

On the Amount of Embedded Information of Watermarking Methods Based on the Parallel Combinatorial Spread Spectrum Scheme

Masaaki FUJIYOSHI^{†a)}, *Student Member and* Takaaki HASEGAWA[†], *Regular Member*

SUMMARY The maximum amounts of embedded information that is important in practical system design of two watermarking methods based on the parallel combinatorial spread spectrum (PC/SS) scheme are discussed in this paper. One is a private watermarking method proposed in this paper and has a practical strong point to make the quality of the watermarked image to be constant in any images. The other is a public watermarking method that was previously proposed by the authors. Through this study, the minimum number of orthogonal sequences for embedding the required amount of information under the condition that quantization noise is only assumed is found in each watermarking method.

key words: digital watermark, PC/SS, real-number sequence, maximum amount of embedded information

1. Introduction

Recently, many researchers have studied digital watermarking technologies to protect intellectual properties on digital contents, for example [1]–[4]. A digital watermarking method embeds related information referred to a watermark into the target content directly. While, the parallel combinatorial spread spectrum (PC/SS) communication system that conveys data by a combination of orthogonal sequences with polarities was proposed and studied [5], [6]. The PC/SS system provides high-speed data transmission capability and simultaneously provides high spectral efficiency. In such a situation, a digital watermarking method based on the PC/SS scheme and an individual identification system that employs this watermarking method have been proposed [7]–[9]. However, the amount of embedded information in this watermarking method has not been evaluated yet. In this paper, the maximum amounts of embedded data that is important for practical system design in digital watermarking methods based on the PC/SS scheme are discussed. Neither noise nor distortion excepts quantization noise is assumed in this fundamental investigation.

In general, there are two types of digital watermarking methods, private and public. A private water-

marking method requires the original image to extract an embedded watermark, on the other hand, a public watermarking method extracts an embedded watermark without any original image. Therefore, this paper adopts the watermarking method [1] proposed in this paper as a private watermarking method. This proposed method improves a well known watermarking method [2] in making the quality of the watermarked image to be constant in any images from a practical point of view. As a public watermarking method, the watermarking method that has been already proposed [7]–[9] is adopted.

Through this study, relation between the amount of embedded information and the number of orthogonal sequences is found in each watermarking method.

2. Parallel Combinatorial Spread Spectrum Systems [5], [6] and the Structure of a Watermark [7]–[9]

2.1 PC/SS Transmitter

In parallel combinatorial spread spectrum (PC/SS) systems [5], [6], a set of M of binary orthogonal pseudo-noise (PN) sequences is assigned for each user, where M is the number of available sequences. Data with k -bits is conveyed by choosing r sequences with polarities among M of PN sequences. Therefore, following expression represents the number of bits per symbol,

$$k = r + \left\lceil \log_2 \binom{M}{r} \right\rceil. \quad (1)$$

Figure 1(a) shows the baseband transmitter model of PC/SS systems. At first, a part of input parallel data is encoded into a constant weight code (CWC) of length M with Hamming weight r . This is referred to an (M, r) -CWC. The element of a CWC corresponds to the on-off sign for M of sequences. The polarity of each PN sequence to be transmitted is determined by the other part of input data. r modulated sequences to be transmitted are summed to form a transmitting signal.

Manuscript received August 29, 2000.

Manuscript revised November 15, 2000.

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

a) E-mail: masaaki@hslab.ees.saitama-u.ac.jp

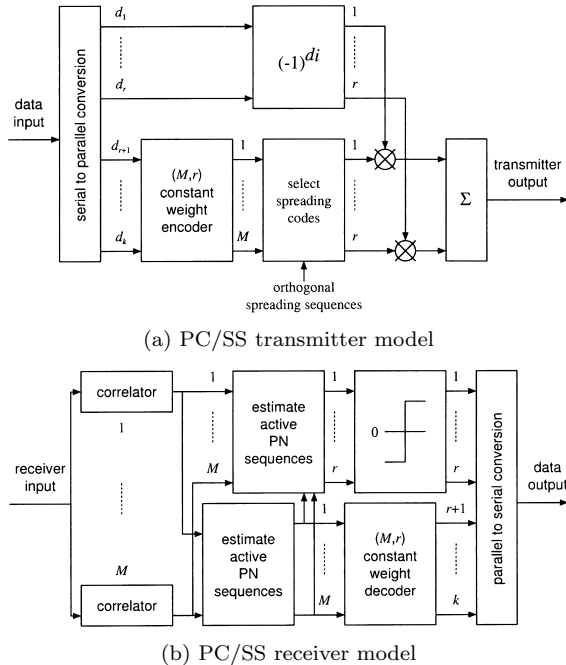


Fig. 1 PC/SS transmitter and receiver model.

