International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A New Class of Digital Watermark Scheme Constructed Based on Double Step Coding and Phase Modulation

Noriaki Minami[1], **Masao Kasahara**[2]

[1] *Faculty of Informatics, Hiroshima Kokusai Gakuin University,*
6-20-1, Nakano, Akiku, Hiroshima, 739-0321, Japan

[2] *Faculty of Informatics, Osaka Gakuin University,*
2-36-1 Kishibe-minami, Suita, Osaka, Japan

Abstract: We have proposed an information embedding method of a new class of digital watermark based on error correcting codes and cryptographic techniques. This method can detect the forgery of the digital image data. In this paper, we propose a new technique which can realize an embedding of the information, detecting the falsification and decoding of the original image for digital watermark based on error correcting code and cryptographic techniques.

Keywords: digital watermark, phase modulation, error correcting codes, RS code RSA cryptosystem

1. Introduction

The various studies have been made of the digital watermark systems [1, 2, 3]. It is very important to carefully consider the relationship between the quality and the security of the reproduced image when applying digital watermark to image processing system. Present authors have already proposed an information embedding system on the basis of phase modulated sampling lattice [4]. This technique has the advantage that the decrypting or the falsifying of the embedded information by the third party becomes difficult due to the fact that the original image is kept and made secret. However, this method has a disadvantage that the application range is limited, because the original image, the reference signal kept secret, is required when decoding. Furthermore it is required to sort out the original image from the database when performing the decoding process. Evidently, these cumbersome operations would not desirable from the standpoint of the practical applications.

In this paper we shall propose a new class of digital watermark system with detection and restoration functions. This system is based on double step coding and phase modulation where no original image is required in the decoding process. We show that the proposed scheme is able to restore an original image even when the falsification occurs [5 - 10]. We shall also propose and discuss on the double encoding method.

2. Embedding method

2.1 Algorithm

The concept of the proposed system is shown in Fig.1. In Fig.1, the followings are defined.

RS inside encoding:
First RS (Reed-Solomon) encoding in Fig.1.

Inside information symbol:
Information symbol of RS inside encoding.

Inside check symbol:
Check symbol of RS inside encoding.

[1] Corresponding author.
Email address: minami@hkg.ac.jp

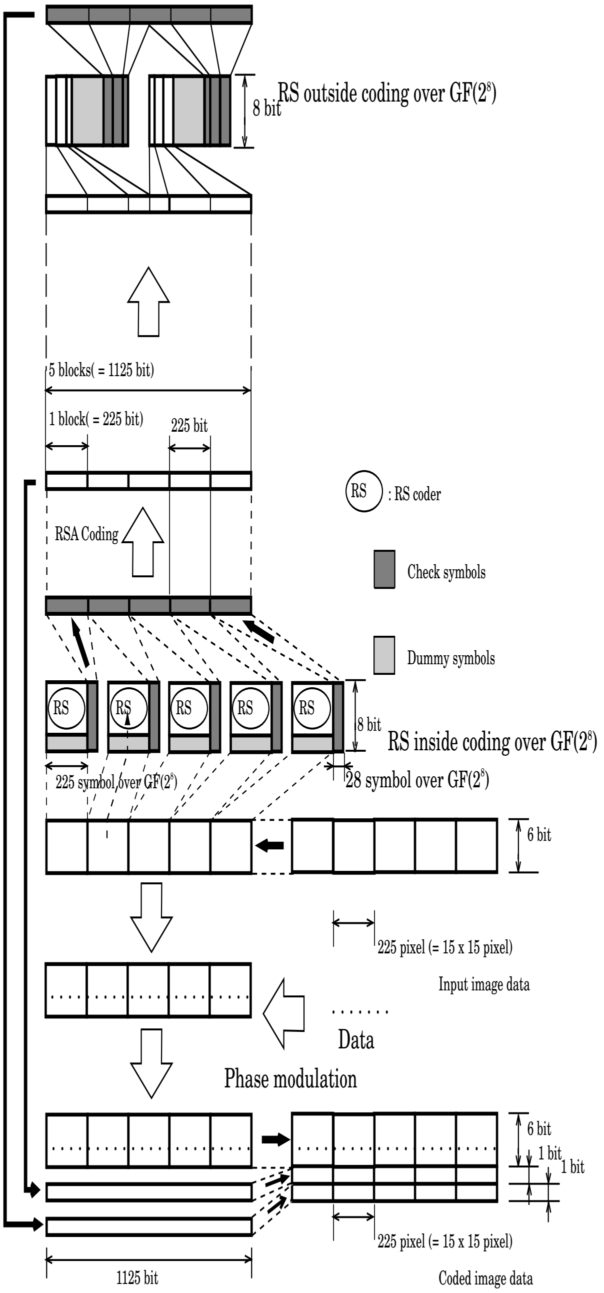

Figure 1. Principles of proposed method.

