Statistical-mechanical approach for multiple watermarks using spectrum spreading

Kazuhiro Senda and Masaki Kawamura *

Yamaguchi University, 1677–1 Yoshida, Yamaguchi-shi, Yamaguchi Japan
kawamura@sci.yamaguchi-u.ac.jp

Abstract. We formulate the Bayes optimum watermarking decoder and derive sub-optimum decoding algorithms for spread spectrum digital image watermarking. The optimum decoder can be obtained by considering the posterior probability under the Gaussian assumption for noise and attacks. The amount of calculation for the decoder is NP-hard. We, therefore, need to derive sub-optimum decoding algorithms in order to decode the watermarks. The proposed decoders are multiple watermarks decoders that estimate the multiple watermarks at the same time. These methods base on the multi-stage demodulation method and the partial interference cancellation method, which are two of the CDMA multiuser demodulation methods. We apply them to the digital watermarking scheme. When the original image is blind, the image itself is regarded as noise. We, therefore, evaluated bit error rates for both cases that the original image is informed and blind. As a result, we found both of the multi-stage watermark decoder and the partial interference cancellation decoder are effective for watermarking. The latter has better performance than the former.

1 Introduction

Misuse of the digital contents emerge as a social issue. The copyright information attached additional headers of the digital contents does not work well for copyright protection. The digital watermarking is one of the solutions for these problems.

The basic idea of the digital watermarking is that some hidden messages or watermarks are invisibly embedded in digital cover contents. The cover contents are images, video, audio, and so on. There are a lot of embedding schemes. For images, either watermarks are simply embedded by adding the watermarks to the cover content, or the cover content are transformed by discrete cosine transform (DCT) or wavelet transform, and then the watermarks are embedded in its transform domain [1–4]. On the other hand, in order to keep a secret, watermarks are encrypted or spread. The spectrum spreading method is one of

* This work was partially supported by a Grant-in-Aid for Young Scientists (B) No. 21700255, the Yamaguchi University Foundation, research grant from the President of Yamaguchi University, and The Nakajima Foundation. The computer simulation results were obtained using the PC cluster system at Yamaguchi University.

efficient methods with robustness. The maximum likelihood estimation [5, 6] and the maximum a posteriori probability (MAP) estimation [7, 8] have been used on existing methods.

Cox *et al.* [1–3] proposed a method based on the communication model. The watermark sequences are chosen independently according to Gaussian distribution, and then are embedded in spatial or transform domain. Since embedded sequences can be generated by independent and identically distributed [2, 9], *multiple* watermarks can be embedded into the same pixel, since they become almost orthogonal. The phrase "multiple watermarks" in this paper means that some spread messages or watermarks are accumulated on the same pixel. Cox *et al.* [1–3] performed the multiple watermarks by computer simulations. However, no decoder for multiple watermarks has been discussed in theory, because of multi-watermarks interference.

In this paper, we formulate the Bayes optimum watermarking decoder for spread spectrum digital image watermarking. The optimum decoder can be obtained by considering the posterior probability under the condition of the Gaussian assumption for noise and attacks. Unfortunately, the amount of calculation to decode all embedded watermarks is NP-hard. We, therefore, need to derive sub-optimum decoding algorithms. We derive sub-optimum decoding algorithms from the optimum decoder. In this manner, because of theoretical difficulty, we consider simple watermarking model, that watermarks are simply embedded into image domain.

We consider decoding algorithms for the spectrum spreading method. This method is also now used in Code Division Multiple Access (CDMA)[10–13]. In the CDMA, more than one user can transmit their information at the same time and within the same cell. Therefore, multiuser interference need to be considered for the CDMA multiuser demodulator problem. Recently Bayes optimum solutions have been proposed on statistical mechanics. The maximum posterior marginal (MPM) estimation is the Bayes optimum [14]. Tanaka has evaluated this problem by the replica method [14–16]. The demodulation methods of CDMA have been proposed by applying a dynamical theory of Hopfield model [17–19]. As in the case of CDMA, statistical-mechanical approaches are progressing in several fields, e.g., image restoration [20, 21], coding theory [22, 23], rate distortion [24], etc. Now, we are addressing theoretical analysis of the digital watermarking model. It is important for the digital watermarking to model, formulate, and derive decoding methods.

By applying the demodulation methods of CDMA to watermarking, multiple watermarks can be decoded simultaneously. Moreover, since multi-watermarks interference can be reduced, bit error rate for watermarks will be improved. From a theoretical viewpoint, distinction between CDMA and watermarking is on assumptions for noises. Channel noise in the CDMA is usually assumed to be independent or thermal noise. In the watermarking, artificial noises occur by illegal users. They are correlated noises, e.g., image noise, block-noise, and distortion. Although the assumption for noises should not intrinsically be Gaussian, almost all of cases would be intractable. Moreover, when the type of attacks

might be blind, we could not formulate its model. Therefore, we have no other choice but to assume the Gaussian assumption. Then, we evaluate decoding performance of the proposed decoders by simulations and theory.

Section 2 outlines our watermarking model. Section 3 describes the Bayes optimum decoder for multiple watermarks, and drive computable multiple decoders in Sec. 4. Section 5 shows results obtained by theory and computer simulations. Section 6 concludes our methods.

2 Mathematical Model of Watermarking

2.1 Embedding Procedure

A gray scale image is divided into N pixels per a block. We don't mind how to divide it if there are no overlaps between blocks. For example, each block may consist of 8×8 pixels, or 64×1 pixels by raster scanning. We only assume the block length stays constant for all blocks. Since each block is processed in turn, we refer only to one block in detail.

