Design of Secure Watermarking Scheme for Watermarking Protocol

Bin Zhao[1], Lanjun Dang[1], Weidong Kou[1], Jun Zhang[2], and Xuefei Cao[1]

[1] The State Key Laboratory of ISN, Xidian University, Xi'an, 710071, China
{binzhao, ljdang, wdkou, xfcao}@mail.xidian.edu.cn
[2] School of CSSE, University of Wollongong, Wollongong, NSW 2522, Australia
jz484@uow.edu.au

Abstract. Watermarking technique enables to hide an imperceptible watermark into a multimedia content for copyright protection. However, in most conventional watermarking schemes, the watermark is embedded solely by the seller, and both the seller and the buyer know the watermarked copy, which causes unsettled dispute at the phase of arbitration. To solve this problem, many watermarking protocols have been proposed using watermarking scheme in the encrypted domain. In this paper, we firstly discuss many security aspects in the encrypted domain, and then propose a new method of homomorphism conversion for probabilistic public key cryptosystem with homomorphic property. Based on our previous work, a new secure watermarking scheme for watermarking protocol is presented using a new embedding strategy in the encrypted domain. We employ an El Gamal variant cryptosystem with additive homomorphic property to reduce the computing overload of watermark embedding in the encrypted domain, and RA code to improve the robustness of the watermarked image against many moderate attacks after decryption. Security analysis and experiment demonstrate that the secure watermarking scheme is more suitable for implementing the existing watermarking protocols.

1 Introduction

With rapid development of information technology, most multimedia contents have become available in digital form, which makes it possible to reproduce perfect copies of digital image, video, and other multimedia contents. The increasing concern about copyright protection is due to the fact that a large number of digital multimedia contents have been illegal distributed at the cost of a huge amount of valid profit. A promising technique for copyright protection is digital watermarking that enables to hide an imperceptible watermark into a multimedia content while preserving quality. In most conventional watermarking schemes, the watermark is embedded solely by the seller in behalf of intellectual property, and then the seller send the watermarked copy to the buyer. Since both the seller and the buyer know the watermarked copy, it causes unsettled dispute at the phase of arbitration. Thus, the watermark could not be considered as legally sufficient evidence for accusing copyright violation.

It is significant in the sense that the watermarking framework needs protocols to solve both the resolution of the rightful ownership problem and the protection of the

H.H.S. Ip et al. (Eds.): PCM 2007, LNCS 4810, pp. 357–366, 2007.

customer's right problem, which is first introduced by L. Qiao and K. Nahrstedt [1]. An effective buyer-seller watermarking protocol is expected to mostly satisfy the following important requirements.

1. No Repudiation (Seller's Security): A guilty buyer producing unauthorized copies should not repudiate the fact and not able to claim that the copies were possibly made by the seller.
2. No Framing (Buyer's Security): An honest buyer should not be falsely accused for reparation by a malicious seller who can reuse the embedded watermark to frame.
3. Traceability: A guilty buyer (traitor / copyright violator) who has illegally distributed digital contents can be traced.
4. Anonymity: A buyer should be able to purchase digital contents anonymously.

For these reasons, many watermarking protocols have been proposed based on the watermarking scheme in the encrypted domain. In such a condition, the seller can not produce copies containing the watermark identifying the buyer, because he can not know the exact watermark from the ciphertext in the embedding procedure. When an illegal copy is found, the seller can prove to a third party that the buyer is certainly guilty. N. Memon and P. W. Wong [2] presented a buyer-seller watermarking protocol to resolve both the pirate tracing problem and the buyer's right problem. Successively, Chin-Laung Lei *et al.* [3] pointed out the unbinding problem and proposed an efficient and anonymous buyer-seller watermarking protocol. Recently, J. Zhang *et al.* [4] proposed a secure buyer-seller watermarking protocol based on the idea of sharing a secret. Additionally, M. Kuribayashi and H. Tanaka [5] presented an anonymous fingerprinting protocol and a quantization-based scheme for embedding encrypted watermark bits by additive homomorphic property.

We aim to promote watermarking schemes and watermarking protocols into real-world application. In this paper, we take many security aspects into consideration and propose a new secure watermarking scheme for watermarking protocol based on our previous work. Our contributions to the secure watermarking scheme involve many facets. (1) A new method of homomorphism conversion between multiplicative and additive are proposed for probabilistic public key cryptosystem with homomorphic property. (2) A new embedding strategy in the encrypted domain is presented to simplify embedding steps and provides another secret key. (3) An El Gamal variant cryptosystem with additive homomorphic property is employed to reduce the computing overload of watermark embedding in the encrypted domain. (4) RA code is used to deal with the synchronization issue and bit errors, and it also improves the robustness of the watermarked image against many moderate attacks after decryption.

