

Watermark with DSA signature using predictive coding

Cheonshik Kim · Ching-Nung Yang

Published online: 29 August 2013

© The Author(s) 2013. This article is published with open access at SpringerLink.com

Abstract This paper presents a predictor-based watermark scheme that embeds secret bit streams and a DSA signature into an image. For the copyrighting of digital media, a DSA signature is appropriate as a watermarking technique. To improve security, we apply an Arnold transform (AT) to secret messages. We propose new predictors, *Left-Top*, which the predict current pixel values using neighboring pixel values. Our proposed scheme conceals secret messages by using the difference between current pixel values and predictive pixel values. Experimental results show that our method has low complexity and achieves a higher embedding performance with good perceptual quality compared to the earlier arts. Experimental results verified our proposed watermark method in multimedia communications.

Keywords Watermarking · DSA signature · Predictors

1 Introduction

A digital watermark is added to a digital file to impart additional information or features. Sometimes the mark is obvious and sometimes it is imperceptible. Imperceptible watermarks are unnoticeable to human eyes. Recently, these have most commonly been used in forensic or tracking applications. Because the watermark

C. Kim (✉)

Department of Digital Media Engineering, Anyang University, 708-113 Anyang 5-dong,
Manan-gu, Anyang-shi, Kyonggi-do 430-714, Republic of Korea
e-mail: mipsan@paran.com

C.-N. Yang

Department of Computer Science and Information Engineering,
National Dong Hwa University, Hualien 9701, Taiwan, Republic of China
e-mail: cnyang@mail.ndhu.edu.tw

is added to the underlying content file, it can impart unique information. For example, watermarks are added to copies of motion pictures and television programs. The ability to track illegal copies to their source is a powerful piracy deterrent. An important advantage of a watermark is its ability to survive digital-to-analog conversion. Thus anyone recording a TV broadcast also records its watermark. If the recording is later posted on the Internet the forensic watermark gets posted as well.

This kind of data hiding is suitable for some specific applications where images are sensitive to further processing, such as medical images, satellite images, and artwork. Data hiding [10, 27] has applications in secure communications [5, 11, 14, 15, 17, 18, 20, 21, 23] where an insecure but readily available medium such as the Internet is used to transmit hidden data. It can also be used for transmitting different kinds of information securely over an existing channel dedicated to transmitting something else, such as transmitting hidden speech over a channel meant for transmitting H.263 video.

Fragile watermarking [26] is used for the authentication of the cover image. A fragile watermark is destroyed, even in the case of minimal modification of the cover image. The digital image is popularly used as a host image to convey side information in the image. In a watermark system, the image used to embed secret data is referred to as the host image (i.e., cover image). The image with the embedded secret data is called a stego image. The stego-image should be perceptually identical to the host image in order to not come under attack from a hacker. Stego images can be used as a copyright and safety channel for data communication. On the Internet, a receiver can extract the secret data from a stego image.

To hide secret data, it is possible to use the spatial domain [10, 12, 27] or frequency domain [3, 9] of an image. The first scheme conceals secret data by flipping the rightmost, four least significant bits (LSB) per pixel.

The second scheme is based on the frequency domain and uses a transformation function such as the discrete cosine transforms (DCT) [9] and the discrete wavelet transforms (DWT) [3]. These schemes are very resistant to attacks; however, their hiding capacities are limited.

Galand and Kabatiansky [8] proposed a new data hiding scheme called matrix encoding. The F5 algorithm [24] implemented by Westfeld was based on matrix. One can find the definition of the cover coding [1, 2, 8] in [7]. Westfeld showed matrix encoding using Hamming codes. The performance of “+/- steganography” was introduced by [25]. Zhang and Wang [29] showed ternary Hamming codes using the concept of efficiency by exploiting the modification direction (EMD). Chang et al. [4] proposed (7, 4) Hamming code for data hiding, which improves on the “Hamming+1” scheme [30]. Yu et al. [28] proposed a data hiding scheme via predictive coding and showed good image quality using MED and GAP predictors, Yu et al. [28] which hide secret data in an image. This scheme shows the high quality and high capacity of stego images.

BCH codes were applied to achieve a tradeoff between the embedding complexity and efficiency [16]. The CPT method [22] shows embedding efficiency by hiding messages based on the weighted value of a block.