Image block consisted of N pixels is represented as $\boldsymbol{I} = (I_1, I_2, \cdots, I_N)^T$. Hereinafter, we refer to this image block as just image. K-bit messages $\boldsymbol{s} = (s_1, s_2, \cdots, s_K)^T$ are embedded to original image in layers, where $s_i = \pm 1$. The diagram of embedding procedure is shown in Fig. 1. The each bit of messages, s_i, is spread by specific spreading code $\boldsymbol{\xi}_i = (\xi_i^1, \xi_i^2, \cdots, \xi_i^N)^T$. The chip rate or length of the spreading codes is equal to N. The each elements of spreading codes ξ_i^μ takes ± 1 with probability

$$P\left[\xi_i^\mu = \pm 1\right] = \frac{1}{2}. \tag{1}$$

Here, we notice $(\xi_i^\mu)^2 = 1$. The spreading codes are usually generated by PN sequence generator. We do not mind their generating methods as long as they satisfy (1).

A watermark to be embedded at the μth pixel, w_μ, is represented by

$$w_\mu = \sum_{i=1}^{K} \xi_i^\mu s_i \ , \quad \mu = 1, 2, \cdots, N, \tag{2}$$

which is sum of spread messages. The stego image $\boldsymbol{X}$ is made by adding the watermarks $\boldsymbol{w} = (w_1, w_2, \cdots, w_N)^T$ to the original image $\boldsymbol{I}$, that is,

$$X_\mu = F_0\left(I_\mu + w_\mu\right) \tag{3}$$

$$\simeq I_\mu + w_\mu + n_{0\mu}, \tag{4}$$

where a function F_0 is the function which limits each pixel value to interval $[0, 255]$. We assume embedding error can be represented as noise $n_{0\mu}$ by linear approximation. In this way, the stego image $\boldsymbol{X}$ is generated and is distributed widely.

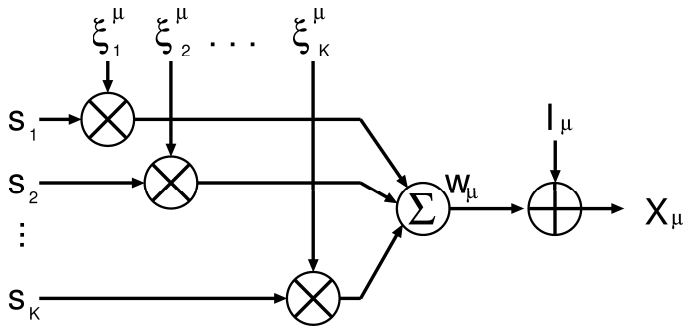


Fig. 1. Diagram of spreading and multiplexing of embedded watermarks.

2.2 Attack

The stego image $\boldsymbol{X}$ is usually attacked by illegal users. The attacks by lossy compression, band-pass filter, geometrical distortion etc. are represented as noises. Since there are a lot of different kinds of attacks, we should intrinsically consider each case of the attacks. These effects cannot be represented as Gaussian distributions. Even if we can represent them by specific distributions, they may be intractable for many cases. Considering we want to formulate the Bayes optimum decoder, we can introduce the Gaussian assumption. This case is on good condition for decoder. So, now tampered stego image $\widetilde{\boldsymbol{X}}$ is given by

$$\widetilde{X}_\mu = X_\mu + n_{1\mu}. \tag{5}$$

From (4), by combining the noise $n_{0\mu}$ and $n_{1\mu}$, we obtain

$$\widetilde{X}_\mu = I_\mu + w_\mu + n_\mu, \tag{6}$$
$$n_\mu = n_{0\mu} + n_{1\mu}. \tag{7}$$

In the following discussions, we assume that noise n_μ obeys the Gaussian distribution $\mathcal{N}(0, \sigma_s^2)$ and the noise is independent of both the original image I_μ and the watermark w_μ.

2.3 Informed Decoder

The watermarks are decoded from the tampered image. When the original image is known, extracted information r_μ is calculated by subtracting the original image I_μ from the tampered image $\widetilde{X}_\mu$, that is,

$$r_\mu = \widetilde{X}_\mu - I_\mu, \tag{8}$$
$$= w_\mu + n_\mu. \tag{9}$$

By multiplying r_μ by the corresponding spreading code $\boldsymbol{\xi}_i$, the output of correlator, h_i, is given by

$$h_i = \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu r_\mu \tag{10}$$

$$= s_i + \frac{1}{N}\sum_{\mu=1}^{N}\sum_{j\neq i}^{K} \xi_i^\mu \xi_j^\mu s_j + \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu n_\mu, \tag{11}$$

where the second term of right-hand side in (11) is multi-watermarks interference term and the third one is the noise term. Then, the estimate value of ith watermark, $\hat{s}_i$, is given by

$$\hat{s}_i = \mathrm{sgn}\left(h_i\right), \tag{12}$$

where a function $\mathrm{sgn}(h)$ is the signum function given by

$$\mathrm{sgn}(h) = \begin{cases} +1, & h \geqq 0 \\ -1, & h < 0 \end{cases}. \tag{13}$$

The method that each watermark is independently estimated is called a single decoder like a single-user demodulator in CDMA.

2.4 Blind Decoder

When the original image is unknown or blind, there are two ways to decode the watermarks: direct inference without estimating the original image and double inference with estimating the original image and watermarks. In the former case, the tampered image $\widetilde{X}_\mu$ itself becomes the extracted information r_μ, that is,

$$r_\mu = \widetilde{X}_\mu \tag{14}$$

$$= w_\mu + n_\mu + I_\mu. \tag{15}$$

The output of correlator, h_i, becomes

$$h_i = \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu r_\mu \tag{16}$$

$$= s_i + \frac{1}{N}\sum_{\mu=1}^{N}\sum_{j\neq i}^{K} \xi_i^\mu \xi_j^\mu s_j + \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu n_\mu + \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu I_\mu, \tag{17}$$

where the fourth term in (17), which differs from (11), is image noise term. Since I_μ takes larger value than value of watermarks, it is hard to estimate the watermarks properly.

