998

[13] P. Loo, N. Kingsbury, "Watermark detection based on the properties of error control codes", IEE Proceedings Vision, Image and Signal Processing, vol. 150, no. 2, pp. 115 – 121, 2003

[14] C.-S. Lu, C.-Y. Hsu, "Near-Optimal Watermark Estimation and Its Countermeasure: Antidisclosure Watermark for Multiple Watermark Embedding", IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 4, 454 – 467, 2007

[15] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers, J.K. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks", IEEE Communications Magazine, vol. 39, no. 8, pp. 118 – 126, 2001

[16] P.H.W. Wong, O.C. Au, Y.M. Yeung, "Novel blind multiple watermarking technique for images", vol. 13, no. 8, pp. 813 – 830, 2003

[17] E.T. Lin, E.J. Delp, "Temporal synchronization in video watermarking", IEEE Transactions on Signal Processing, vol. 52, no. 10, pp. 3007 – 3022, 2004

[18] 15. HyeRan L.; KyungHyun R.: Reversible Data Embedding for Tamper-Proof Watermarks, ICICIC '06, International Conference on Innovative Computing, Information and Control, 3, 487 – 490 ,2006)

[19] H. Yongjian, S. Kwong, H. Jiwu, "Using invisible watermarks to protect visibly watermarked images", Proceedings of the 2004 International Symposium on Circuits and Systems, vol. 5, pp. 584 – 587, 2004

[20] C. Ee-Chien, M. Orchard, "Geometric properties of watermarking schemes", International Conference on Image Processing, vol. 3, pp. 714 – 717, 2000

[21] Z. Liu, A. Inoue, "Audio watermarking techniques using sinusoidal patterns based on pseudorandom sequences", IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 801 – 812, 2003