In this paper, we propose a novel steganographic watermarking scheme, which is used to conceal a bit in each pixel to predict the original pixel's value using a *Left-Top* Predictor. This will help securely transmit secret data to the receiver. Based on

this, we propose an image-hiding scheme based on predictive coding, which exploits the prediction error values to hide secret data.

The advantage of our technique is that we can conceal more bits in an image than previous schemes. Hence, our technique is robust to attacks such as noise and cropping.

The following are the major contributions of this paper:

- Identification of the copyright of an image through watermarking as an important and technically challenging problem for multimedia.
- Experiment of the robustness and effectiveness of the proposed technique to demonstrate the feasibility of watermarking images.

The remainder of this paper is organized as follows. In Section 2, descriptions of some schemes related to this paper are provided. In Section 3, we present our proposed scheme. The experimental results are given in Section 4. Finally, the conclusions are given in Section 5.

2 Related works

2.1 Arnold transform (AT)

In 1960, *Vladimir Arnold* proposed Arnolds cat map (ACM) or the Arnold Transform (AT) [19], which is a chaotic map that randomizes a digital image when applied to it, rendering the image imperceptible or noisy. However, it has a period p and if iterated p number of times, the original image reappears.

Definition 1 The generalized form of Arnold’s cat map can be given by the transformation $\Gamma : T2 \rightarrow T2$ such that:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{N} \quad (1)$$

where $x, y \in \{0, 1, 2, \dots, N - 1\}$ and N is the size of a digital image. Let p be the transform period of an $N \times N$ digital image I . Applying ACM for a random iteration of t times ($t \in [1, p]$) to I , a scrambled image I is obtained which is completely chaotic and is different from I .

2.2 Prediction of JPEG-LS

The prediction and modeling units in JPEG-LS are based on the causal template depicted in Fig. 1, where x denotes the current pixel, and $a, b, c,$ and $d,$ are neighboring pixels in the relative positions shown in Fig. 1. Variables $a, b, c, d,$ and x denote both the values of the pixels and their locations. By using the template shown in Fig. 1, JPEG-LS limits its image buffering requirement to one scan line. The value guessed for the current pixel x should depend on $a, b, c,$ and d through an adaptive model of the local edge direction. A fixed predictor performs a primitive

Fig. 1 MED predictor

c	b	d							
a	x								

test to detect vertical or horizontal edges. Specifically, the fixed predictor in LOCO-I/JPEG-LS [28] guesses:

$$\check{x} = \begin{cases} \min(a, b) & \text{if } d \geq \max(a, b) \\ \max(a, b) & \text{if } c \leq \min(a, b) \\ a + b - c & \text{otherwise} \end{cases} \tag{2}$$

The predictor in (2) switches between three simple predictors: it tends to pick b in cases where a vertical edge exists to the left of the current location, a in cases of an horizontal edge above the current location, or $a + b - c$ if no edge is detected. The guessed value is seen as the median of three fixed predictors, a , b , and $a + b - c$. By combining both interpretations, this predictor was renamed during the standardization process as “median edge detecto” (MED).

2.3 DSA Digital Signature Algorithm

The Digital Signature Algorithm (DSA) [13] is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS).

Definition 2 (Digital Signature Algorithm) The triplet (p, q, r) denotes public parameters, where p and q are prime numbers satisfying $q|p-1$ and $g \in \mathbb{Z}_p^*$ is the generator of the subgroup of order q in \mathbb{Z}_p^* , i.e., $g^q \equiv 1 \pmod p$. The private key $x \in \mathbb{Z}_q$ is chosen randomly with a uniform distribution. The corresponding public key $y \in \mathbb{Z}_p$ is computed as $y = g^x \pmod p$. The couple (x, y) is called the DSA key pair. To create a signature (r, s) for a message $m \in 0, 1^*$, the owner of the private key x first generates a random number $k \in \mathbb{Z}_p^*$, which is usually referred to as a nonce (number used once). The signer computes

$$\begin{aligned} r &= (g^k \pmod p) \pmod q \\ s &= k^{-1}(h(m) + xr) \pmod q \end{aligned} \tag{3}$$

where h is the hash function SHA-1 and $k^{-1}k \equiv (\text{mod } q)$. To verify the validity of the signature pair (r, s) of message m , the verifier first checks whether $0 < r < q$ and $0 < s < q$ hold: he rejects the signature otherwise. Secondly, he computes.