As the other method, we can infer an estimated image from the tampered image $\widetilde{X}_\mu$. The estimated image $\hat{I}_\mu$ can be reconstructed by some filtering and so

on. Then, the extracted information r_μ is calculated by subtracting the estimated image $\hat{I}_\mu$ from the tampered image $\widetilde{X}_\mu$, and is given by

$$r_\mu = \widetilde{X}_\mu - \hat{I}_\mu \tag{18}$$

$$= w_\mu + n_\mu + I_\mu - \hat{I}_\mu. \tag{19}$$

Therefore, the output of correlator, h_i, becomes

$$h_i = \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu r_\mu \tag{20}$$

$$= s_i + \frac{1}{N}\sum_{\mu=1}^{N}\sum_{j\neq i}^{K} \xi_i^\mu \xi_j^\mu s_j + \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu n_\mu + \frac{1}{N}\sum_{\mu=1}^{N} \xi_i^\mu \left(I_\mu - \hat{I}_\mu\right). \tag{21}$$

Whenever the estimated image $\hat{I}_\mu$ is similar enough to the original image I_μ, the image noise term of (21) can be reduced.

3 Optimum Multiple Watermarks Decoder

Since 1-bit message is spread by N-bits spreading codes, the embedded capacity or payload decreases to $1/N$. On the other hand, by spreading the messages, more than one messages can be embedded at the same pixel in piles. In this case, multi-watermarks interference cannot be eliminated. We, therefore, consider how to eliminate this interference.

The multi-watermarks interference term consists of messages s_i and their corresponding spreading codes $\boldsymbol{\xi}_i$. The spreading codes are available for owner, but information regarding the messages is blind. Therefore, the effect of the interference term can be decreased by using both estimated messages $\hat{\boldsymbol{s}}$ and the spreading codes $\boldsymbol{\xi}_i$. Multiple watermark decoders such that all estimated messages are used to infer them simultaneously corresponds to the multiuser demodulators method in CDMA [14–16]. The Bayes optimum decoder can eliminate the multi-watermarks interference. Now we formulate multiple watermarks decoder under the Gaussian assumption. Let us start to calculate the posterior probability of messages $\boldsymbol{s}$, given the extracted information $\boldsymbol{r}$.

3.1 Posterior Probability

In the multiple watermarks decoder, we start to obtain the posterior probability. Since the estimated image $\hat{I}_\mu$ can be reconstructed by mean filter or Wiener filter and we guess it is similar enough to the original one, we assume the original image is informed for simplicity. From (2) and (19), the noise term becomes

$$n_\mu = r_\mu - \sum_{i=1}^{K} \xi_i^\mu s_i, \tag{22}$$

and obeys Gaussian distribution,

$$P\left(n_\mu\right) = \frac{1}{\sqrt{2\pi\sigma_s^2}} \exp\left[-\frac{\left(n_\mu\right)^2}{2\sigma_s^2}\right]. \tag{23}$$

The conditional probability of the extracted information $\boldsymbol{r}$, given the true messages $\boldsymbol{s}$, is given by

$$P\left(\boldsymbol{r}|\boldsymbol{s}\right) = \prod_{\mu=1}^{N} P\left(r_\mu|\boldsymbol{s},\boldsymbol{\xi}\right) \tag{24}$$

$$\propto \exp\left[-\frac{\beta_s}{2N}\sum_{\mu=1}^{N}\left(r_\mu - \sum_{i=1}^{K}\xi_i^\mu s_i\right)^2\right], \tag{25}$$

where $\sigma_s^2 = N/\beta_s$. From Bayes' theorem, the posterior probability of messages $\boldsymbol{s}$, given the extracted information $\boldsymbol{r}$, is given by

$$P\left(\boldsymbol{s}|\boldsymbol{r}\right) = \frac{P\left(\boldsymbol{r}|\boldsymbol{s}\right)P\left(\boldsymbol{s}\right)}{P(\boldsymbol{r})} \tag{26}$$

$$= \frac{P\left(\boldsymbol{r}|\boldsymbol{s}\right)P\left(\boldsymbol{s}\right)}{\sum_{\boldsymbol{x}} P\left(\boldsymbol{r}|\boldsymbol{x}\right)P\left(\boldsymbol{x}\right)}. \tag{27}$$

The prior probability of the messages, $P(\boldsymbol{s})$, is assumed to be uniform distribution, that is,

$$P(\boldsymbol{s}) = 2^{-K}. \tag{28}$$

Therefore, the posterior probability is given by

$$P\left(\boldsymbol{s}|\boldsymbol{r}\right) = \frac{P(\boldsymbol{s})}{Z(\boldsymbol{r})}\exp\left[-\frac{\beta}{2N}\sum_{\mu=1}^{N}\left(r_\mu - \sum_{i=1}^{K}\xi_i^\mu s_i\right)^2\right], \tag{29}$$

where we set in a parameter β instead of true parameter β_s, since true parameter is unknown for decoder. And also $Z(\boldsymbol{r})$ is defined as

$$Z(\boldsymbol{r}) = \sum_{\boldsymbol{s}} P(\boldsymbol{s})\exp\left[-\frac{\beta}{2N}\sum_{\mu=1}^{N}\left(r_\mu - \sum_{i=1}^{K}\xi_i^\mu s_i\right)^2\right], \tag{30}$$

where summation over $\boldsymbol{s}$ is defined as

$$\sum_{\boldsymbol{s}} = \sum_{s_1=\pm 1}\sum_{s_2=\pm 1}\cdots\sum_{s_K=\pm 1}. \tag{31}$$

