PAPER *Special Section on Spread Spectrum Techniques and Applications*

A Novel Individual Identification System Using a Watermarking Method Based on the Parallel Combinatorial Spread Spectrum Scheme

Masaaki FUJIYOSHI[†], *Student Member and* **Takaaki HASEGAWA**[†], *Regular Member*

SUMMARY This paper describes a new individual identification system employing a novel application of the PC/SS scheme. Since the proposed system requires no magnetic information, it is robust to various changes in environment. Moreover, it is applicable to contemporary identification systems as an officer identifies one's face with the card's portrait at immigration. In addition, cooperation with existing identification systems using magnetic information and this proposed system provides more secure identification. The proposed system embeds a cardholder-related information that forms a watermark generated by the modulating manner of the PC/SS scheme into cardholder's portrait printed on the card using a simple watermarking scheme also proposed in this paper. Experimental results show that the proposed system extracts embedded information correctly as its fundamental ability. Furthermore, various properties of this system have been investigated, and it has been found that the spatial resolution of scanners is the most dominant to the performance of the proposed system.

key words: *identification, digital watermark, PC/SS, real number sequence, portrait*

1. Introduction

Recently, many researchers have studied digital watermarking technology multiplexing digital contents and related information referred to a watermark to protect rights on contents, for example [1]. A digital watermarking scheme embeds a watermark into the related content directly and imperceptibly.

While, a new spread spectrum communication system that provides a high-speed data transmission capability and an efficient use of radio frequency is required for wireless mobile communications. In such a situation, the parallel combinatorial spread spectrum (PC/SS) communication system was proposed and studied [2], [3].

On the other hand, although magnetic information is vulnerable against intentional modifications or changes in environment, contemporary individual identification systems use information recorded magnetically on the one's ID card. Thus, we need a novel individual identification system employing a new robust storing scheme.

In this paper, a new individual identification system as a novel application of the PC/SS scheme is proposed. In this proposed system, a card issuer embeds card owner-related information that forms a watermark generated by the modulating manner of the PC/SS scheme into the one's facial portrait on their own card. Since no magnetic information is used for identification in the proposed system, this system is robust to intentional modifications or various environments.

This proposed system is applicable to existing identification systems that a person is identified by one's own ID card holding the cardholder's portrait on itself as a passport, a car license, and a recent credit card. Therefore, this proposed system is an upper compatible system to contemporary identification systems that a human identifies a cardholder's face with the portrait on the card. Nevertheless, the cooperation between contemporary identification systems using magnetic information and the proposed system provides more secure identification.

Furthermore, it requires no communication facility for transactions between a card reader and the database. Because the employed watermarking scheme also proposed in this paper needs no original image in its watermark extracting process.

2. Parallel Combinatorial Spread Spectrum System [2], [3]

The parallel combinatorial spread spectrum (PC/SS) system is a kind of multi-code direct sequence spread spectrum system, and uses combinations of pseudo-noise (PN) sequences. The baseband modulation of the PC/SS system is described here.

A transmitter has a set of M orthogonal sequences whose element is -1 or $+1$. An input sequence of k-bits data ($\boldsymbol{d}_{in} = (d_1, d_2, \cdots, d_k), d_i \in \{0, 1\}$) is converted to data of k parallel channels, and a mapping circuit chooses r transmitting PN sequences from the M assigned sequences according to the paralleled data.

The mapping method carried out as follows: First, $\boldsymbol{d}_{in}$ is split into two parts. The former $\boldsymbol{d}_s = (d_1, d_2, \cdots, d_r)$ represents the + or − signature of each chosen sequence. A state of the rest part $\boldsymbol{d}_c = (d_{r+1}, d_{r+2}, \cdots, d_k)$ specifies a combination of r se-

Manuscript received March 15, 2000.

Manuscript revised May 26, 2000.

[†]The authors are with the Department of Electrical and Electronic Systems, Faculty of Engineering, Saitama University, Urawa-shi, 338-8570 Japan.

quences.

Next, to select r PN sequences, $\boldsymbol{d}_c$ is coded into a constant weight code of length M and weight r ($\boldsymbol{c} = (c_1, c_2, \cdots, c_M), c_i \in \{0, 1\}$) referred to a (M, r) constant weight code. The mapping circuit chooses the i-th PN sequence for transmitting when $c_i = 1$.