2.2 PC/SS Receiver

Configuration of the PC/SS demodulator is shown in Fig. 1(b). The received signal passes through M of correlators. The decision variable of each orthogonal PN sequence is obtained as the output of the corresponding correlator.

According to the descending order of the magnitude of decision variables, r elements are decoded to '1,' and the other elements are decoded to '0.' This procedure forms an (M, r) -CWC that estimates r of active sequences. A part of the data that consists of the $(k - r)$ -bits is obtained by decoding the CWC.

From the correlators' outputs and the (M, r) -CWC, the other part of the data is acquired by demodulating the polarities of those r sequences. Finally, the receiver output is obtained through parallel to serial conversion.

2.3 The Watermark Sequence Structure Based on the PC/SS System [7]–[9]

The watermark sequence structure based on the modulating manner of the PC/SS system described in Sect. 2.1 is shown here. An individual identification system that the authors have previously proposed [7]–[9] employs this watermark structure.

Since the degree of freedom of real-number orthogonal sequences is greater than that of binary orthogonal sequences, real-number orthogonal sequences are employed instead of binary orthogonal sequences used in

the PC/SS system. It is to be noted that we obtain various sets of M of L -length real-number orthogonal sequences easily by applying Gram-Schmidt orthogonalization to M of L -length real-number sequences, as far as $M \leq L$. L is the length of M of sequences and is also the length of a watermark.

Similar to the modulating manner of the PC/SS scheme, it chooses r of sequences with polarities among M orthogonal sequences according to information with k -bits, and gathers selected sequences to form a watermark sequence. Since each component of an orthogonal sequence has the standard normal distribution in this structuring method, components of a watermark generated from r of sequences have the normal distribution with mean zero and variance r .

3. Embedding Algorithms

Two algorithms that embed real-number sequences into images are described in this section. One is Code Energy Adaptive Watermarking (CEAW) [1] proposed in this paper and is employed as a private watermarking method in this paper. The other is Simple Watermarking based on Neighbor Coefficient Statistics (SWNCS) that was previously proposed [7]–[9] and is used as a public watermarking method in this paper.

3.1 Code Energy Adaptive Watermarking [1]

A novel watermarking method [1] that improves a well known watermarking scheme proposed by Cox et al. [2] is proposed here, those schemes are classified into private watermarking that requires original images in each extracting process.

In Cox's scheme, a 1000-length sequence that the components of each sequence have the standard normal distribution is embedded, while, this proposed scheme inserts L -length sequence $\mathbf{w} = (w_1, \dots, w_L)$ that w_l have the normal distribution with mean zero and a certain variance.

The quality of a watermarked image fluctuates in the conventional method. In contrast, the proposed scheme adjusts the variance of an embedded watermark adaptively so that the quality of a watermarked image is constant not only in any images but also with any watermarks. Since this proposed method improves Cox's method from this practical point of view, the proposed method differs from other improved methods [3], [4].

In addition, the proposed algorithm restricts insertion candidates to low frequency components as depicted in Fig. 2. Therefore, this method overcomes low-pass-filtering including shrinking and JPEG lossy compression that are usually applied to images for transmission or reuse.

Here, the definite algorithm is described. Firstly, a discrete cosine transform (DCT) matrix of target image I is obtained, moreover, the proposed method re-

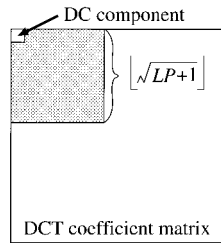


Fig. 2 An example of insertion candidates.

stricts insertion candidates to low frequency components according to user-defined ratio P . Secondly, L of the highest magnitude alternating frequencies ($\mathbf{f} = (f_1, \dots, f_L)$) are chosen from insertion candidates. Because the proposed scheme employs the same equation as that of the conventional scheme shown as Eq. (2) to obtain watermarked coefficients ($\mathbf{f}' = (f'_1, \dots, f'_L)$), this algorithm has to compute the adaptive energy of a watermark with a feedback manner.

$$f'_l = f_l(1 + \alpha w_l), \quad (2)$$

where α is constant and is set to 0.1 in this paper.