$$\begin{aligned} w &= s^{-1} \text{ mod } q \\ u_1 &= h(m)w \text{ mod } q \\ u_2 &= rw \text{ mod } q \\ v &= (g^{u_1} y^{u_2} \text{ mod } p) \text{ mod } q \end{aligned} \quad (4)$$

The signature is accepted if and only if $v = r$;

Lemma 1 *Let (r, s) be a given signature of message m to be verified. Then the value v computed during the signature verification is equal to r , if (r, s) was generated using the DSA signing operation described in Definition 1.*

Proof The definition of s yields $l \in \mathbb{Z}$ such that $k = w(h(m) + xr)lq$. Let $v' = g^{u_1} y^{u_2} \text{ mod } p$. By the definition of u_1 and u_2 , there exist $l_1, l_2 \in \mathbb{Z}$ such that

$$\begin{aligned} v' &= g^{h(m)w+l_1q} y^{rw+l_2q} \text{ mod } p = g^{w(h(m)+l_1q)} g^{xrw+xl_2q} \text{ mod } p \\ &= g^{w(h(m)+l_1q)} g^{(l_1+xl_2)q} \text{ mod } p = g^{k+lq} g^{(l_1+xl_2)q} \text{ mod } p \\ &= g^k (g^q)^{l+l_1+xl_2} \text{ mod } p = g^k \text{ mod } p, \end{aligned}$$

Since $g^q \equiv 1 \text{ (mod } p)$. Finally, $v = v' \text{ mod } q \text{ (} g^k \text{ mod } p) \text{ mod } q = r$. \square

3 Proposed scheme

In this section, we shall present the proposed image hiding based on the predictive coding technique.

3.1 Left-Top pixel predictor

We propose a predictor method, the *Left-Top* pixel predictor. In Fig. 2a, x is the current pixel, a and b are a neighboring pixels. The x' pixel can be predicted using (5). Figure 2b shows the procedure for reading the next x pixel. In Fig. 2b, pixels x is supposed to be the pixel b , respectively. The function $\lfloor \cdot \rfloor$ transforms a real value into an integer value.

$$x' = \lfloor (a + b)/2 \rfloor \quad (5)$$

3.2 Embedding procedure

Our proposed scheme for embedding a watermark into a cover image is shown in Fig. 3. Before the embedding procedure, the watermark is scrambled and encrypted. We generate hash a code using SHA-1 with the watermark. Applying SHA-1 to the

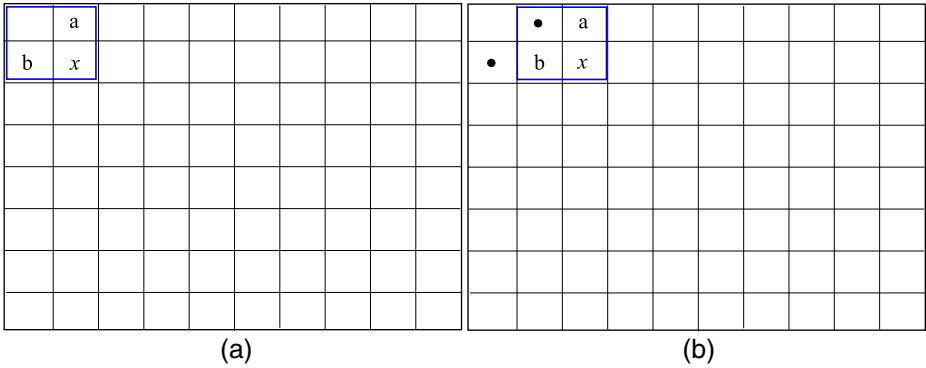


Fig. 2 Example of *Left-Top* predictor

watermark can reduce the signature. To authenticate the watermark, DSA encryption is used with the watermark for authentication. These message bits and DSA signature are embedded in the cover image. We present the embedding procedure step by step:

Input: Cover image I with size $H \times W$ and binary secret message m .

Output: A watermarked image I' with size $H \times W$.

- Step 1: Scramble a copyright image (watermark) m using (1). After scrambling, we get m' , which is the scrambled secret message.
- Step 2: The scrambled watermark is encrypted using a one way hash function SHA-1, i.e., $sm = h(m')$.