A signature sequence for a set of transmitting sequences is derived from $(-1)^{d_i} (i = 1, 2, \cdots, r)$. Then, a transmitter multiplies a PN sequence set with $\boldsymbol{d}_s$, and transmits the sum of multiplied sequences forms a multi-level signal with $(r + 1)$ levels.

At a receiver, M matched filters are used to despread a received signal. Each filter matches the assigned PN sequence that is the same with the counterpart in a transmitter.

In the decision circuit, the r-out-of-M combination of transmitted PN sequences is estimated from matched filter outputs $\boldsymbol{y} = (y_1, y_2, \cdots, y_M)$. According to the descending order of ${y_i}^2$, the r largest elements of ${y_i}^2$ are decoded to ‘1,’ and the others are decoded to ‘0.’

Then, the estimated combination of sequences is transformed into a (M, r) constant weight code that becomes the latter part of the received data. From $\boldsymbol{y}$ and a constant weight code, we get the signature-dependent data that becomes the former part of the received data. The decoded data is ‘1’ when $y_i \geq 0$, and the others are decoded into ‘0.’

Finally, the receiver output is obtained through parallel to serial conversion.

3. Proposed Watermarking Scheme

A simple image-watermarking scheme extracting an embedded watermark without any original image is proposed here. In this proposed scheme, a watermark is an L-length real number sequence $\boldsymbol{X} = (x_1, x_2, \cdots, x_L)$ instead of the multi-level combined sequence using in the PC/SS system.

First in each embedding process, a DCT coefficient matrix ($F = f(u, v)$) is extracted from each digital document D by applying two-dimensional DCT to the whole D. u and v represent the horizontal frequency and the vertical frequency respectively.

Then, the scheme inserts $\boldsymbol{X}$ multiplied by the scaling factor α into F according to the L-length secret key $\boldsymbol{S} = (s_1, s_2, \cdots, s_L)$ derived from the preliminary investigation described below. To obtain the watermarked matrix ($F' = f'(u, v)$), the following equation is employed.

$$f'(u_i, v_i) = \alpha x_i + \frac{1}{8} \left\{ \begin{array}{c} f(u_i - 1, v_i - 1) + f(u_i, v_i - 1) \\ +f(u_i + 1, v_i - 1) + f(u_i - 1, v_i) \\ +f(u_i + 1, v_i) + f(u_i - 1, v_i + 1) \\ +f(u_i, v_i + 1) + f(u_i + 1, v_i + 1) \end{array} \right\}, \tag{1}$$

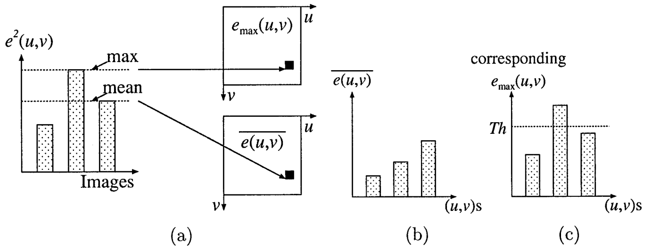

Fig. 1 (a) Obtaining $\overline{e(u,v)}$ and $e_{\max}(u,v)$, (b) $\overline{e(u,v)}$s in ascending order, and (c) $e_{\max}(u,v)$s ordered according to the ascending order of $\overline{e(u,v)}$. Since the second $e_{\max}$ is greater than the threshold Th in (c), its corresponding $\overline{e(u,v)}$ is not chosen as a component of $\boldsymbol{S}$, although its corresponding $\overline{e(u,v)}$ is smaller than that of the third $e_{\max}(u,v)$ in (b).

where u_i and v_i represent the horizontal frequency and the vertical frequency pointed by s_i respectively. Finally, the watermarked image D' is acquired by IDCT.

A hidden watermark is extracted with the same $\boldsymbol{S}$ that is the counterpart in the inserting process.

An algorithm to determine a secret key $\boldsymbol{S}$ is described here. $\boldsymbol{S}$ is derived from a preliminary investigation using several images.