Consequently, the peak-to-peak signal-to-noise ratio (PSNR) is acquired by embedding sequence $\mathbf{w}' = (w'_1, \dots, w'_L)$ that w'_l have the normal distribution with mean zero and variance v^2 into I . The following expression gives adaptive energy $L \cdot \sigma^2$ from the obtained PSNR and user required PSNR_u .

$$\sigma^2 = \frac{XYA^2}{10^{0.1\text{PSNR}_u} \alpha^2 \sum_{l=0}^{L-1} (f_l w'_l)^2}, \quad (3)$$

where X and Y represent the horizontal number of pixels of the target image and the vertical number of pixels, respectively. Furthermore, A denotes the dynamic range of the luminance of I . The PSNR is the defined as follows,

$$\text{PSNR} = 10 \log_{10} \frac{XYA^2}{\sum_x \sum_y \{d(x, y) - d'(x, y)\}^2}, \quad (4)$$

where $d(x, y)$ and $d'(x, y)$ represent the luminance level of the pixel (x, y) of I and that of watermarked image I' , respectively.

Then, the proposed algorithm multiplies each component of \mathbf{w}' by σ/v so that the variance of the modified sequence is σ^2 , and inserts modified sequence \mathbf{w} into the target image. Finally, I' is produced by applying inverse DCT to the watermarked DCT matrix.

3.2 Simple Watermarking Based on Neighbor Coefficient Statistics [7]–[9]

The watermarking algorithm used in an individual

identification system that the authors have already proposed [7]–[9] is simply described here. This watermarking scheme is a public watermarking scheme that requires no original image in each watermark extracting process.

This watermarking scheme inserts L -length sequence $\mathbf{w} = (w_1, \dots, w_L)$ that w_l have the normal distribution with mean zero and a certain variance into L of coefficients. Moreover, L of coefficients are L of the smallest coefficients according to the ascending order of the index values to keep the quality of a watermarked image high. The index value in this method is the difference between the mean of surround eight coefficients and itself in the DCT domain. Accordingly, set of such coefficients $\mathbf{h} = (h_1, \dots, h_L)$ referred as secret key \mathbf{h} is derived from the preliminary investigation.

Each preliminary investigation employs several images. Let us define that u and v denote the horizontal frequency and the vertical frequency, respectively. Firstly, this algorithm gets DCT matrix $F_i = \{f_i(u, v)\}$ of i -th image I_i , and computes error DCT matrix $E_i = \{e_i(u, v)\}$ with the following expression.

$$e_i(u, v) = f_i(u, v) - \frac{1}{8} \begin{Bmatrix} f_i(u-1, v-1) + f_i(u, v-1) \\ + f_i(u+1, v-1) + f_i(u-1, v) \\ + f_i(u+1, v) + f_i(u-1, v+1) \\ + f_i(u, v+1) + f_i(u+1, v+1) \end{Bmatrix}. \quad (5)$$

Secondly, this algorithm acquires maximum error DCT matrix $E_{max} = \{e_{max}(u, v)\} = \{\max_i (e_i^2(u, v))\}$. Finally, secret key \mathbf{h} whose components are L of the smallest frequencies according to ascending order of the values of $e_{max}(u, v)$ is constructed. We suppose that either an embedding user or a watermarking system provider can make various \mathbf{h} depending on not only the set of images for the above mentioned investigation but also the order of chosen frequencies obtained from the result of the investigation itself.

Here, the definite algorithm is described. Firstly, a DCT matrix of I is obtained, and this scheme inserts a watermark sequence into frequencies $h_l = f(u_l, v_l)$ pointed by prior determined \mathbf{h} , the following expression is used to obtain watermarked matrix $F' = \{f'(u, v)\}$.

$$f'(u_l, v_l) = \beta w_l + \frac{1}{8} \begin{Bmatrix} f(u_l-1, v_l-1) + f(u_l, v_l-1) \\ + f(u_l+1, v_l-1) + f(u_l-1, v_l) \\ + f(u_l+1, v_l) + f(u_l-1, v_l+1) \\ + f(u_l, v_l+1) + f(u_l+1, v_l+1) \end{Bmatrix}, \quad (6)$$

where β is Eq. (7).

$$\beta = \sqrt{\frac{XYA^2}{Lr10^{0.1\text{PSNR}_u}}}, \quad (7)$$

Finally, we get I' by applying inverse DCT to F' .