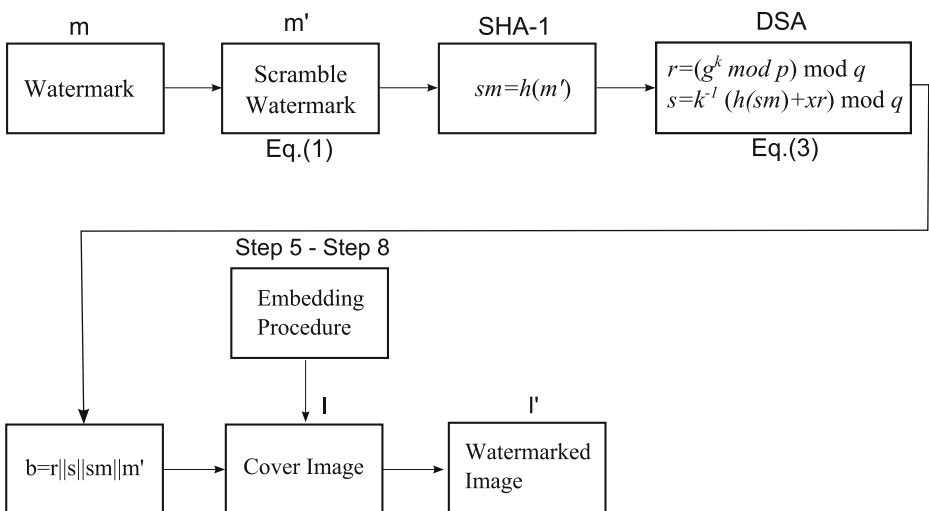


Fig. 3 Schematic diagram of the embedding procedure

- Step 3: A DSA signature is applied to sm to get r and s using (3). From the next step, we will show the procedure for concealing encryption value s , which is composed of $\{0, 1\}^{160}$. The triplet (p, q, r) is generated based on Definition 1.
- Step 4: Concatenate r, s, sm , and m' .

$$b = r||s||sm||m' \tag{6}$$

- Step 5: A block of pixels is assigned to variables such as a, b, c, d , and x , which are read as a 2×2 pixel block from the cover image I of Fig. 2a. To read the next block, move from left to right 1 pixels, as seen in Fig. 2b.

$$[a, b, x] = \sum_{i=1}^n \sum_{j=1}^m (I_{i,j} : I_{i+1,j+1}) \tag{7}$$

- Step 6: Compute prediction value x' of a block using (5). Choose one bit out of b .

$$d = \sum_{i=1}^n b(i) \tag{8}$$

- Step 7: The “ \oplus ” operator denotes “Exclusive Or.” This equation can be used to hide a binary bit at this stage. The x in the following equation is the current pixel.

$$I'_{i,j} = \begin{cases} \text{no change} & \text{if } LSB(x) = d \oplus LSB(x'_i) \\ x = x + 1 & \text{otherwise} \end{cases} \tag{9}$$

- Step 8: If count = 0, then exit. Otherwise, count = count – 1. Go to Step 5.

3.3 Extraction procedure

In Fig. 4, we show the extraction procedure for the watermarked image using the proposed scheme. After finishing the extraction procedure, DSA verifies the

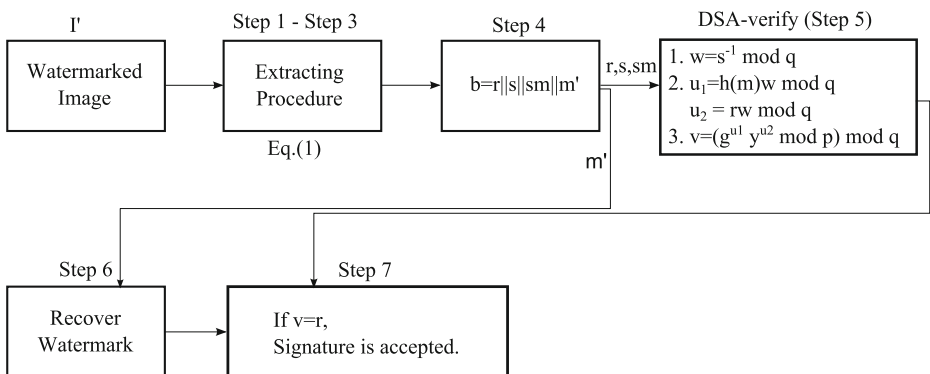


Fig. 4 Schematic diagram of extraction procedure

signature s . If $s = r$, then the signature is accepted. That is, the original watermark can be authenticated using the DSA signature. We present step-by-step extraction procedure:

Input: Stego image I' with size $H \times W$, ls is number of blocks, and $cnt = 0$.