Firstly, the error matrix ($E = e(u, v)$) of each image is obtained, where $e(u, v)$ is the difference between $f(u, v)$ and the mean value of its surrounding eight coefficients defined as

$$e(u, v) = f(u, v) - \frac{1}{8} \left\{ \begin{array}{c} f(u - 1, v - 1) + f(u, v - 1) \\ +f(u + 1, v - 1) + f(u - 1, v) \\ +f(u + 1, v) + f(u - 1, v + 1) \\ +f(u, v + 1) + f(u + 1, v + 1) \end{array} \right\}. \tag{2}$$

Secondly, the matrix of the mean square of $e(u, v)$ among images ($\overline{E} = \overline{e(u, v)}$) and the matrix of the maximum square of $e(u, v)$ among images ($E_{\max} = e_{\max}(u, v)$) are obtained (Fig. 1(a)).

Finally, according to the ascending order of $\overline{e(u, v)}$ whose corresponding $e_{\max}(u, v)$ is smaller than the threshold Th, L of (u, v)s are chosen to construct $\boldsymbol{S}$ (Figs. 1(b) and (c)). We suppose that either an embedding user or a watermarking system provider can make various $\boldsymbol{S}$ depending on not only the set of images for the above mentioned investigation but also the order of (u, v)s obtained from the result of the investigation itself.

4. Proposed Identification System

Figure 2 depicts the block diagram of the proposed identification system.

In the issuing process, a watermark indicating the cardholder is generated by the manner of the transmission in PC/SS communication systems described in 2. A card issuer chooses r sequences from assigned M orthogonal sequences according to a k bit user-identifying

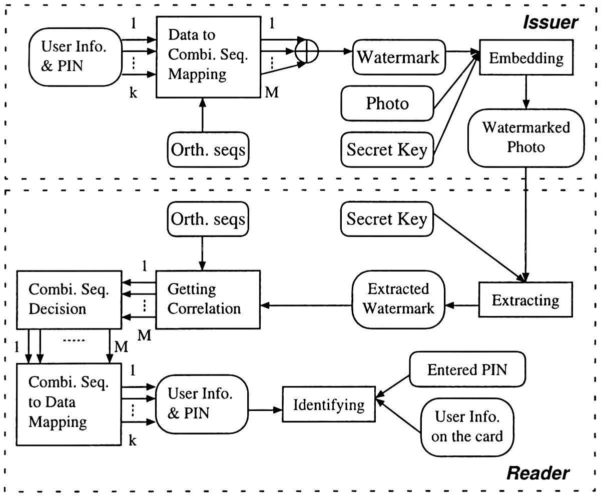

Fig. 2 The block diagram of the proposed system.

data that may consist of the user-defined PIN and user-related information. Assigned sequences consist of L-length real number sequence that has standard normal distribution. Note that each card-issuing house may make their own orthogonal sequences by applying the Gram-Schmidt orthogonalization to real number sequences for growing the security level up.

Each selected sequence is modulated with -1 or $+1$ according to the user-identifying data, and a watermark is derived from the sum of all modulated sequences. A digital watermarking scheme embedding a real number watermark like the watermarking scheme described above inserts a generated watermark into one's facial portrait, and the watermarked image is printed on the one's ID card.

A cardholder inserts the cardholder's own card into a card reader and enters his/her own PIN to the reader. Then, the card reader scans the portrait and related items from the inserted ID card. The resolution of the scanned image is adjusted to that of the original image, and then the watermarking scheme extracts the embedded watermark from the portrait.

The decision circuit calculates zero-shift cross correlation values between the extracted watermark and each orthogonal sequence. Each sequence is the same with the counterpart in the issuer. It is determine that the set of r sequences whose squared cross correlation values are the r largest values is selected to generate the embedded watermark. The user-identifying data is derived from the combination of determined r sequences and the signature state of them. Finally, the card reader compares the scanned item with the information from the decoded data to detect tampering of the card, and compares the user-entered PIN to PIN from the decoded data to identify the cardholder.