4. Estimation of the Maximum Amount of Embedded Data

4.1 An Approach to Performance Evaluation [10]

A watermark described in Sect. 2.3 is formed by summing chosen r sequences with polarities among M orthogonal sequences, moreover passes through M of correlators in each decoding process. Let us define that $C_m (m = 1, \dots, M)$ denotes the m -th largest correlator output in magnitude. Since M of PN sequences are orthogonal, C_r^2 differs from C_{r+1}^2 greatly. Noises and distortions, however, make C_r^2 to be closer to C_{r+1}^2 . Thus, we estimate the degradation of an extracted watermark using the ratio C_{r+1}^2 versus C_r^2 [8], [10] defined as

$$\gamma = \frac{C_{r+1}^2}{C_r^2}. \tag{8}$$

Furthermore, we discuss the watermarking scheme performance by the distribution of γ .

γ always gets zero under the ideal condition and is close to one under the noisy and distorted condition, various $F(\gamma)$'s are plotted in Fig. 3. Hence, the large value of $\int_0^1 F(\gamma) d\gamma$ means that the average performance of the watermarking scheme is high. On the other hand, slow convergence to one (Fig. 4) means existence high value of γ , and also means misdecoding possibility. Therefore, the 95th percentile of $F(\gamma)$ is also used as an index of the worst performance of a watermark method.

4.2 Common Evaluation Conditions

In the following subsections, $F(\gamma)$ is obtained from experimental statistics that several watermarks are embedded into several images using two watermarking algorithms; one is Code Energy Adaptive Watermarking (CEAW) proposed in Sect. 3.1 as a private watermarking method and the other is Simple Watermarking based on Neighbor Coefficient Statistics (SWNCS) described in Sect. 3.2 as a public watermarking method.

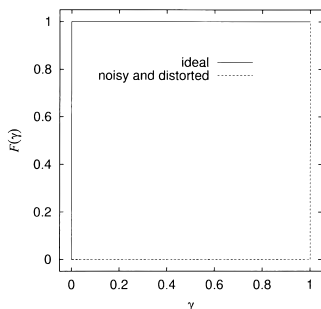


Fig. 3 Cumulative distribution functions of γ ; under the ideal condition and under the noisy and distorted condition.

Sample distribution functions are obtained by applying the following equation to each set of γ 's ($\mathbf{g} = (g_1, \dots, g_N)$) obtained from each experiment.

$$F_{\mathbf{g}}(\gamma) = \begin{cases} 0, & \gamma < g(1) \\ \frac{n}{N}, & g(n) \leq \gamma < g(n+1), \\ & n = 1, \dots, N-1 \\ 1, & \gamma \geq g(N) \end{cases}, \tag{9}$$

where, $g(n), n = 1, \dots, N$ is the order statistics of the sampled data \mathbf{g} .

Let us set $L = M$. Experimental parameters are shown in Tables 1 and 2.

System performance is evaluated in SER; the SER is $S_e = 1 - P_{cc} \cdot P_{cs}$, where P_{cc} and P_{cs} represent the probability of deciding the r -out-of- M combination correctly and the probability of correct decision of the polarity-dependent data, respectively [5].

Neither noise nor distortion excepts quantization noise is assumed in this paper.

4.3 Embedding by Code Energy Adaptive Watermarking

Nine of gray-scale images that have different charac-

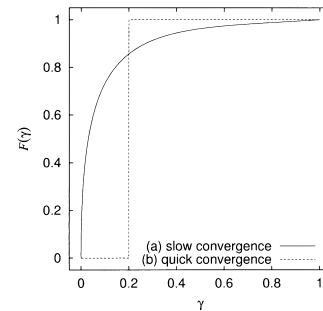


Fig. 4 Examples of $F(\gamma)$. (a) $F(\gamma)$ converges to one slowly (b) $F(\gamma)$ converges to one quickly.

Table 1 Conditions on sequences.

M	100, 300, 500, 700, 1000
# of set of orthogonal seqs	3 per M
# of watermarks	5 per set of orthogonal seqs

Table 2 Employed r for each pair of k and M .

k [bits]	M				
	100	300	500	700	1000
64	13	9	8	8	7
128	37	22	19	17	16
154	62	27	23	22	20
256	—	55	45	40	37
471	—	197	105	90	79
512	—	—	120	101	88
787	—	—	323	195	160
1024	—	—	—	331	238
1104	—	—	—	457	270
1579	—	—	—	—	652

teristics are selected for experiments from the SIDBA standard image database and are shown in Fig. 5. Each picture consists of 256×256 pixels and has 256 levels from zero to 255. The PSNR is set to 40 [dB] in all the watermarked images. Figure 6 illustrates $F_g(\gamma)$ obtained from the experiments that use the nine images mentioned above. Table 3 shows the SERs.