Therefore, the performance of the multiple watermark decoder can be evaluated as the multiuser demodulators in CDMA [14–16]. The maximum a posteriori

(MAP) estimation and maximum posterior marginal (MPM) estimation can be applied to infer the messages $\boldsymbol{s}$. The estimated values by the MAP and MPM estimations are given by

$$\hat{\boldsymbol{s}}^{\mathrm{MAP}} = \arg\max_{\boldsymbol{s}} P\left(\boldsymbol{s}|\boldsymbol{r}\right), \tag{32}$$

$$\hat{s}_i^{\mathrm{MPM}} = \arg\max_{s_i} P\left(s_i|\boldsymbol{r}\right), \tag{33}$$

where probability $P\left(s_i|\boldsymbol{r}\right)$ is a marginal probability given by

$$P\left(s_i|\boldsymbol{r}\right) = \sum_{\boldsymbol{s}\setminus s_i} P\left(\boldsymbol{s}|\boldsymbol{r}\right), \tag{34}$$

where summation $\sum_{\boldsymbol{s}\setminus s_i}$ is summation over $\boldsymbol{s}$ excepting s_i and is defined as

$$\sum_{\boldsymbol{s}\setminus s_i} = \sum_{s_1=\pm 1} \cdots \sum_{s_{i-1}=\pm 1} \sum_{s_{i+1}=\pm 1} \cdots \sum_{s_K=\pm 1}. \tag{35}$$

The MPM estimation is to find the code which maximizes marginal posterior probability $P\left(s_i|\boldsymbol{r}\right)$.

The MPM estimation is Bayes' optimum estimation [14]. We, therefore, consider decoding algorithm inferring the messages $\boldsymbol{s}$ by the MPM estimation. From (33), estimated messages $\hat{s}_i^{\mathrm{MPM}}$ can be calculated by

$$\hat{s}_i^{\mathrm{MPM}} = \mathrm{sgn}\left(\sum_{s_i=\pm 1} s_i P\left(s_i|\boldsymbol{r}\right)\right) \tag{36}$$

$$= \mathrm{sgn}\left(\langle s_i \rangle\right), \tag{37}$$

where $\langle s_i \rangle$ is average over the posteriori distribution and is defined as

$$\langle s_i \rangle = \frac{\sum_{s_i=\pm 1} s_i P\left(s_i|\boldsymbol{r}\right)}{\sum_{s_i=\pm 1} P\left(s_i|\boldsymbol{r}\right)}. \tag{38}$$

As mentioned above, we could formulate the Bayes optimum multiple watermarks decoder.

The estimation error is measured by the bit error rate P_b, which is defined as

$$P_b = \frac{1-M}{2}, \tag{39}$$

where M is a overlap or degree of coincidence between the true messages s_i and the estimated messages $\hat{s}_i$, and is defined as

$$M = \frac{1}{K}\sum_{i=1}^{K} s_i \hat{s}_i. \tag{40}$$

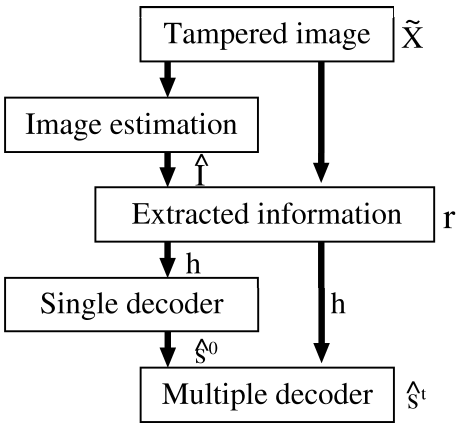


Fig. 2. Decoding procedure for multiple watermarks.

The MPM estimation is optimum, but unfortunately its computational complexity is NP-hard in the number of messages. Its proof is given by the case of CDMA [10]. In other words, if one decoded watermarks using (37), enormous number of computational time might be required in order to calculate the posteriori probability. Therefore, dynamics or computation algorithm such that it achieves one of optimum or sub-optimum solutions should be considered.

4 Decoding Procedure

We propose multiple watermark decoders on the basis of the Bayes optimum decoder. Decoding procedure is shown in Fig. 2. We obtain the extracted information r_μ by (18) using the estimated image $\hat{I}_\mu$, whose image is reconstructed by mean filter. Then, the output of correlator, h_i, is obtained by (20). At the initial states, the estimated message $\hat{s}_i^0$ is given using the single decoder by

$$\hat{s}_i^0 = \mathrm{sgn}\left(h_i\right). \tag{41}$$

Next, we consider how to reduce the multi-watermarks interference. Since the optimum decoder is hard to compute, we need step-by-step algorithms whose computational time is relatively small.

4.1 Multiple watermark decoders

From (29), we obtain the posterior probability in the form of Hamiltonian or energy function, $H(\boldsymbol{s})$:

$$P\left(\boldsymbol{s}|\boldsymbol{r}\right) \propto \exp\left[-\beta H(\boldsymbol{s})\right], \tag{42}$$

$$H(\boldsymbol{s}) = \frac{1}{2}\sum_{i=1}^{K}\sum_{j=1}^{K} J_{ij}s_i s_j - \sum_{i=1}^{K} h_i s_i, \tag{43}$$

where J_{ij} is defined as

$$J_{ij} = \frac{1}{N} \sum_{\mu=1}^{N} \xi_i^\mu \xi_j^\mu . \tag{44}$$

According to (32) and (33), maximizing the posterior probability $P(\boldsymbol{s}|\boldsymbol{r})$ corresponds to minimize the Hamiltonian $H(\boldsymbol{s})$. We, therefore, obtain following equation by the steepest descent method,

$$-\frac{\partial H(\boldsymbol{s})}{\partial s_i} = h_i - \sum_{j \neq i}^{K} J_{ij} s_j . \tag{45}$$

The steepest descent method can find one of optimum or sub-optimum solutions, since it stops at the local minimum.