It is important that this proposed system has upper compatibility to contemporary identification systems. An example is immigration, that is, an immigration inspector identifies the face of the cardholder facing the inspector with the portrait on the card. Cardholder's portrait photo is sometimes printed on the holder's credit card, thus this proposed system is useful at a shop where customers use their credit card. In addition, because no original image is required in the watermark extracting process, it is possible that only the standalone card reader without any communication facility for transactions is needed.

It is assumed that an issuer prints a portrait on the regular position of an ID card precisely and a card reader holds an ID card regularly so that the scanner mounted on a reader scans a picture precisely. Moreover, we assume that all of the secret information such as a set of orthogonal sequences and $\boldsymbol{S}$ are protected by a black box in each card issuer or each card reader. It is mentioned that parameters used in the proposed system have to satisfy the inequality

$$k \geq r + \log_2({}_M\mathrm{C}_r). \tag{3}$$

5. Performance Evaluation

Performances of the proposed system are investigated by computer simulation under the conditions described in 5.1. The fundamental performance is examined in 5.2, moreover properties against possible degradations on a scanned image are evaluated from 5.3 to 5.5. The properties examined include: the spatial resolution property (in 5.3), the γ property (in 5.4) and the quantization resolution property (in 5.5). Furthermore, combined properties thereof are evaluated.

5.1 Conditions

Nine pictures that appear in Fig. 3 are employed for evaluations. Each picture consists of 128 × 128 pixels and has 256 levels from zero to 255 in each RGB channel, as known as 24-bits color. The luminance level of each image is adjusted between 10 and 240 linearly. It is mentioned that only the Y channel of Y/Cb/Cr representation is used to insert a watermark. Photogenic subjects are male.

M of L-length orthogonal real number sequences are obtained by applying the Gram-Schmidt orthogonalization to M of L-length real number sequences that each sequence has the standard normal distribution. Magnitudes of each orthogonal sequence are adjusted so that an orthogonal real number sequence that has the standard normal distribution. Both L and M are set to 1000 in this evaluation.

Considering that an user-identifying data consists of a four digit PIN represented by 14 bits and a 32 bits user-related information, k is set to 46. Moreover, allowing that an user-related data becomes 128 bits, the condition of k = 142 is also employed. r should be the smallest value satisfied inequality (3) for each k;

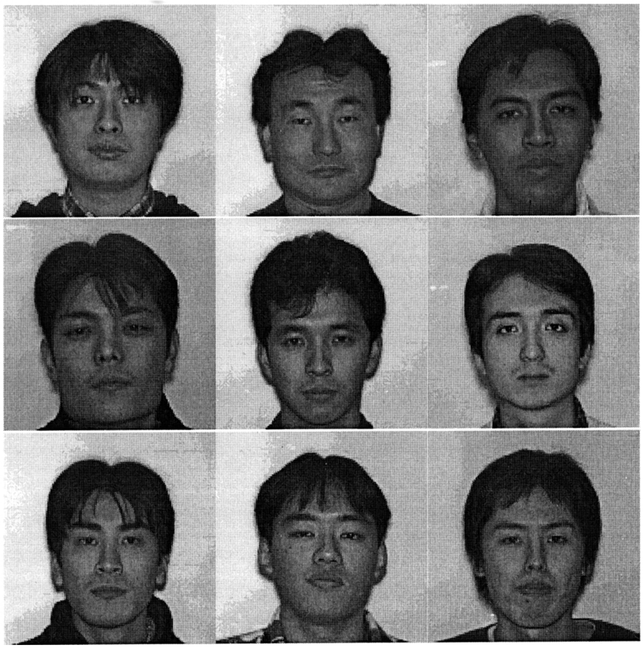

Fig. 3 Luminance level adjusted portraits.

when $k = 46$, r is set to five, and $r = 18$, when $k = 142$.

Five watermarks are used for each r, and each watermark is the sum of random selected sequences that are modulated randomly with -1 or $+1$. Since each orthogonal real number sequence that has the standard normal distribution, a watermark generated from r real number sequences has the distribution $N(0, r)$.