RS outside encoding:
Second RS encoding in Fig.1.

Outside information symbol:
Information symbol of RS outside encoding.

Outside check symbol:
Check symbol of RS outside encoding.

Let us define two classes of coding

Single Step Coding (Single encoding):
The embedding method of the additional information where RS encoding is applied only once.

Double Step Coding (Double encoding):
The embedding method of the additional information based on both RS outside encoding and RS inside encoding.

Embedding of additional information.

Step 1. The image information (original image) is quantized to 6 bits. The image information with the size of $H \times V$ pixel is constituted. In addition, this image information is divided into the block of size $M \times N$ pixel. In the followings, we assume that $M = N = 15$.

Step 2. The information symbol which consist of the 225 symbols over $GF(2^8)$ is encoded using RS inside encoder over $GF(2^8)$ (See Fig.1).

Step 3. Inside check symbol of the RS inside code over $GF(2^8)$ is encrypted, yielding RSA cryptogram.

Step 4. Inside check symbol encrypted to RSA cryptogram is located in Location 2 as outside information symbol (See Fig.2).

Step 5. Outside information symbol obtained in Step4 is encoded using RS outside encoder over $GF(2^8)$, yielding outside check symbol. It is located in Location 1 (See Fig.2).

Step 6. The additional information is embedded on the randomly chosen pixel based on the phase modulation.

2.2 Two-dimensional phase modulation of sampling lattice.

Let the pixel value of the image be represented by $f(x, y)$, where x and y show the horizontal and the vertical direction coordinates, respectively . Using a square sampling lattice of the period T , $f(x, y)$ is sampled, yielding the following digital image data:

$$\{f_{m,n}\} = \{f(mT, nT)\}. \tag{1}$$

The $f(x, y)$ is then represented by

$$f(x, y) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} f_{m,n} \cdot h(x - mT, y - nT), \tag{2}$$

where

$$h(u, v) = \text{sinc}(\pi u/T) \cdot \text{sinc}(\pi v/T) \tag{3}$$

and
sinc$(\cdot)$ denotes the sampling function.

Letting the sampling lattice be denoted by the coordinates (mT, nT), let us denote the small displacement by $(\varepsilon(m, n)T, \delta(m, n)T)$. We assume that the sampling lattice with small displacement belongs to L^*, as shown below:

$$(mT, nT) \in L. \tag{4}$$

$$(mT + \varepsilon(m, n)T, nT + \delta(m, n)T) \in L^*. \tag{5}$$

Re-sampling the original image f(x,y) with L^*, the following equation is obtained:

$$g_{m,n} = \sum_{i=-\infty}^{\infty} \sum_{j=-\infty}^{\infty} f_{m-i,n-j} \cdot$$

$$h((i + \varepsilon(m, n)) \cdot T, (j + \delta(m, n)) \cdot T). \tag{6}$$

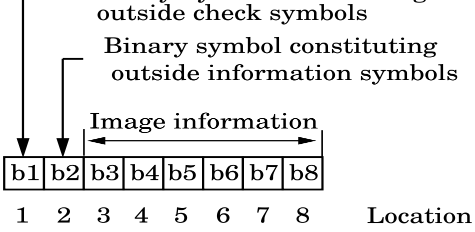

Figure 2. Structure of $GF(2^8)$.

2.3 Embedding method based on phase modulation

Let the coordinate of the pixel where the additional information is embedded, by (m, n). Let the embedded additional information take on the value $w(w \in \{0, \cdots, 3\})$. The small displacement can be represented by

$$(\varepsilon(m, n), \delta(m, n)) = (a \cdot Re[e^{j\theta}], a \cdot Im[e^{j\theta}]), \tag{7}$$

where θ is given by

$$\theta = w * \pi/2 \tag{8}$$

and $a(0 < a < 0.5)$ is the amount of a phase shift.

We thus see that it is possible to embed the additional information of 2 bits per 1 block.

2.4 Number of pixels which can be utilized for phase modulation

The number of outside binary check symbols of the outside RS code is given by $225 \times 5 \div 2$ bits, yielding 70 symbols over $GF(2^8)$. The minimum distance of the code is given by d=71, yielding the error correction capability of 35 symbols errors.

Let us define the following symbols.

N_b : maximum number of falsified blocks that can be decoded.

c : number of pixels that embed the additional information, per block.