We consider discrete dynamics, and introduce the multistage watermark decoder is obtained by

$$\hat{s}_i^{t+1} = \mathrm{sgn}\left(h_i - \sum_{j \neq i}^{K} J_{ij} \hat{s}_j^t \right), \tag{46}$$

where $\hat{s}_i^t$ represents estimated message at the t-th stage. This basic idea has been appeared in the CDMA multiuser demodulation problem as a multistage demodulator [11, 12, 18].

The reliability of estimation for early stages in the multistage watermark decoder (46) is low due to noises and use of the single decoder. Therefore, a interference cancellation parameter P_t is introduced to the multi-watermarks interference term. The partial interference cancellation method is proposed in the CDMA [13, 25–28]. The parameter P_t takes initially small value, and then it becomes large value with time for increasing reliability. The estimated message at the $(t+1)$th stage, $\hat{s}_i^{t+1}$, in the partial interference cancellation decoder is given by

$$\hat{s}_i^{t+1} = \mathrm{sgn}\left(h_i - P_t \sum_{j \neq i}^{K} J_{ij} \hat{s}_j^t \right). \tag{47}$$

At the initial stage, $\hat{s}_i^0$ is given by (41). When we put $P_t = 1$ for all stage, it is equivalent to the multistage watermark decoder (46).

4.2 Theory

In the CDMA, the performance of the partial interference cancellation method is analyzed under the assumption that noises obey Gaussian distribution by the statistical mechanics [18, 19]. Mizutani *el al.*[18] proposed a decoding algorithm assuming that the last one step correlation between stages is only effective, and correlations between other stages can be ignored.

According to the CDMA, we analyze the performance for multiple watermarks estimation. The variance of the noise is σ_s^2. We consider the large-system limit $K \to \infty$ and $N \to \infty$, while the ratio $\beta \equiv K/N$ is kept finite. We define variance V as sum of the variance of the noise, σ_s^2, and the ratio β:

$$V = \beta + \sigma_s^2. \tag{48}$$

Under the random spreading assumption and the large-system limit, we redefine the bit error rate as P_b^{t+1} for time evolution. The value of P_b^{t+1} is to be evaluated by the following recursive formulas:

$$M_{t+1} = \sum_{\lambda=\pm 1} \frac{1+\lambda M_{t-1}}{2} \mathrm{erf}\left(\frac{1-(1-\lambda P_{t-1})P_t U_t}{\sqrt{2V_t^2}}\right), \tag{49}$$

$$V_t^2 = V - 2P_t C_t + P_t^2 S_t^2, \tag{50}$$

$$U_{t+1} = \beta \sum_{\lambda=\pm 1} \frac{1+\lambda M_{t-1}}{\sqrt{2\pi V_t^2}} \exp\left[-\frac{\{1-(1-P_{t-1}\lambda)P_t U_t\}^2}{2V_t^2}\right], \tag{51}$$

$$C_t = \beta M_t + U_t\left(V - P_{t-1}C_{t-1}\right), \tag{52}$$

$$S_t^2 = \beta + U_t^2 V_{t-1}^2 + 2\beta U_t M_t\left(1 - P_{t-1}M_{t-1}\right), \tag{53}$$

where $\mathrm{erf}(x)$ is the error function, which is defined as

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \exp\left[-u^2\right] du. \tag{54}$$

For the initial stage $t = 0$, equations are given by

$$M_{-1} = C_{-1} = S_{-1}^2 = 0, \tag{55}$$

$$M_0 = \mathrm{erf}\left(\frac{1}{\sqrt{2V_{-1}^2}}\right), \tag{56}$$

$$U_0 = \beta\sqrt{\frac{2}{\pi V_{-1}^2}} \exp\left[-\frac{1}{2V_{-1}^2}\right], \tag{57}$$

$$M_1 = \mathrm{erf}\left(\frac{1-P_0U_0}{\sqrt{2V_0^2}}\right), \tag{58}$$

$$U_1 = \beta\sqrt{\frac{2}{\pi V_0^2}} \exp\left[-\frac{(1-P_0U_0)^2}{2V_0^2}\right]. \tag{59}$$

The parameter P_t for the partial interference cancellation decoder is given by

$$P_t = \frac{U_t V(P_{t-1}+1) - C_t}{U_t C_t(P_{t-1}+1) - S_t^2}, \tag{60}$$

and for the multistage watermark decoder it is $P_t = 1$. For the detailed derivation, refer to [18].

5 Simulation Results

We proposed the decoding algorithms for multiple watermarks using spreading codes. In order to evaluate the performance of the multistage watermark decoder and the partial interference cancellation decoder, we analyze the bit error rate P_b for number of multiple K using SIDBA GIRL. The length of the spreading codes is $N = 256 \times 1$, and the variance of noise is $\sigma_s^2 = 64$, i.e., the noise obeys the Gaussian distribution $\mathcal{N}(0, \sigma_s^2)$.