$\boldsymbol{S}$ is derived from the preliminary investigation using nine images mentioned above and is constructed by L chosen (u, v)s under the ascending order of $e(u, v)$ whose corresponding $e_{max}(u, v)$ is smaller than Th among R, G, B, and Y channels of each image. Th is set to 22. According to the preliminary subjective examination for evolving the maximum α that makes an identification with a watermarked image by eyes possible, α is set to $\sqrt{4500/r}$.

The performance of the proposed system is evaluated in terms of symbol error rate (SER) characteristics as those of PC/SS systems. The SER is $P_e = 1 - P_{cc} \cdot P_{cs}$, where P_{cc} and P_{cs} represent the probability of deciding the r-out-of-M combination correctly and the probability of decoding the signature-dependent data correctly, respectively [2].

5.2 Fundamental Performance

Both P_{cs} and P_{cc} are equal to one among 90 examinations: nine images, two of r's, and five watermarks, all the P_e of this proposed system result in being equal to zero. Figure 4 illustrates a watermarked image with the PSNR is about 23 [dB]. It is still enough for a human to identify the cardholder's face with the card's portrait under the condition of PSNR ≈ 23 [dB].

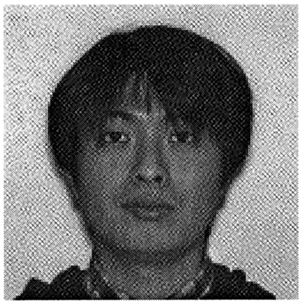

Fig. 4 A watermarked image, $r = 18$, PSNR $= 23$ [dB].

Table 1 Spacial resolution properties.

	Scaling factor							
r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05
5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18	0.99	0.45	0.00	0.00	0.00	0.00	0.00	0.00

5.3 Spatial Resolution Property

The spatial resolution of the scanner in a card reader may differ from that of the printer in a card issuer. Scaling and rescaling a watermarked picture simulates under such conditions. The quadratic interpolation [4] used in StirMark [5], [6] is employed as its scaling method, because StirMark is expected to be a standard fair benchmark for image-watermarking systems. Scaling factors employed for evaluation are 0.30, 0.70, 0.90, 0.95, 0.99, 1.01, 1.05, 1.10, and 1.2, because scaling by these factors introduce nonlinear interpolation to an image. The symbol error rates are shown in Table 1. When scaling factor is set to 1.1 and 1.2, P_e results in zero, therefore those results are left out from Table 1 for its simplicity.

Table 1 demonstrates that P_e is equal to zero on image enlargements. On image reduction as the scaling factor is set to 0.3 or 0.7, P_e marks high. Because image reduction that is equivalent to the low-pass-filtering deletes high frequency coefficients where most of the watermarks are embedded. This proposed system is robust under the conditions that a little difference in size may make large nonlinear affection on an image as the scaling factor is equal to 0.95, 0.99, 1.01, and 1.05.

5.4 γ Property

Card readers may have a scanner that has the different γ property each other. The normalized luminance level of a color channel of a γ-controlled image (L_O) is obtained by the equation $L_O = {L_I}^{\gamma}$, where L_I represents the normalized luminance level of a color channel of a watermarked photo. Selected γ's are 0.1, 0.2, 0.5, 2.0, 5.0, and 10.0.

Among all examinations, both P_{cc} and P_{cs} are equal to one, and the results show that P_e is equal to zero. It is found that the proposed system works correctly, although the γ property of a scanner varies.

5.5 Quantization Resolution Property

Each card reader may have various quantization resolutions q's that affect the system performance. Through all the evaluations in this paper, both q's of original portraits and watermarked images are eight in each R/G/B channel as described in 5.1. In this performance evaluation, q's of a degraded image fluctuates between one and seven for each color channels. Note that zero or 255 is represented when $q = 1$.

Table 2 presents that this proposed system extracts the embedded information correctly under all the conditions excepting the condition that $r = 18$ and $q = 1$. Since the energy for inserting a watermark generated from 18 sequences is smaller than that of a watermark generated from five sequences led from 5.1, the performance is affected by the q, when $r = 18$.

Table 2 Quantization resolution properties.

	q							
r	1	2	3	4	5	6	7	8
5	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
18	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00

5.6 Spatial Resolution and γ Combined Property

Card reader's scanner may have not only the different spatial resolution but also the different γ property from card issuer's printer. Evaluation simulates the combined conditions described at 5.3 and 5.4, and results are pointed in Table 3.