For the single step coding, the following equation holds:

$$2 \times N_b + c \leq 14. \tag{9}$$

For the double step coding, the following equation holds:

$$2 \times N_b \leq 14. \tag{10}$$

$$N_b + c \leq 14. \tag{11}$$

The results obtained from Eq. (10) and (11) are shown in Table1.

3. Falsification detection and decoding of additional information

3.1 Decoding algorithm

The decoding algorithm is given as follows:

Step 1. 8 bits image data with the size of $H \times V$ pixel is divided into the blocks of size $M \times N$ pixel.

Step 2. The symbols in Locations 1 and 2 are decoded using RS outside decoder.

Step 3. The outside information symbol is decoded with the RSA decoder, and the decoded symbol is regarded as the inside check symbol.

Step 4. The image information along with inside check symbol obtained in Step3 is decoded using RS inside decoder.

Step 5. The embedded position is determined according to the same random number used at the encoder.

Whether or not the error symbol position agrees with the position of additional information is checked.

Step 6. The additional information embedded by phase modulation in the image is decoded.

Table 1. Possible number of additional information that can be embedded

N_b	0	1	2	3	4	5	6	7
c for Single Step Coding	14	12	10	8	6	4	2	0
c for Double Step Coding	14	13	12	11	10	9	8	7

4. Various considerations

4.1 Computation amount

Let us define the following symbols:

A_c : computation amount.

C_u : processing time which is defined as 1 time of decryption + 2 times of error correction.

u : total number of the RSA coded blocks.

b_v : v-th image block.

n_{oc} : number of outside check symbol.

n_{ic} : number of inside check symbol.

q : $\lfloor n_{oc}/n_{ic} \rfloor$, integer part of n_{oc}/n_{ic}.

It is assumed that the falsification is made on block b_v.

Although the details of doing so are omitted, the computation amount, A_c, is given as follows:

(i) single step encoding:

$$A_c = (1 + 2^q)/2 \times u + (2^q - 1) \times v - 2^q + 1. \quad (12)$$

(ii) double step encoding:

$$A_c = u. \quad (13)$$

For the block size of 15×15 pixels, the total number of pixels that constitute 15×15 blocks takes on the value of 225×225 pixels. In this case q is given by $q = 5$. When a falsification is committed on the central block (the 113th block), the average computation amount A_c, is given as follows:

(i) single step encoding:

$$A_c \approx 4.21 \times 10^3. \quad (14)$$

(ii) double step encoding:

$$A_c = u = 45 (= (225 \times 225)/(15 \times 15)/5). \quad (15)$$

We see that the significant improvement by a factor 1/90 has been achieved on the computation amount. It should be noted that the average value can be given as a central block.

4.2 Picture quality

When the additional information is regarded as noise, the mean square error, $\bar{x^2}$ is given by the following equation:

$$\bar{x^2} = \sum_{k=0}^{2^\nu - 1} \frac{k^2}{2^\nu}, \quad (16)$$

where ν is the size (in bits) assigned to the additional information.

The signal-to-noise ratio of η_A is given by the following equation:

$$\eta_A = 20 \log \left((2^{(m+\nu)} - 1) / \sqrt{\frac{1}{2^\nu} \sum_{k=0}^{2^\nu - 1} k^2} \right), \quad (17)$$

where m is the size of the binary symbols.

where $m = 6$, $\nu = 2$ are substituted for Eq.(17), the signal-to-noise ratio of $\eta_A \approx 42.7$ dB is obtained.

The simulation has been carried out for the standard images “Barbara”, “Zelda”, “Toy” and “Boat”. The SN ratio observed is given by approximately 42.7dB for all images. This value is almost same as the theoretical value. We thus see that the additional information can be considered random noise. In the subjective evaluation, the noise is proved not visually conspicuous.

5. Falsification restoration by outside coding

In this section we shall discuss on two decoding schemes, a simple conventional decoding scheme[9] and a new decoding scheme. We shall refer to the former as D-decoding and the latter, $\widetilde{D}$-decoding. These are be defined by follows.

D-decoding : decoding scheme with error correction only.

$\widetilde{D}$-decoding : decoding scheme with both error correction and erasure error correction.