Figures 7 and 8 illustrate the integral of $F_g(\gamma)$ and



Fig. 5 Nine of gray-scale images from SIDBA.

95th percentile of $F_g(\gamma)$. It is considered that 95th percentile is appropriate as a performance index of performance of CEAW from Table 3, Fig. 7, and Fig. 8.

Table 3 Average S_e , embedding using CEAW.

k	M				
	100	300	500	700	1000
64	0.00	0.00	0.00	0.00	0.00
128	0.00	0.00	0.00	0.00	0.00
154	0.01	0.00	0.00	0.00	0.00
256	—	0.00	0.00	0.00	0.00
471	—	0.04	0.00	0.00	0.00
512	—	—	0.00	0.00	0.00
787	—	—	0.05	0.01	0.00
1024	—	—	—	0.34	0.01
1104	—	—	—	0.07	0.01
1579	—	—	—	—	0.06

Table 4 Average S_e , embedding using SWNCS.

k	M				
	100	300	500	700	1000
64	0.00	0.00	0.00	0.00	0.00
128	0.00	0.00	0.00	0.00	0.00
154	0.00	0.00	0.00	0.00	0.00
256	—	0.00	0.00	0.00	0.00
471	—	0.00	0.00	0.00	0.00
512	—	—	0.00	0.00	0.00
787	—	—	0.00	0.00	0.00
1024	—	—	—	0.00	0.00
1104	—	—	—	0.02	0.00
1579	—	—	—	—	0.15

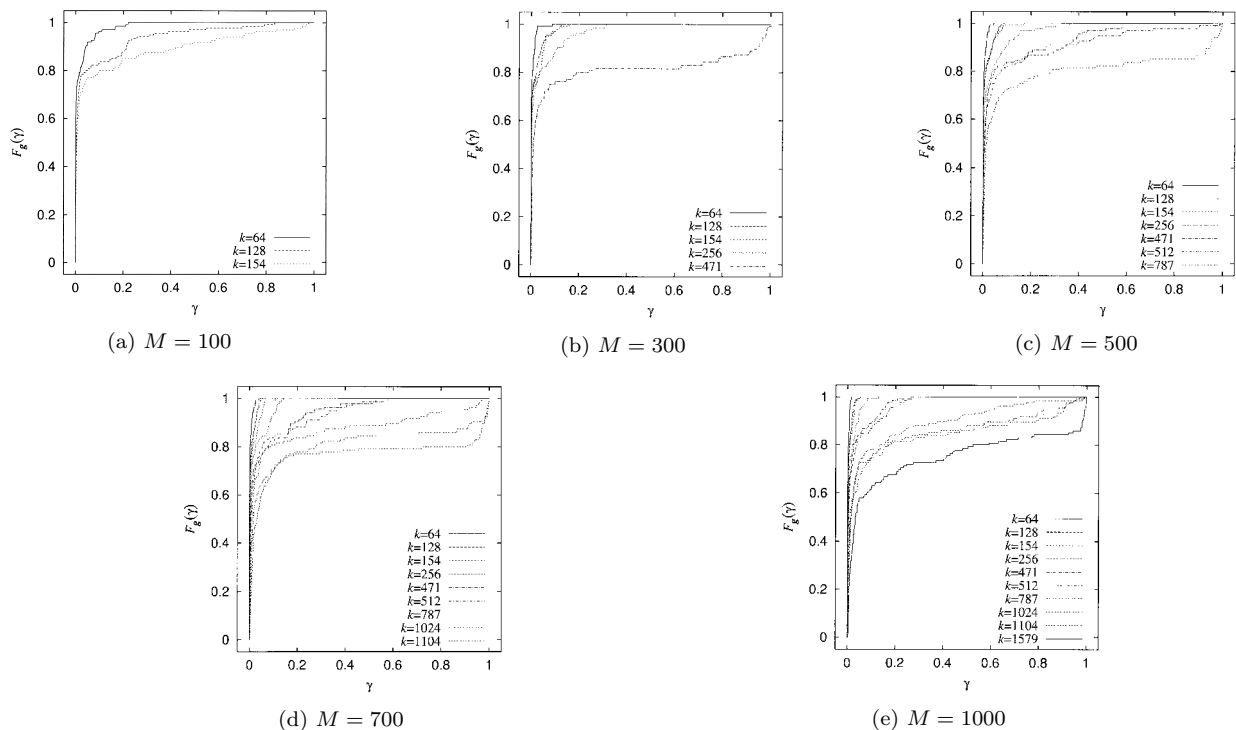


Fig. 6 Sample distribution functions, embedding using CEAW.