On image enlargements, it is found that P_e results in being equal to zero under all the γ variation excepting only one condition; $r = 18$, the scaling factor is 1.05, and $\gamma = 10.0$. It follows from the results that P_e becomes greater in proportion to increases in the distance between γ and one. The fluctuation of γ introduces little degradation to P_e under the conditions the scaling factor is 0.90 or 0.95 in comparison with the spatial resolution properties described in Table 1.

5.7 Spatial Resolution and Quantization Resolution Combined Property

Table 4 shows that the spatial resolution and the quantization resolution combined properties obtained from combined simulations using the schemes described in

Table 3 Spatial resolution and γ combined properties.

		Scaling factor									
γ	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
0.1	5	1.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.62	0.06	0.06	0.00	0.00	0.00	0.00	0.00	0.00
0.2	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	1.00	0.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.5	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.41	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2.0	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.56	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
5.0	5	0.99	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.66	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00
10.0	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.70	0.01	0.04	0.00	0.00	0.00	0.01	0.00	0.00

Table 4 Spatial resolution and quantization resolution combined properties.

		Scaling factor									
q	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
1	5	0.99	0.71	0.01	0.00	0.01	0.00	0.02	0.00	0.00	0.00
	18	0.99	0.90	0.44	0.52	0.49	0.01	0.47	0.37	0.18	0.19
2	5	0.99	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.77	0.04	0.11	0.00	0.00	0.00	0.00	0.00	0.00
3	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.49	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
5	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.98	0.46	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
6	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.41	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
7	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.98	0.45	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
8	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.45	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

5.3 and 5.5. From the results, P_e becomes larger with decreasing q. In particular, P_e's mark high under the conditions $r = 18$ and $q = 1$. Nevertheless, the spatial resolution property is the dominant factor on the performance when $q \geq 3$, consequently the q variation introduces a little influence to the proposed system looking general.

5.8 γ and Quantization Resolution Combined Property

The γ and the quantization resolution combined properties appear in Table 5. When $q \geq 3$, all of the P_e's are equal to zero, thus Table 5 contains properties under the condition that $q \leq 2$. Under the condition that q is equal to one or two, performances using a watermark generated from 18 sequences is influenced. It is shown that the fluctuation of γ affects the proposed system's performance smaller than that of the spatial resolution varying in comparison with Table 3.

Table 5 γ and quantization resolution combined properties.

		γ						
q	r	0.1	0.2	0.5	1.0	2.0	5.0	10.0
1	5	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.14	0.06	0.00	0.00	0.00	0.00	0.05
2	5	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.04	0.00	0.00	0.00	0.00	0.00	0.00

5.9 All Combined Property

Combined properties under the conditions that all the factors described between 5.3 and 5.5 move independently appear through Table 6 to Table 11. It is shown that the spatial resolution is the key item on the property, in particular, image reduction with the scaling factor that is less equal to 0.7. When the scaling factor is between 0.95 and 1.05, the γ property is the dominant cause for degradation of P_e. It is found that P_e becomes greater with decreasing q under the specified combined conditions of the spatial resolution and the γ.

Table 6 All combined properties, $\gamma = 0.1$.

		Scaling factor									
q	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
1	5	1.00	0.89	0.81	0.72	0.85	0.00	0.90	0.58	0.56	0.45
	18	1.00	0.97	0.93	0.93	0.95	0.14	0.96	0.89	0.86	0.85
2	5	1.00	0.39	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.83	0.44	0.48	0.38	0.04	0.32	0.30	0.20	0.14
3	5	1.00	0.39	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	1.00	0.80	0.26	0.38	0.20	0.00	0.19	0.16	0.05	0.02
4	5	1.00	0.21	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.72	0.29	0.30	0.12	0.00	0.09	0.17	0.03	0.00
5	5	0.99	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.66	0.81	0.14	0.01	0.00	0.00	0.02	0.01	0.00
6	5	1.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	1.00	0.62	0.05	0.07	0.00	0.00	0.00	0.00	0.00	0.00
7	5	1.00	0.04	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	1.00	0.63	0.07	0.09	0.00	0.00	0.00	0.01	0.00	0.00
8	5	1.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.62	0.06	0.06	0.00	0.00	0.00	0.00	0.00	0.00

Table 7 All combined properties, $\gamma = 0.2$.