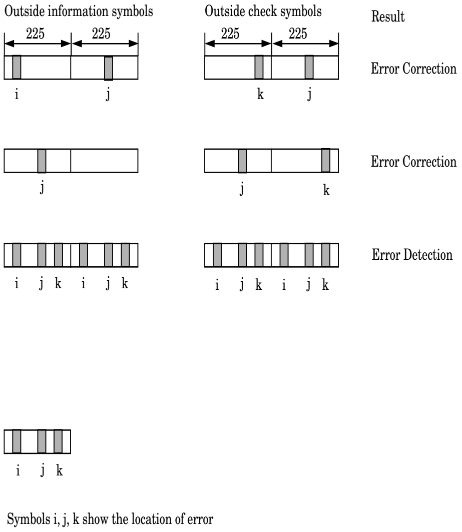

Figure 3. Principles of $\widetilde{D}$-decoding.

For an easy understanding, we shall explain $\widetilde{D}$-decoding by an example given in Fig.3. Although the details of doing so are omitted all the pixels constituting each block are interleaved in order to disperse the effect of a falsification, in our proposed scheme. As the result, as shown Fig.3, a falsification committed on a block disperse to the same location, for example, at Locations i, j and k with the probability 1/2.

Thus almost half of the codewords are successfully decoded and the remaining half of the codewords are only detected errors. However fortunately, as shown in Fig.3, the locations of error can be successfully found and these errors can be regarded as erasure errors. Thus the codewords with the detected errors can be corrected based on erasure error correction.

In Table 2 we show the performances of two decoding schemes. We see that $\widetilde{D}$-decoding yields a remarkable performance compared with D-decoding.

Table 2. Performance of D-decoding and $\widetilde{D}$-decoding

Total number of falsified blocks	Fraction of sucessful restoration for D-decoding	Fraction of sucessful restoration for $\widetilde{D}$-decoding
7	1.000	1.000
8	1.000	1.000
9	0.994	1.000
10	0.955	1.000
11	0.699	1.000
12	0.308	1.000
13	0.075	1.000
14	0.018	1.000

6. Conclusion

In this paper, we have proposed the new class of digital watermark. This method is based on error correcting code (RS code), cryptographic technique (RSA crypto system) and two-dimensional phase modulation. The proposed method has the following advantages .

1. It can detect the falsification of the image. In addition, under the specific condition, the falsification can be restored.

2. It hardly deteriorates the image quality. It necessitates no original image when performing the decoding process.

3. It presents the double step coding method which is superior to the single step coding method previously proposed by the present authors.

4. Computation amount of the proposed method takes on sufficiently small value regardless of the size of the falsification.

5. It presents $\widetilde{D}$-decoding that yields the large error correction capability compared with D-decoding.

References

[1] K.Matsui, J.Ohnishi, Y.Nakamura, “Embedding a Signature to Pictures under Wavelet Transformation,” *IEICE Trans. Inf. & Syst.*, Vol.J79–D–II, No.6, pp.1017–1024, June 1996.

[2] K.Matsui, *The Fundamentals of Digital Watermark*, MORIKITA publishing company.

[3] N.Minami, S.Tazaki, Y.Yamada, “Embedding Method of Additional Information for Visual Data using Vector Quantization,” *Journal of IIEEJ*, Vol. 27, No. 5, pp.492–498, Oct. 1998.

[4] N.Minami, Y.Yamada, S.Tazaki, “Data Embedding Method Based on the Phase Modulation of Sampling Lattice,” *Journal of IIEEJ*, Vol. 28, No. 3, pp.278–283 June 1999.

[5] N.Minami, K.Wakasugi, M.Kasahara, S.Tazaki, “A Construction Method of Recoverable Visual Data and Its Evaluation,” *IEICE Trans. Inf. & Syst.*, Vol.J81-D-II, no.11, pp.2535-2546, Dec. 1998.

[6] N.Minami, M.Kasahara, “Digital Watermark based on Error Correcting Codes and Cryptography,” *Journal of IIEEJ*, Vol.31, No.6, pp.1208–1212, Dec. 2002.

[7] N.Minami, M.Kasahara, “A New Decoding Method for Digital Watermark Based on Error Correcting Codes and Cryptography,” *IEICE Trans. Fundamentals*, Vol.J87–A, No.7, pp.967–975, July 2004.

[8] N.Minami, M.Kasahara, “A Note on Digital Watermark based on Error Correcting Codes and Cryptography,” *IEICE Trans. Fundamentals*, Vol.J88–A, No.5, pp.658–662, May 2005.

[9] N.Minami, M.Kasahara, “Digital Watermark based on Error Correcting Codes and Cryptography with the Structure of the Double Coding,” *Journal of IIEEJ*, Vol. 35, No. 6, pp.909–913 , Nov. 2006.

[10] N.Minami, Y.Yamada, M.Kasahara, “Detection and Restoration Method based on Digital Watermark Using Phase Modulation,” *Symposium on Cryptography and Information Security*, 2B1-3,6p, Jan. 2007.