2 Security Aspects in the Encrypted Domain

2.1 Probabilistic Public Key Cryptosystem with Homomorphic Property

The conventional public key cryptosystem has been considered as functions $E(\bullet)$ in such a way that the message M presumably cannot be computed from the encryption $E(M)$. However, even if the adversary cannot identify M exactly, he may be able to obtain some partial information about M, for example tell whether M is an even number

or odd, etc. An extreme case of this problem exist in watermarking schemes in the encrypted domain, because the watermark represented by 0 and 1 is encrypted bit by bit separately, and the adversary knows each encrypted bit is one of two possibilities, 0 or 1. Since the same public key is employed to encrypt each watermark bit, what the adversary needs to do is compare $E(0)$ and $E(1)$ with each ciphertext $E(M)$. Hence, he can know the entire watermark bits by this means, which causes both framing issue and repudiation issue as mentioned before. Therefore, deterministic public key cryptosystems could not be used in the watermarking protocols, for example, the plain RSA cryptosystem [6].

Probabilistic public key cryptosystem, first introduced by Shafi Goldwasser and Silvio Micali [7], could be employed to solve this problem. Instead of $E(M)$ being a single determinate ciphertext, the same message M has many different ciphertexts at different time, and the ciphertexts of different messages is indistinguishable, because $E(M)$ involves a random number r during encryption.

A public key cryptosystem used in watermarking protocols should have homomorphic property, either additive or multiplicative homomorphism, which means multiplying two ciphertexts $E(x,r_1)$ and $E(y,r_2)$ leads to addition or multiplication of two plaintexts x and y after decryption.

$$D(E(x,r_1)\bullet E(y,r_2)) = D(E(x+y,r')) = x+y \mod n \tag{1}$$

$$D(E(x,r_1)\bullet E(y,r_2)) = D(E(x\bullet y,r')) = x\bullet y \mod n \tag{2}$$

It is known that El Gamal cryptosystem [8], Paillier cryptosystem [9] and Okamoto-Uchiyama cryptosystem [10] are probabilistic with homomorphic property. El Gamal cryptosystem is multiplicative homomorphism, while Paillier cryptosystem and Okamoto-Uchiyama cryptosystem are additive homomorphism.

2.2 New Method of Homomorphism Conversion and El Gamal Variant Cryptosystem

In many watermarking protocols, watermark embedding relies significantly on the public key cryptosystem with additive homomorphic property. In some scenarios, the constraint on the type of cryptosystem limits the flexibility of watermarking protocol. For instance, El Gamal cryptosystem, a well-known public key cryptosystem with multiplicative homomorphism, appears unsuitable for the watermarking protocol based on the additive homomorphic property in [5]. As for practical applications, it is necessary to provide more types of public key cryptosystem for watermarking schemes in the encrypted domain.

Fortunately, a simple exponential-logarithmic method can mutually convert homomorphism between multiplicative and additive. homomorphism conversion from multiplicative to additive could be achieved by means of replacing x by an exponential operation based on g.

$$\begin{aligned} D(E(g^x,r_1)\bullet E(g^y,r_2)) &= D(E(g^x\bullet g^y,r')) \\ &= D(E(g^{x+y},r')) \\ &= g^{x+y} \mod n \end{aligned} \tag{3}$$

The inverse conversion from additive to multiplicative could be achieved by means of replacing x by a logarithmic operation based on g.

$$\begin{aligned} D(E(\log_g x, r_1) \bullet E(\log_g y, r_2)) &= D(E(\log_g x + \log_g y, r')) \\ &= D(E(\log_g (x \bullet y), r')) \\ &= \log_g (x \bullet y) \mod n \end{aligned} \tag{4}$$

Essentially, a variant of original El Gamal cryptosystem has the same additive homomorphic property. Let n be a secure large prime number and g be a generator of $\boldsymbol{Z}_n^*$. A public key y is defined by $y = g^x \bmod n$ where $x \in \boldsymbol{Z}_{n-1}$ is a private key.

[Encryption] Let g^m be a plaintext to be encrypted, where $0 \le g^m \le (n-1)$, and r be a random number chosen from $\boldsymbol{Z}_{n-1}$.

$$E(m, r) = (B; C) \quad \text{where } B = g^m \bullet y^r \bmod n \text{ and } C = g^r \bmod n \tag{5}$$

[Decryption] Extract the two parts c and d from the ciphertext, the decrypted plaintext is:

$$D(E(m, r)) = B \bullet C^{-x} = g^m \bullet y^r \bullet g^{-x \bullet r} = g^m \bullet g^{x \bullet r} \bullet g^{-x \bullet r} = g^m \mod n \tag{6}$$

Then compute the original message m from a logarithmic operation without modular arithmetic.