		Scaling factor									
q	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
1	5	1.00	0.48	0.04	0.69	0.07	0.00	0.08	0.03	0.02	0.00
	18	0.99	0.87	0.63	0.63	0.62	0.06	0.65	0.48	0.43	0.31
2	5	1.00	0.45	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.81	0.23	0.37	0.23	0.00	0.17	0.14	0.04	0.03
3	5	1.00	0.14	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.71	0.13	0.15	0.06	0.00	0.09	0.03	0.00	0.00
4	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.59	0.03	0.03	0.00	0.00	0.00	0.00	0.00	0.00
5	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	1.00	0.49	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00
6	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.49	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
7	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.47	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
8	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	1.00	0.48	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table 8 All combined properties, $\gamma = 0.5$.

		Scaling factor									
q	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
1	5	1.00	0.52	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.84	0.26	0.44	0.22	0.00	0.22	0.17	0.06	0.04
2	5	0.99	0.19	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.78	0.13	0.19	0.17	0.00	0.10	0.04	0.01	0.01
3	5	1.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.59	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.47	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
5	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.43	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
6	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.43	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
7	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.42	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
8	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.41	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table 9 All combined properties, $\gamma = 2.0$.

		Scaling factor									
q	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
1	5	1.00	0.81	0.07	0.10	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.93	0.53	0.55	0.23	0.00	0.24	0.39	0.25	0.27
2	5	1.00	0.15	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.75	0.05	0.04	0.00	0.00	0.00	0.01	0.00	0.00
3	5	1.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.66	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.59	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
5	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.55	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
6	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.58	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
7	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.56	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
8	5	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.56	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Table 10 All combined properties, $\gamma = 5.0$.

		Scaling factor									
q	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
1	5	1.00	0.31	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.80	0.16	0.20	0.02	0.00	0.27	0.88	0.05	0.04
2	5	1.00	0.29	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.79	0.14	0.13	0.00	0.00	0.00	0.04	0.00	0.00
3	5	1.00	0.07	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.70	0.05	0.06	0.00	0.00	0.00	0.01	0.00	0.00
4	5	1.00	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.68	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00
5	5	1.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.68	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00
6	5	1.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.66	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00
7	5	0.99	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.66	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00
8	5	0.99	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.66	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00

Table 11 All combined properties, $\gamma = 10.0$.

		Scaling factor									
q	r	0.30	0.70	0.90	0.95	0.99	1.00	1.01	1.05	1.10	1.20
1	5	1.00	0.48	0.17	0.17	0.05	0.00	0.06	0.11	0.09	0.04
	18	0.99	0.83	0.44	0.44	0.21	0.05	0.20	0.35	0.27	0.24
2	5	1.00	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.80	0.16	0.16	0.02	0.00	0.03	0.08	0.06	0.05
3	5	0.99	0.08	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.71	0.04	0.07	0.00	0.00	0.00	0.02	0.00	0.00
4	5	0.99	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.72	0.00	0.06	0.00	0.00	0.00	0.01	0.00	0.00
5	5	1.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.69	0.01	0.05	0.00	0.00	0.00	0.01	0.00	0.00
6	5	1.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.69	0.01	0.04	0.00	0.00	0.00	0.01	0.00	0.00
7	5	1.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.69	0.01	0.05	0.00	0.00	0.00	0.00	0.00	0.00
8	5	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	18	0.99	0.70	0.01	0.04	0.00	0.00	0.00	0.01	0.00	0.00

6. Conclusions

A new individual identification system as a novel application of the PC/SS scheme has been proposed in this paper. In the proposed system, an issuer encodes cardholder-related information into a real number watermark by the PC/SS scheme, and inserts the watermark into cardholder's facial portrait printed on his/her own ID card by the simple image-watermarking scheme that has been also proposed in this paper. No magnetic information is used for identification, therefore the proposed system is robust to intentional modifications or various changes in environment.