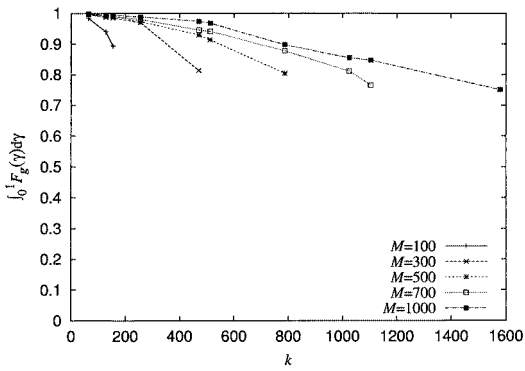


Fig. 7 $\int_0^1 F_g(\gamma) d\gamma$ versus k , embedding using CEAW.

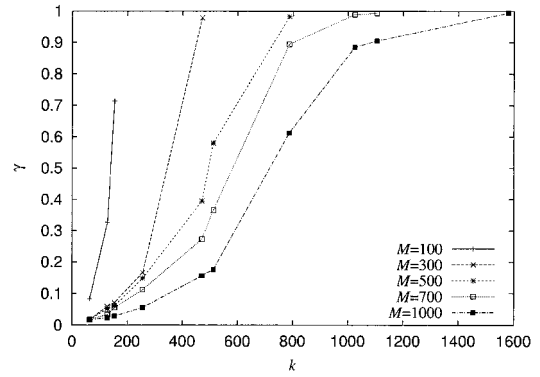


Fig. 8 95th percentile versus k , embedding using CEAW.



Fig. 9 Thirteen of male facial portraits.

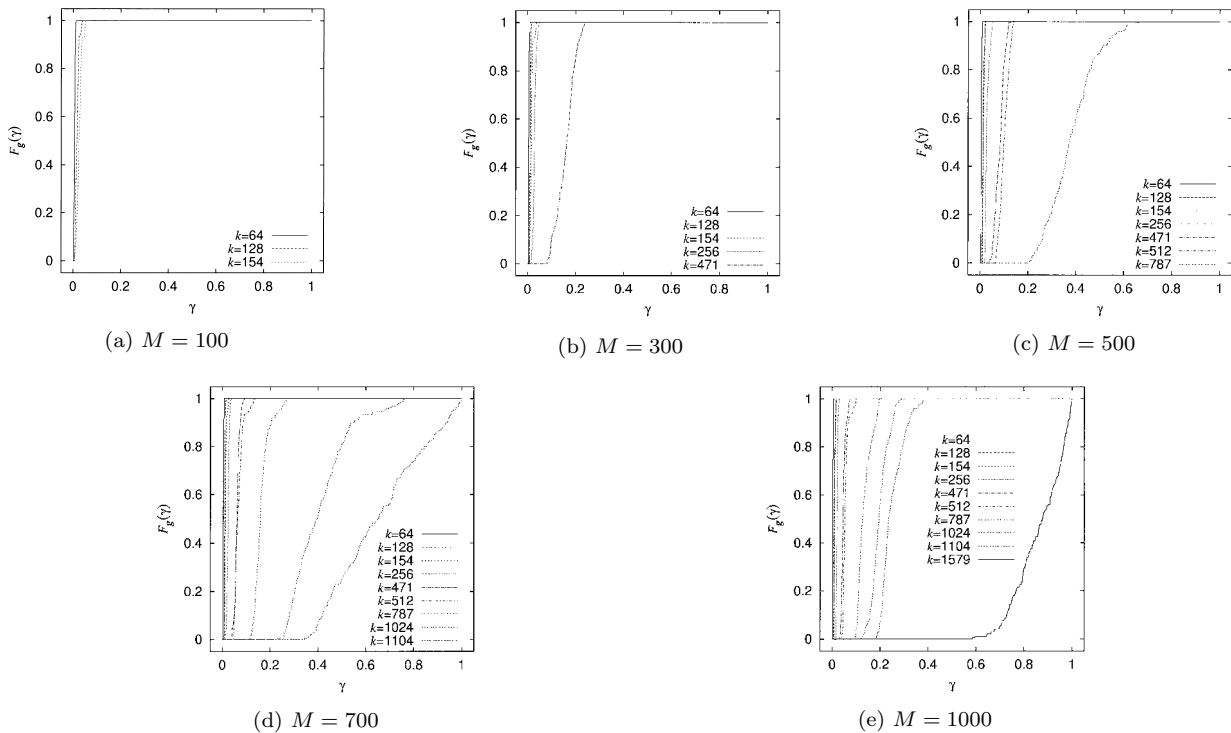


Fig. 10 Sample distribution functions, embedding using SWNCS.