Output: Secret message b , DSA signature bits $v = r$.

- Step 1: A block of pixels is assigned to variables such as a, b , and x read as 2×2 pixel block from the watermarked image I' of Fig. 2a. To read the next block, move from left to right 1 pixels, as can be seen in Fig. 2b.
- Step 2: Compute prediction value x' of x with a and b using (5).
- Step 3: If $(cnt > ls)$, go to step 4. Otherwise, go to step 1.

$$b(cnt++) = LSB(x) \oplus LSB(x') \tag{10}$$

- Step 4: Extract the keys and digital values from string b .

$$(r, s, sm, m') = \text{division}(b);$$

```
function division (b) {
    [r, s, sm, m'] = (b(1:16), b(17:32), b(33:193),
        b(194:size(m')));
    return ([r, s, sm, m']);
}
```

- Step 5: Compute v as follows. That is, $w = s^{-1} \text{ mod } q, u_1 = h(sm)w \text{ mod } q, u_2 = rw \text{ mod } q, v = (g^{u_1} y^{u_2} \text{ mod } p) \text{ mod } q$.
- Step 6: Recover original watermark with vector m' using (1).
- Step 7: If $v = r$, the signature is accepted, else the signature is not accepted.

4 Experimental results

We proposed a watermarking scheme based on grayscale images using the *Left-Top* predictor, which is applied to blocks in the images. Our proposed scheme has a higher dB than previous schemes. The predictor based fragile watermarking schemes show the steganography features. Thus, it is difficult to detect watermark images using the human eye. To prove that our proposed scheme is correct, we performed an experiment to verify that the hidden image can be restored. The results showed that it is feasible to use our method for making good quality watermarked images from the original grayscale image. The proposed scheme includes an authentication function using the DSA signature. To carry out our experiment, 512×512 grayscale images were used as cover images. Figure 5 shows a cover image used in the experiment to verify our proposed scheme. In our experiments, the quality of each watermarked images was measured using the peak-signal-to-noise ratio (PSNR) [3]. PSNR is the most popular criterion for measuring the distortion between the original image and shadow images. It is defined as follows:

$$PSNR = 10 \times \log_{10}(255^2/MSE) \tag{11}$$

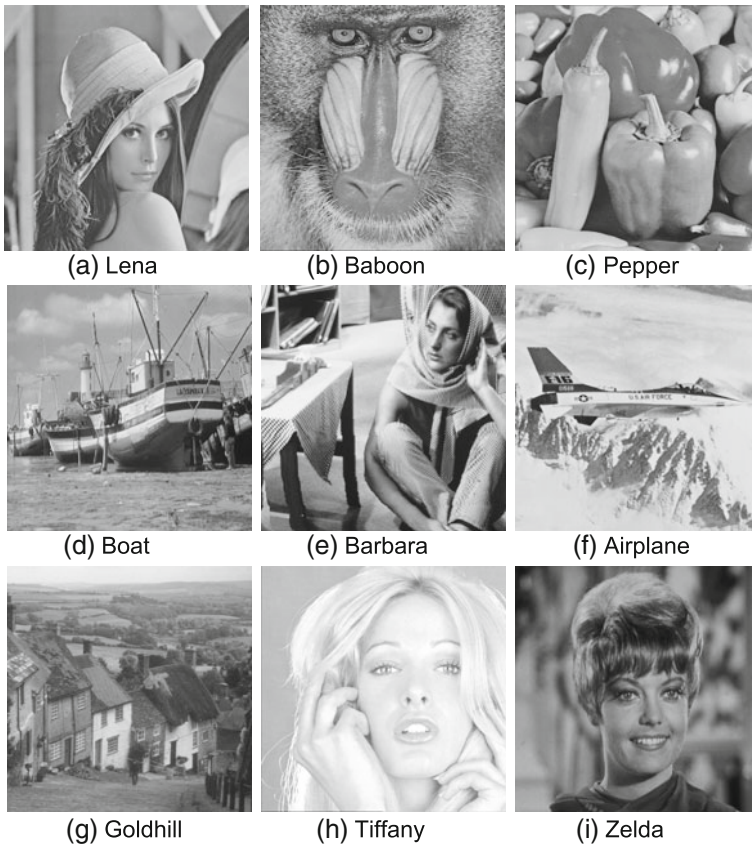


Fig. 5 512×512 grayscale cover images for watermark experiment

where MSE is the mean square error between the original grayscale image and the shadow image:

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n [I(i, j) - I'(i, j)]^2 \quad (12)$$

The variables $I(i, j)$ and $I'(i, j)$ represent the pixel values of the original grayscale image and the watermarked image at position (i, j) , respectively; m and n are the width and height of the original image, respectively.

$$p = \frac{|b|}{m \times n} (bpp) \quad (13)$$

In (13), p denotes the bits-per-pixel (bpp), which is the embedding payload. Our experiment compared the number of secret bits that can be carried by a cover pixel. $|b|$ is the number of bits for watermark b . There is a tradeoff between the payload and quality of an image. Increasing the embedding rate clearly requires a sacrifice in image quality.

Table 1 Comparison results of Matrix encoding, Hamming+1 scheme, and proposed scheme

Images	Matrix coding [6]		Hamming+1 [30]		Scheme-MED (h = 1) [28]		Scheme-GAP(h = 1) [28]		Left-Top predictor	
	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload	PSNR	Payload
Baboon	56.44	0.43	54.71	0.499	51.11	0.25	51.12	0.25	51.17	0.9961
Barbara	56.65	0.43	48.60	0.499	51.15	0.25	51.16	0.25	51.19	0.9961
Boats	54.75	0.43	49.37	0.499	51.15	0.25	51.14	0.25	51.20	0.9961
Goldhill	57.02	0.43	53.73	0.499	51.15	0.25	51.14	0.25	51.19	0.9961
Airplane	55.84	0.43	51.61	0.499	51.15	0.25	51.15	0.25	51.18	0.9961
Lena	56.05	0.43	52.43	0.499	51.16	0.25	51.14	0.25	51.20	0.9961
Pepper	54.01	0.43	47.26	0.499	51.16	0.25	51.12	0.25	51.118	0.9961
Tiffany	53.40	0.43	47.46	0.499	51.14	0.25	51.12	0.25	51.22	0.9961
Zelda	56.40	0.43	54.04	0.499	51.16	0.25	51.14	0.25	51.21	0.9961
Average	56.44	0.43	50.91	0.499	51.14	0.25	51.13	0.25	51.30	0.9961

Through a comparison between our proposed scheme and previous schemes, we explain superiority of the proposed scheme's performance. Yu et al. [28] proposed a data hiding method based on the frequency domain using MED and GAP predictors. Comparisons of the PSNRs of the watermarked images are shown in Table 1. According to the results, shown in Table 1, the PSNRs of the watermarked image of the proposed scheme are better than those of Scheme-MED, Scheme-GAP, and "Hamming+1." The average PSNR value of the watermarked images in the proposed scheme is more than 51.19 dB, whereas the values for Scheme-MED and Scheme-GAP are 51.14 and 51.13 dB, respectively. The "Hamming+1" scheme shows various PSNRs based on the frequencies of the images used for the experiments. However, the average values of the proposed schemes are higher than that of the "Hamming+1" scheme. The matrix coding scheme is a steganographic scheme and the embedding rate is 0.43. Thus, it shows high PSNR values. Therefore, our method is feasible for making good quality watermarked images from the original grayscale image. However, if it is possible to maintain the balance between the payload and the quality of an image, we then accomplish our purpose from the perspective of steganography. The payload of the "Hamming+1" scheme is 0.499 bpp, while those of MED & GAP schemes are 0.25 bpp. Matrix coding has a value of 0.43, while the other schemes' payload is 0.9961 bpp.

There are two kinds of watermark attacks: non-intentional attacks such as the compression of a legally obtained, watermarked image or video file, and intentional attacks such as an attempt by a multimedia pirate to destroy the embedded information and prevent the tracing of illegal copies of a watermarked image. In our experiment, we considered salt and pepper noise and cropping. Salt and pepper









Attacked Image (Salt & Pepper noise)	Reconstructed Logo	Attacked Image (Salt & Pepper noise)	Reconstructed Logo
			