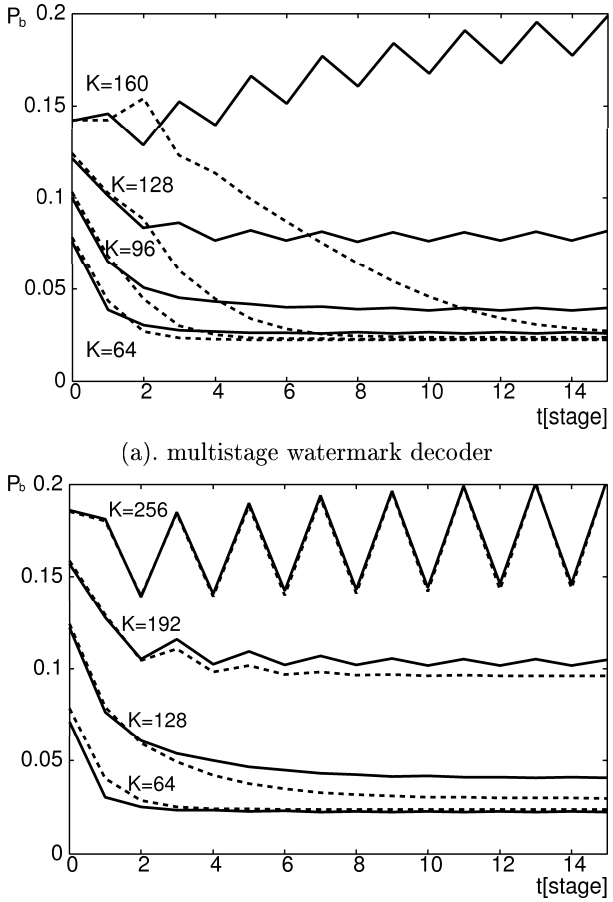
5.1 Results for informed decoder

In the case that the original image is known and attacks can be AWGN, the bit error rate P_b is evaluated. Figure 3 shows P_b for stage t. Solid lines in Fig. 3 (a) represent results obtained by computer simulations of the multistage watermark decoder. Broken lines represent theoretical values by time evolutions of equations (49)–(53), where $P_t = 1$. The result of initial stage denoted by $t = 0$ is obtained by the single decoder. From Fig.3 (a), the multistage watermark decoder improves the bit error rate rather than the single decoder for $K = 128$ or less. For $K = 160$, the single decoder gives better result, since estimation error becomes large due to iterative calculation.

Solid lines in Fig. 3 (b) represent results obtained by computer simulations of the partial interference cancellation decoder. Broken lines represent theoretical values by time evolutions of equations (49)–(53), where P_t is given by (60). The result of initial stage denoted by $t = 0$ is obtained by the single decoder. From Fig.3 (b), the partial interference cancellation decoder improves the bit error rate rather than the single decoder for $K = 192$ or less. For $K = 256$, it cannot improve because of estimation error. Comparing these two decoders, the partial interference cancellation decoder has better ability than the multistage watermark decoder, since the interference cancellation parameter P_t is introduced.

5.2 Results for blind decoder

In the case that the original image is blind, the bit error rate P_b is evaluated. We apply mean filter to the tampered image in order to obtain estimated image $\hat{\boldsymbol{I}}$. Figure 4 shows the bit error rate P_b for stage t, using the partial interference cancellation decoder. Figure 4 (a) shows results of the case that no estimated image is used, i.e., the extracted information is $r_\mu = \widetilde{X}_\mu$ from (14). Figure 4 (b) shows results using the estimated image $\hat{\boldsymbol{I}}$, i.e., $r_\mu = \widetilde{X}_\mu - \hat{I}_\mu$ from (18). Solid lines represent results obtained by computer simulations, and broken lines represent theoretical values by time evolutions of equations (49)–(53), where P_t is given by (60). Since we take into account the one step correlation in theory in 4.2, these results agree for the first few steps. Without estimated image, the performance of the partial interference cancellation decoder becomes worse than the single decoder in steps. This reason is that estimation error becomes large due to iterative calculation. Because of using the estimated image, it keeps a good performance.



(a). multistage watermark decoder

(b). partial interference cancellation decoder

Fig. 3. Bit error rate P_b for stage t in case of original image is known, where (a). $K = 64, 96, 128, 160$ and (b). $K = 64, 128, 192, 256$. Solid and broken lines represent results by computer simulations and theory, respectively.

Table 1. Bit error rate P_b at stage $t = 0$ (single decoder) and $t = 14$ (multiple decoder).

	Girl		Moon		Aerial		Facs		Title	
	$t = 0$	$t = 14$	$t = 0$	$t = 14$	$t = 0$	$t = 14$	$t = 0$	$t = 14$	$t = 0$	$t = 14$
$K = 8$	0.075	0.068	0.085	0.080	0.150	0.150	0.190	0.181	0.364	0.379^*
$K = 64$	0.117	0.091	0.128	0.106	0.186	0.175	0.210	0.203	0.366	0.430^*
$K = 96$	0.140	0.113	0.153	0.126	0.201	0.189	0.227	0.234^*	0.368	0.445^*
$K = 128$	0.162	0.130	0.167	0.139	0.213	0.223^*	0.240	0.262^*	0.368	0.446^*

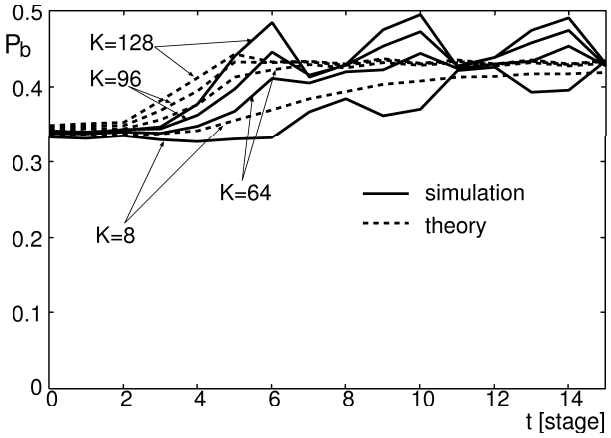
We also evaluate our method by others images; SIDBA Moon, Aerial, Facs, and Title. Figure 5 shows results for these images by computer simulations using estimated images and by theory of partial interference cancellation decoder, and Table 1 shows the bit error rate P_b at stage $t = 0$ for the single decoder and at stage $t = 14$ for the multiple decoder by computer simulations. In cases when the results by the multiple decoder become worse than those by the single decoder, we put mark * on values. For low load case, namely, small K, the multiple decoder improve the bit error rate. Since we use mean filter, the performance for natural images, e.g., Moon and Aerial, is better than artificial ones which have lots of edges. The result for Title in Fig.5 (d) shows the worst case. Brightness of the image takes 0 and 255 in many pixels, and then embedding errors have been occurred. However, for many images, multiple watermarks decoder is effective as estimated image in terms of the bit error rate.