This proposed system is applicable to all the identification systems using the ID card that holds cardholder's portrait photograph on itself. Thus, the proposed system is upper compatible to contemporary identification systems that a human identifies cardholder's face with the card's portrait. However, the cooperation between contemporary identification systems using magnetic information and the proposed system provides more secure identification. Moreover, since the employed watermarking scheme also proposed in this paper does not require the original image in its watermark extracting process, no communication facility for transactions between a card reader and the database is needed.

Experimental evaluation among nine male portraits, two multiplets sequences, and five watermarks for each multiplet has shown that this proposed system has the perfect performance as its fundamental ability and has robustness against the γ fluctuation on scanners. Since the energy for hiding a watermark generated from 18 sequences is small, performances under the conditions that image reduction and the quantization resolution is small are degraded. It has been found that the spatial resolution of a scanner is rather dominant than the γ property or the quantization resolution of a scanner for the performance degradation.

While modifying a picture for ordinary watermarking systems means to change the luminance level of the picture, to modify a picture for the proposed system means changing the card itself, because a watermarked image is printed on the owner's ID card made of plastic or paper. Furthermore, since the number of possible orthogonal sequences that form a possible watermark is huge, it is very hard for a forger to counterfeit a valid card.

The authors are developping a modified system that embeds a watermark combined from orthogonal binary sequences and a new system that generates watermarks by the manner of multi-level modulations. Employing a canceling system with binary watermarks is also a further work. Analyzing the maximum amount of embedded data $k_{\max}$ is an other further work.

Acknowledgements

The authors appreciate goodness of Prof. Hitoshi Maekawa at Saitama University.

References

[1] M. Fujiyoshi and T. Hasegawa, "Code energy adaptive watermarking," Proc. 1998 International Symposium on Inf. Theory and its Application, vol.II, no.TA3-3, pp.364–367, Mexico City, Mexico, Oct. 14–16, 1998.

[2] S. Sasaki, J. Zhu, and G. Marubayashi, "A study of mapping and demodulating method for parallel combinatory spread spectrum communication system," IEICE Trans., vol.J75-A, no.4, pp.824–830, April 1992.

[3] S. Sasaki, G. Kikuchi, J. Zhu, and G. Marubayashi, "Multiple access performance of parallel combinatory spread spectrum communication systems in nonfading and rayleigh fading channels," IEICE Trans. Commun., vol.E78-B, no.8, pp.1152–1161, Aug. 1995.

[4] N.A. Dodgson, "Quadratic interpolation for image resampling," IEEE Trans. Image Process., vol.6, no.9, pp.1322–1326, Sept. 1997.

[5] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, “Attacks on copyright marking systems,” Proc. 1998 International Workshop on Inf. Hiding, pp.219–239, Portland, the U.S., April 15–17, 1998.

[6] F.A.P. Petitcolas and R.J. Anderson, “Evaluation of copyright marking systems,” Proc. 1999 IEEE International Conf. on Multimedia Computing and Syst., vol.1, pp.574–579, Florence, Italy, June 7–11, 1999.

Masaaki Fujiyoshi received his B. Liberal Arts and M.E. degrees from Saitama University in 1995 and 1997, respectively, where he is currently working toward the Ph.D. degree in Information and Computer Engineering. His research interests include spread spectrum communications, image processing, and secure communications. He is a student member of IEEE.

Takaaki Hasegawa received his B.E. and M.E. and Ph.D. degrees in Electrical Engineering from Keio University in 1981, 1983, and 1986, respectively. He joined the Faculty of Engineering at Saitama University in 1986. He has been an Associate Professor since 1991. During 1995–1996 he was a visiting scholar at The University of Victoria. His research interests include human communications (HC), mobile agents, human machine interfaces, Spread Spectrum (SS) Communications and Intelligent Transport Systems (ITS). He is the author of the book Primary C Language Note (Japanese, HBJ, 1989), a co-author of the books: Fundamentals and Applications of Spread Spectrum Communication Technologies (Japanese, Triceps, 1987), Application Technologies of Spread Spectrum Communications (Japanese, Triceps, 1992), and Personal Communications and Consumer Communications (Japanese, Baifukan, 1994). He is a member of IEEE and SITA.