$$m = \log_g (g^m) \tag{7}$$

The El Gamal variant cryptosystem is as secure as the original El Gamal cryptosystem [8] based on the difficulty of the discreet logarithm problem in finite fields, which is too difficult to solve. This variant cryptosystem is of ideal semantic security, because the plaintext m is just replaced by a power of g in a cyclic group [11]. The additive homomorphic property of this variant cryptosystem can be represented as following.

$$\begin{aligned} D(E(x, r_1) \bullet E(y, r_2)) &= D((B; C) \bullet (F; G)) \\ &= D((B \bullet F; C \bullet G)) \\ &= D(E(x + y, r_1 + r_2)) \\ &= x + y \mod n \end{aligned} \tag{8}$$

3 Secure Watermarking Scheme for Watermarking Protocol

In the watermarking protocols [2]-[5], for the sake of no repudiation and no framing, watermark bits should be encrypted by the buyer's public key unexposed to the seller. As watermark embedder, the seller usually has the original image and the encrypted watermark bits. Using the watermarking scheme in the encrypted domain, the seller can embed the encrypted watermark bits into the encrypted host image, and then he sends the encrypted watermarked image to the buyer.

This work is a further extension of our previous research [12], which enhances the original SEC scheme in [13] and then applies the enhanced scheme in the encrypted domain using the embedding method proposed in [5]. Here, we propose a new embedding strategy to embed encrypted watermark bits into encrypted selected coefficients, and apply it to our previous work. Compared with the embedding method in [5], the new embedding strategy in the encrypted domain simplifies embedding steps and provides the odd-even information of cutoff result as another secret key. In this section, we briefly summarize a new secure watermarking scheme for watermarking protocol, and the detailed steps can be referred to [12].

3.1 Watermark Embedding

In watermark embedding procedure, the seller should save many parameters as a set of secret keys, such as a positive integer threshold t for the threshold criterion, the value of designated QF, the number N of candidate coefficients per block in a fixed low frequency band ($1 \le k \le N$), a random permutation $P(\bullet)$, and the odd-even information *INFO* of cutoff result.

After 8×8 block partition, DCT, division by the quantization table at designated QF and zig-zag scanning, in a fixed low frequency band ($1 \le k \le N$), the quantized coefficient $\widehat{c_k}$ whose magnitude lies between threshold t and (t+1) are rounded to the nearest integer as a preprocessing.

$$\widehat{c_k} = \begin{cases} \pm t, & \text{if } t < \left|\widehat{c_k}\right| < (t+\frac{1}{2}), \text{ and } 1 \le k \le N, \\ \pm(t+1), & \text{if } (t+\frac{1}{2}) \le \left|\widehat{c_k}\right| < (t+1), \text{ and } 1 \le k \le N, \\ \widehat{c_k}, & \text{otherwise.} \end{cases} \tag{9}$$

The new embedding strategy is employed in the following steps. The quantized coefficients $\widehat{c_k}$ in a fixed low frequency band ($1 \le k \le N$) whose magnitude $\left|\widehat{c_k}\right|$ is greater than threshold t as the threshold criterion are selected and cutoff to the nearest integer $\overline{c_k}$ whose magnitude is less than $\widehat{c_k}$. The odd-even information *INFO* of cutoff result $\overline{c_k}$ is saved for watermark extracting.

$$\overline{c_k} = \text{int}_{cutoff}(\widehat{c_k}), \quad \text{for } \left|\widehat{c_k}\right| > t, \text{ and } 1 \le k \le N. \tag{10}$$

All the selected coefficients $\overline{c_k}$ are inverse zig-zag scanned to obtain $\overline{c_{ij}}$ and then every $\overline{c_{ij}}$ is encrypted with the buyer's public key and a random number b_n to calculate the encrypted coefficient $E(\overline{c_{ij}}, b_n)$. Note that each embedding position is represented by subindex ij in that block.

In the embedding positions, the encrypted watermarked coefficients $E(\overline{d'_{ij}}, r')$ can be calculated by multiplying two ciphertexts $E(\overline{c_{ij}}, b_n)$ and $E(w_p, a_m)$.

$$\begin{aligned} E(\overline{d'_{ij}}, r') &= (E(\overline{c_{ij}}, b_n) \bullet E(w_p, a_m))^{M_{ij}^{QF}} \\ &= (E(\overline{c_{ij}} + w_p, b_n + a_m))^{M_{ij}^{QF}} \\ &= E((\overline{c_{ij}} + w_p) \bullet M_{ij}^{QF}, (b_n + a_m) \bullet M_{ij}^{QF}) \end{aligned} \tag{11}$$

In the other positions, the unwatermarked coefficients are rounded to the nearest integer by the following operations.