6 Conclusions

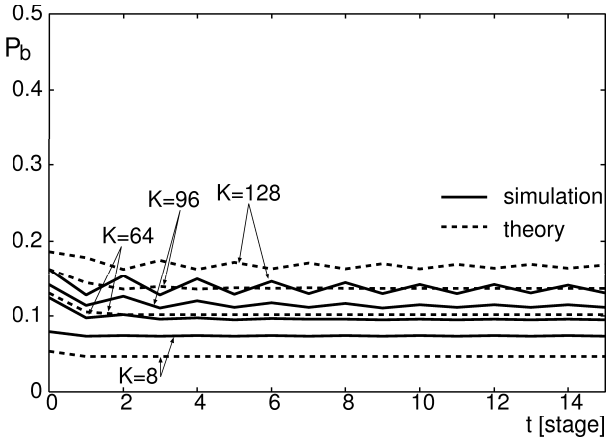
By spreading watermarks using spreading codes, the watermarks can be concealed, and they can also have error correcting capability. Although the payload decreases to $1/N$ without multiplexing, multiple watermarks can be embedded at the same pixel. We considered the decoding algorithms for multiple watermarks, and evaluated their performances using the bit error rate.

For multiple watermarks, the problem is how to estimate all messages simultaneously. We formulate the Bayes optimum decoder under the Gaussian assumption. Since the optimum decoder is NP-hard, We derive dynamics or computation algorithms as multiple watermarks decoders. We introduced the multistage watermark decoder and the partial interference cancellation decoder for watermarking. Since watermarks are embedded in an image, image noise needs to be taken into account in the blind case. Therefore, we analyzed both cases that original image is informed and blind. We reconstructed estimated image by using mean filter.

When the original image is informed, the partial interference cancellation decoder is better than the multistage watermark decoder, and both two decoders are better than the single decoder. When the bit error rate of the initial stage is large, estimation error may become large. When the original image is unknown or blind, the partial interference cancellation decoder is not effective without

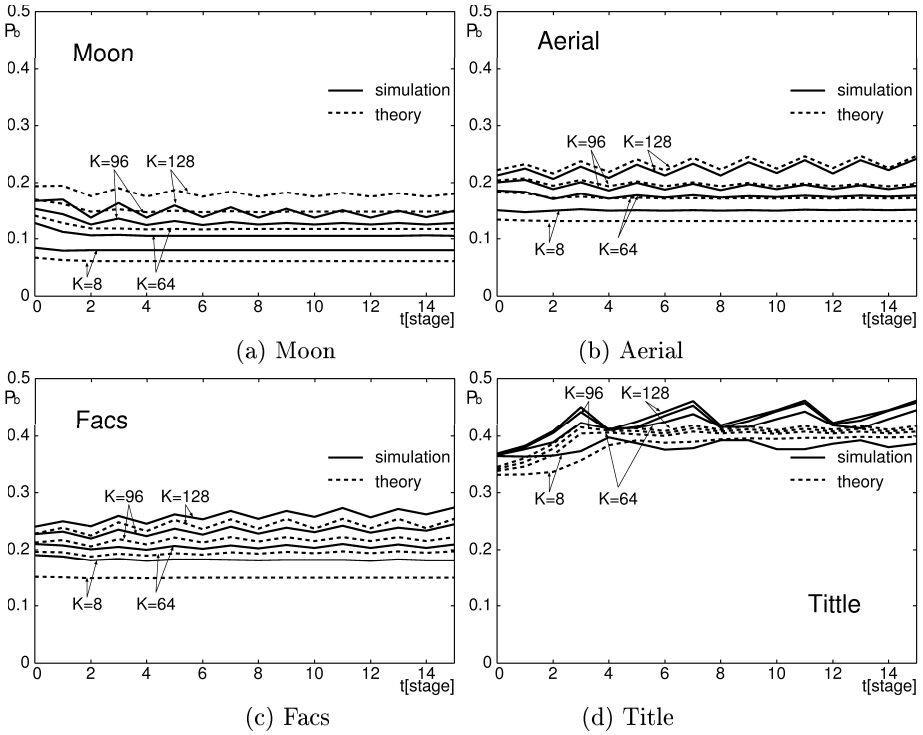


(a). case without estimated image: $\boldsymbol{r} = \widetilde{\boldsymbol{X}}$



(b). case with estimated image: $\boldsymbol{r} = \widetilde{\boldsymbol{X}} - \hat{\boldsymbol{I}}$

Fig. 4. Bit error rate P_b for stage t in case of original image is blind, (a). in case without estimated image, and (b). in case with estimated image. Solid and broken lines represent results by computer simulations and theory, respectively, where $K = 8, 64, 96, 128$.



(a) Moon (b) Aerial

(c) Facs (d) Title

Fig. 5. Bit error rate P_b in case with estimated image for various images; (a) Moon, (b) Aerial, (c) Facs, and (d) Title. Solid and broken lines represent results by computer simulations and theory, respectively, where $K = 8, 64, 96, 128$.

estimated image. However, using the estimated image, which is reconstructed by mean filter, the performance by the decoder can be improved enough.