10%	Logo	20%	Logo
			
30%	Logo	40%	Logo

Fig. 6 Watermarked image, attacked image and recovered logo

noise is a form of noise typically seen in images. It presents itself as randomly occurring white and black pixels. In this section we show the result of our proposed scheme after using salt and pepper noise to corrupt images by up to 40 %. This algorithm can recover the embedded information from the effected watermarked images. From the results (see Fig. 6) it is clear that the proposed algorithm can withstand even a 40 % salt and pepper attack with ease, and the information logo that is derived from the watermarked image closely resembles the information logo that was embedded in the image. Thus we can say that the proposed algorithm efficiently handles salt and pepper noise. The robustness of the proposed method against different types of image cropping operations that may be performed (as deliberate external attacks) on the watermarked image was also tested. In all cases the extracted watermarks, although affected by noise by different amounts, were still recognizable. Figure 7 shows that the visual quality of the extracted watermark will as good if watermark pixels are inserted, even in the desired area of the cover image in a sequential manner rather than the pseudo-random fashion obtained by chaotic mixing.











Attacked Image (Cropping)	Reconstructed Logo	Attacked Image (Cropping)	Reconstructed Logo
			
Cropping #1	Logo	Cropping #2	Logo
			
Cropping #3	Logo	Cropping #4	Logo
			
Cropping #5	Logo		

Fig. 7 Watermarked image, attacked image (cropping), and recovered logo

5 Conclusion

Fragile watermarking is necessary for digital rights management, information protection, and concealing secrets, because it is not easy to protect a secret message from hackers and attackers. Most watermarks are based on the frequency domain. Thus, the hidden bit capacity is lower than that of a domain based scheme. In this paper, we proposed a *Left-Top* predictor schemes that uses the LSBs of pixels in an image, using the difference errors between the original pixels and the predicted pixels. The results of experiments showed that the watermarked images of our proposed scheme had PSNR values greater than 51.19 dB, which demonstrated that our scheme is a reasonably acceptable steganography method. Thus, we can conclude that the *Left-Top* predictors are suitable for steganographic applications.

Acknowledgement This research was supported by the Basic Science Research Program Through the National Research Foundation of Korea (NRF) by the Ministry of Education, Science and Technology (20120192).

Open Access This article is distributed under the terms of the Creative Commons Attribution License which permits any use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

References

1. Bierbrauer J (2005) Introduction to coding theory. Section 14.2, Chapman and Hall, CRC Press
2. Bierbrauer J, Fridrich J (2006) Constructing good covering codes for applications in steganography. Available: <http://www.ws.binghamton.edu/fridrich/>. Accessed 1 Mar 2013
3. Chan PW, Lyu MR (2003) A DWT-based digital video watermarking scheme with error correcting code. In: Lecture notes in computer science, vol 2836, pp 202–213
4. Chang CC, Kieu TD, Chou YC (2008) A high payload steganographic scheme based on (7, 4) hamming code for digital images. In: International symposium on electronic commerce and security, pp 16–21
5. Chen CW, Tsai YR, Wang SJ (2012) Cost-Saving key agreement via secret sharing in two-party communication systems. Journal of Convergence 3(4):29–36
6. Crandall R (1998) Some notes on steganography. Posted on steganography mailing list. <http://os.inf.tu-dresden.de/westfeld/crandall.pdf>
7. Fridrich J, Soukal D (2006) Matrix embedding for large payloads. IEEE T Inf Foren Sec 1(3):390–394
8. Galand F, Kabatiansky G (2004) Information hiding by coverings. In: Proc. IEEE information theory workshop 2004, pp 151–154
9. Han WY, Yang Y, Zhi HL (2012) Digital watermark encryption algorithm based on Arnold and DCT transform. In: Lecture notes in electrical engineering, vol 138, part 5, pp 613–621
10. Kim HJ, Kim C, Choi Y, Wang S, X Zhang (2010) Improved modification direction methods. Comput Math Appl 60(2):319–325
11. Luo Y, Hoerber O, Chen Y (2013) Enhancing Wi-Fi fingerprinting for indoor positioning using human-centric collaborative feedback. Hum-cent Comput Inf Sci 3(2):1–23
12. Mielikainen J (2006) LSB matching revisited. IEEE Signal Proc Lett 13(5):285–287
13. Nenadic A, Zhang N, Barton S (2004) A secure and fair DSA-based signature exchange protocol. In: Proceedings of the ninth international symposium, ISCC 2004, vol 2, pp 412–417
14. Peng K (2012) Efficient and general PVSS based on elgamal encryption. J Inf Process Syst 8(2):375–388
15. Peng K (2013) A secure network for mobile wireless service. J Inf Process Syst 9(2):247–258
16. Schonfeld D, Winkler A (2006) Embedding with syndrome coding based on BCH codes. In: Proc. 8th ACM workshop on multimedia and security, pp 214–223