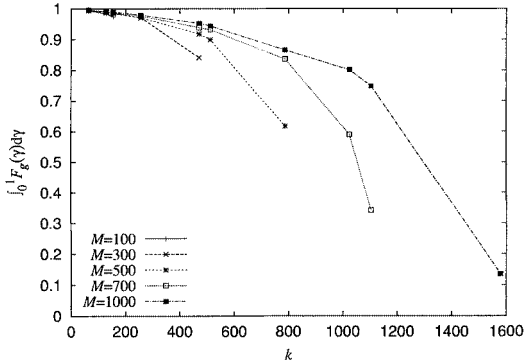


Fig. 11 $\int_0^1 Fg(\gamma)d\gamma$ vs k , embedding using SWNCS.

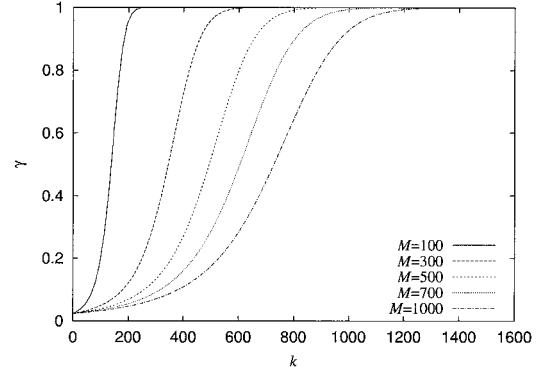


Fig. 13 Approximated unified function for CEAW.

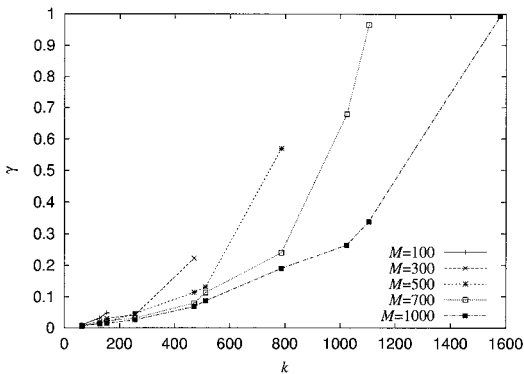


Fig. 12 95th percentile vs k , embedding using SWNCS.

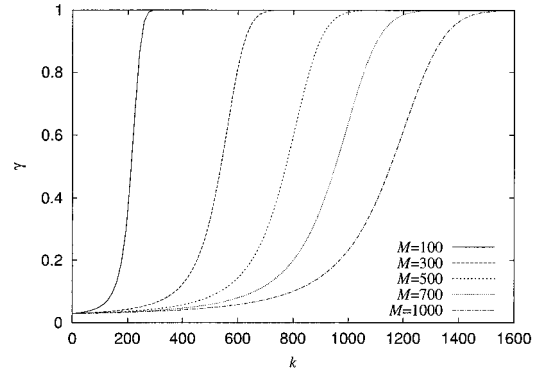


Fig. 14 Approximated unified function for SWNCS.

4.4 Embedding by Simple Watermarking Based on Neighbor Coefficient Statistics [10]

Thirteen of color male portraits depicted in Fig. 9 are used for experiments. Each picture consists of 128×128 pixels and has 256 levels from zero to 255 in each RGB channel. The PSNR is set to 24 [dB] that is enough for a human to identify the cardholder's face with the card's portrait in all the watermarked images. Figure 10 illustrates $Fg(\gamma)$ obtained from the experiments that use the thirteen images mentioned above. Table 4 shows the SERs.

Figures 11 and 12 depict the integral of $Fg(\gamma)$ and 95th percentile of $Fg(\gamma)$. It is considered that 95th percentile is appropriate as a performance index of performance of SWNCS from Table 4, Fig. 11, and Fig. 12.