We consider a simple watermarking model in order to discuss optimum or sub-optimum decoders. For practical use, more elaborate procedure is required as we all know. For statistical-mechanical approach, these cases are interesting problems.

References

1. Cox, I. J., Kilian, J., Leighton, T., and Shamoon, T.: Secure spread spectrum watermarking for images, audio and video. IEEE Int. Conf. Image Processing 3, 243–246 (1996)
2. Cox, I. J., Kilian, J., Leighton, T., and Shamoon, T.: Secure spread spectrum watermarking for multimedia. IEEE Trans. Image Processing. 6 (12), 1673–1687 (1997)
3. Cox, I. J., Miller, M., Bloom, J.A., Fridrich, J., and Kalker, T.: Digital Watermarking and Steganography, 2nd Ed., Morgan Kaufmann (2007)

4. Ruanaidh, J. J. K. Ó, and Pun, T.: Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal Processing 66, 303–317 (1998)
5. Hernández, J. R., and González, F. P.: Statistical analysis of watermarking schemes for copyright protection of images. Proc. IEEE 87 (7), 1142–1166 (1999)
6. Su, J., Hartung, F., and Girod, B.: A channel model for a watermark attack. Proc. SPIE Security and Watermarking of Multimedia Contents 3657, 159–170 (1999)
7. Kutter, M., Voloshynovskiy, S., and Herrigel, A.; Watermark copy attack. Proc. SPIE Security and Watermarking of Multimedia Contents 3971, 371–380 (2000)
8. Voloshynovskiy, S., Herrigel, A., Baumgaertner, N., and Pun, T.: A stochastic approach to content adaptive digital image watermarking. Inter. Workshop Inform. Hiding, Springer Berlin / Heidelberg, LNCS 1768, 211–236 (2000)
9. Wong, P. H. W., Au, C., and Yeung, Y. M.: A novel blind multiple watermarking technique for images. IEEE Trans. Circuits Syst. Video Technol. 13 (8), 813–830 (2003)
10. Verdú, S.: Computational complexity of optimum multiuser detection. Algorithmica 4 (1), 303–312 (1989)
11. Varanasi, M. K., and Aazhang, B.: Multistage detection in asynchronous code-division multiple-access communications. IEEE Trans. Commun. 38, 509–519 (1990)
12. Varanasi, M. K., and Aazhang, B.: Near-optimum detection in synchronous code-division multiple-access systems. IEEE Trans. Commun. 39, 725–736 (2001)
13. Divsalar, D., Simon, M. K., and Raphelli, D.: Improved parallel interference cancellation for CDMA. IEEE Trans. Commun. 46 (2), 258–268 (1998)
14. Tanaka, T.: A statistical-mechanics approach to large-system analysis of CDMA multiuser detectors. IEEE Trans. Info. Theory 48 (11), 2888–2910 (2002)
15. Tanaka, T.: Statistical mechanics of CDMA multiuser demodulation. Europhys. Lett. 54, 540–546 (2001)
16. Nishimori, H.: Statistical physics of spin glasses and information processing. Oxford Univ. Press (2001)
17. Kabashima, Y.: A CDMA multiuser detection algorithm on the basis of belief propagation. J. Phys. A: Math. Gen. 36, 11111-11121 (2003)
18. Mizutani, A., Tanaka, T., and Okada, M.: Improvement of multistage detector with partial interference cancellation. IEICE Trans. Fundamentals (Japanese Edition), J87-A (5), 661–671 (2004)
19. Tanaka, T. and Okada, M.: Approximate belief propagation, density evolution, and statistical neurodynamics for CDMA multiuser detection. IEEE Trans. Inf. Theory 51 (2), 700–706 (2005)
20. Tanaka, K.: Statistical-mechanical approach to image processing. J. Phys. A: Math. Gen. 35 (37), R81–R150 (2002)
21. Tanaka, K. Shouno, H., Okada, M.and Titterington, D. M.: Accuracy of the Bethe Approximation for Hyperparameter Estimation in Probabilistic Image Processing. J. Phys. A: Math. Gen. 37 (36), 8675–8696 (2004)
22. Skanzos, N., Saad, D. and Kabashima, Y.: Analysis of common attacks inpublic-keycryptosystems based on low-density parity-check codes. Phys. Rev. E 68, 056125 (2003)
23. Kabashima, Y., and Saad, D.: Statistical mechanics of low-density parity-check codes. J. Phys. A 37, R1–R43 (2004)
24. Murayama, T.: Statistical mechanics of the data compression theorem. J. Phys. A: Math. Gen. 35 (8), L95–L100 (2002)
25. Sawahashi, M., Andoh, H., and Higuchi, K.: Interference rejection weight control for pilot symbol-assisted coherent multistage interference canceler in DS-CDMA mobile radio. IEICE Trans. Fundamentals E81-A (5), 957–972 (1998)

26. Xue, G., Weng, J., Le-Ngoc, T., and Tahar, S.: Adaptive Multistage Parallel Interference Cancellation for CDMA. IEEE J. Sel. Areas. Commun. 17 (10), 1815–1827 (1999)
27. Buehrer, R. M., Correal, N. S., and Woerner, B. D.: ADSP-based DS-CDMA multiuser receiver employing partial parallel interference cancellation. IEEE J. Sel. Areas. Commun. 17 (4), 613–630 (1999)
28. Han, S. H., and Lee, J. H.: Multi-stage partial parallel interference cancellation receivers multi-rate DS-CDMA system. IEICE Trans. Commun. E86-B (1), 170–180 (2003)