17. Sharma MJ, Leung VCM (2012) IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks. *Hum-cent Comput Inf Sci* 2(16):1–19
18. Singh B, Lobiyal DK (2012) A novel energy-aware cluster head selection based on particle swarm optimization for wireless sensor networks. *Hum-cent Comput Inf Sci* 2(13):1–18
19. Sujatha SS, Sathik MM (2010) Feature based watermarking algorithm by adopting Arnold transform. *Commun Comput Inform Sci* 101(1):78–82
20. Truong TT, Tran MT, Duong AD (2012) Improvement of the more efficient & secure ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC. *Journal of Convergence* 3(2):25–36
21. Tsai CL, Chen CJ, Zhuang DJ (2012) Trusted M-banking verification scheme based on a combination of OTP and biometrics. *Journal of Convergence* 3(3):23–30
22. Tseng Y-C, Chen Y-Y, Pan H-K (2002) A secure data hiding scheme for binary images. *IEEE Trans Commun* 50(8):1227–1231
23. Verma OP, Nizam M, Ahmad M (2013) Modified multi-chaotic systems that are based on pixel shuffle for image encryption. *J Inf Process Syst* 9(2):271–286
24. Westfeld A (2001) F5: a steganographic algorithm. In: *Proc. 4th int. workshop information hiding 2001. Lecture notes in computer science*, vol 2137, part 1, pp 289–302
25. Willems F, Dijk M (2005) Capacity and codes for embedding information in gray-scale signals. *IEEE Trans Inf Theory* 51(3):1209–1214
26. Wu HC, Yeh CP, Tsai CS (2006) A semi-fragile watermarking scheme based on SVD and VQ techniques. In: *Lecture notes in computer science*, vol 3982, pp 406–415
27. Yang CN, Ye G-C, Kim C (2011) Data hiding in halftone images by XOR block-wise operation with difference minimization. *KSII Trans Internet Inform Syst* 5(2):457–476
28. Yu YH, Chang CC, Hu YC (2005) Hiding secret data in images via predictive coding. *Pattern Recogn* 38:691–705
29. Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. *IEEE Commun Lett* 10(11):781–783
30. Zhang W, Wang S, Zhang X (2007) Improving embedding efficiency of covering codes for applications in steganography. *IEEE Commun Lett* 11(8):680–682



Cheonshik Kim received his B.S. degree in Computer Engineering from Anyang University, Korea, in 1995; his M.S. degree in Computer Engineering from Hankuk University of Foreign Studies (HUFS), Korea, in 1997; and his Ph.D. degree in Computer Engineering from HUFS in 2003. From March 2013, he was a professor of Department of Digital Media Engineering, Anyang University, Korea. He won a research award from the IEEK in 2012. He has served as the Editor for *ICACT Transaction on Advanced Communications Technology (TACT)* since 2012. He has program chair of International conference, GPC 2013, IEEK Computer Society in various capacities, including Vice-President since 2010. He is a member of IEEE. His research interests include Multimedia Systems, Data Hiding, and Watermarking. His research is supported by NRF.



Ching-Nung Yang received the B.S. degree and the M.S. degree, both from Department of Telecommunication Engineering at National Chiao Tung University. He received Ph.D. degree in Electrical Engineering from National Cheng Kung University. He is presently a professor in the Department of Computer Science and Information Engineering at National Dong Hwa University, and is also an IEEE senior member. He has published a number of journal and conference papers in the areas of information security, multimedia security and coding theory. He is the guest editor of a special issue on “Visual Cryptography Scheme” for Communication of CCISA, and a coauthor of a series of articles on “Image Secret Sharing” for the Encyclopedia of Multimedia. He is the coeditor of the book “Visual Cryptography and Secret Image Sharing” published by CRC Press/Taylor & Francis. He serves as a technical reviewer for over 30 major scientific journals in the areas of his expertise, and serves as editorial boards of some journals. Also, has served member of program committees of various international conferences committees. He is the recipient of the 2000, 2006, 2010 and 2012 Fine Advising Award in the Thesis of Master of Science awarded by Institute of Information & Computer Machinery.