5. The Minimum Number of Orthogonal Sequences for the Required Amount of Data

Using the 95th percentile considered to be appropriate as a performance index of each watermarking method in Sects. 4.3 and 4.4, let us try to find the unified approximated function for the performance index in each watermarking scheme. Equations (10) and (11) are obtained by means of the least mean square (LMS)

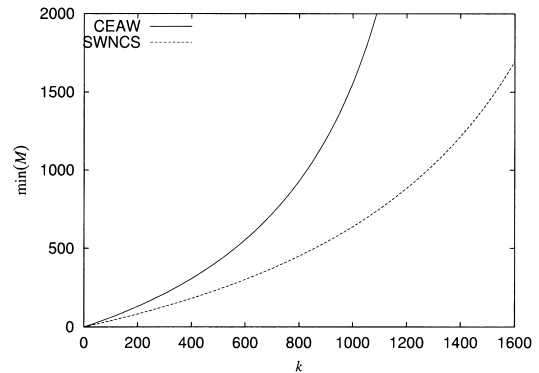


Fig. 15 Minimum M for embedding k -bits data without errors.

method for CEAW and for SWNCS, respectively, and these unified approximated functions below are shown in Fig. 13 and Fig. 14.

$$f(k, M) = \frac{1}{1 + \exp(6.14694 - a)},$$

$$a = \exp(0.885198 + bk),$$

$$b = (0.000669895 + 0.608876/M). \quad (10)$$

$$f(k, M) = \frac{1}{1 + \exp(3.68348 - a)},$$

$$a = \exp(-1.65413 + bk),$$

$$b = (0.00130721 + 1.25756/M). \quad (11)$$

Table 3 and Fig. 8 show that there is no error in CEAW decoding when the 95th percentile is less than 0.7. Therefore, let us consider that the maximum embedding is done in CEAW under the condition that 95th percentile is equal to 0.7. In the same way, Table 4 and Fig. 12 show that there is no error in SWNCS decoding when the 95th percentile is less than 0.8. Therefore, let us consider that the maximum embedding is done in SWNCS under the condition that 95th percentile is equal to 0.8.

Finally, let us try to find the relationship between k and M under the condition that maximum amount of data is embedded in each watermarking method. Figure 15 illustrates the minimum number of M versus k in each watermarking algorithm, and we can get the important knowledge in system design of each watermarking method from Fig. 15.

6. Conclusions

The maximum amounts of embedded information that is important for practical system design in two watermarking methods based on the PC/SS scheme have been discussed in this paper. One is a private watermarking method referred to CEAW that has been also proposed in this paper and has a practical strong point to make the quality of the watermarked image to be constant in any images. The other is a public watermarking method referred to SWNCS that was previously proposed in [7]–[9].

From analyses under the condition that quantization noise is only assumed, the minimum number of orthogonal sequences for embedding the required amount of information is found in each watermarking method.

The effects of other noises and distortions will be investigated as a further work.

Acknowledgement

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

References

- [1] M. Fujiyoshi and T. Hasegawa, "Code energy adaptive watermarking," Proc. 1998 Int'l Symposium on Inf. Theory and its Applications, vol.II, pp.364–367, Mexico City, Mexico, Oct. 14–16, 1998.
- [2] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol.6, no.12, pp.1673–1687, Dec. 1997.
- [3] C.I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," IEEE J. Sel. Areas Commun., vol.16, no.4, pp.525–539, May 1998.
- [4] S. Craver, N. Memon, B.-L. Yeo, and M.M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," IEEE J.

Sel. Areas Commun., vol.16, no.4, pp.573–586, May 1998.

- [5] 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.
- [6] 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.
- [7] M. Fujiyoshi and T. Hasegawa, "A novel individual identification system using the parallel combinatorial spread spectrum," IEICE Technical Report, IT99-93, March 2000.
- [8] M. Fujiyoshi and T. Hasegawa, "A novel individual identification system using a digital watermark technique and its decodeless rejection," Proc. 2000 Int'l Symposium on Inf. Theory and its Applications, vol.II, pp.943–946, Honolulu, HI, USA, Nov. 5–8, 2000.
- [9] M. Fujiyoshi and T. Hasegawa, "A novel individual identification system using a watermarking method based on the parallel combinatorial spread spectrum scheme," IEICE Trans. Fundamentals, vol.E83-A, no.11, pp.2129–2137, Nov. 2000.
- [10] M. Fujiyoshi and T. Hasegawa, "A study on maximum amount of embedded information of simple watermarking based on neighbor coefficient statistics," IEICE Technical Report, SST2000-53, Oct. 2000.



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), Personal Communications and Consumer Communications (Japanese, Baifukan, 1994), and Mobile Computing Textbook (Japanese, ASCII, 1998). He is a member of IEEE and SITA (The Society of Information Theory and its Applications, Japan).