$$\overline{d_{ij}} = \begin{cases} \text{int}_{near}(c_{ij}), & \text{for } 0 \le \left|\widehat{c_k}\right| < t, \text{ and } 1 \le k \le \text{N}, \\ \pm t \bullet M_{ij}^{QF}, & \text{for } \left|\widehat{c_k}\right| = t, \text{ and } 1 \le k \le \text{N}, \\ \text{int}_{near}(c_{ij}), & \text{for } \forall \left|\widehat{c_k}\right|, \text{ and } k = 0 \bigcup \text{N} < k \le 63. \end{cases} \tag{12}$$

Then, each $\overline{d_{ij}}$ is encrypted with the same public key as encrypted watermark and a random number *r* to obtain ciphertext $E(\overline{d_{ij}}, r)$. After block-by-block processing, seller obtains all the encrypted DCT coefficients of the watermarked image, and then he sends them to buyer. Finally, buyer obtains the watermarked image by decrypting all the DCT coefficients and employing IDCT to gain his image in plaintext.

3.2 Watermark Extracting

In watermark extracting procedure, watermark extractor uses the same threshold criterion and secret keys as the watermark embedder to extract the watermark bits.

After 8×8 block partition, DCT, division by the quantization table at designated QF and zig-zag scanning, in a fixed low frequency band ($1 \le k \le \text{N}$), all the quantized DCT coefficients are rounded to the nearest integer. The quantized DCT coefficient integers $\overline{d_k}$ whose magnitude is greater than the threshold *t* as the same threshold criterion are considered as embedding a watermark bit. Hence, every watermark bit w_p can be readily extracted using the following judgments.

If *INFO* is odd, then

$$w_p = \begin{cases} 0, & \text{if } \overline{d_k} \text{ is odd}, \quad \left|\overline{d_k}\right| > t, \text{ and } 1 \le k \le \text{N}, \\ 1, & \text{if } \overline{d_k} \text{ is even}, \quad \left|\overline{d_k}\right| > t, \text{ and } 1 \le k \le \text{N}. \end{cases} \tag{13}$$

Else *INFO* is even, then

$$w_p = \begin{cases} 1, & \text{if } \overline{d_k} \text{ is odd}, \quad \left|\overline{d_k}\right| > t, \text{ and } 1 \le k \le \text{N}, \\ 0, & \text{if } \overline{d_k} \text{ is even}, \quad \left|\overline{d_k}\right| > t, \text{ and } 1 \le k \le \text{N}. \end{cases} \tag{14}$$

4 Security Analysis

For the El Gamal variant cryptosystem, the security certification relays sufficiently on the following testimonies. (1)The El Gamal variant cryptosystem is based on the difficulty of the discreet logarithm problem in finite fields. (2) The El Gamal variant cryptosystem is of semantic security. (3) The El Gamal variant cryptosystem is probabilistic cryptosystem with additive homomorphic property.

For both seller's security and buyer's security, firstly, because the watermark is embedded in the encrypted domain, the seller can not know the exact watermark from the ciphertext. In addition, only the buyer can obtain the watermarked image, since the watermarked image is encrypted by the buyer's public key and no one knows the private key to decrypt it. On the one hand, the seller can not reproduce the watermarked image, and a guilty buyer making unauthorized copies could not repudiate the fact. On the other hand, the seller can not obtain the embedded watermarked, and an honest buyer can not be framed by a malicious seller.

For traceability, if the buyer never redistributes an unauthorized copy to the market, he is innocent and the watermark is concealed. If the buyer's watermark is found in an illegal copy, the seller can trace the buyer's identity and prove that the buyer is certainly guilty using watermark as legally sufficient evidence.

For anonymity, it is supplied by watermarking protocol, not by watermarking scheme in the encrypted domain.

5 Experimental Results

All the tests were performed on the 256×256 grayscale image "Lena", the same test image reported in [5]. The enciphering rate of both El Gamal variant cryptosystem and Paillier cryptosystem is 1/2, which is higher than that of Okamoto-Uchiyama cryptosystem 1/3. For the sake of less ciphertext length and higher computing efficiency, $|n|$=512-bit El Gamal variant cryptosystem with additive homomorphic property is employed in our experiments. One benefit of this variant cryptosystem is that the computing overload of watermark embedding is reduced to a large extent by multiplying two times the corresponding ciphertext parts with half ciphertext length, rather than multiplying two ciphertexts with full ciphertext length at one time.

Error correction code with powerful erasure and error correction is proved to be a good solution to deal with the synchronization issue and bit errors in the previous watermarking scheme in the encrypted domain [12]. RA code [14], an effective error correction code, is used in our experiments because of flexible coding rate, simple realization and near-capacity correction performance in erasure channels. At a specified rate $1/q$, RA encoding involves q-repetition, random interleaving, and bitstream accumulation. Decoding employs the soft-decision iterative sum-product algorithm [15]. The length of RA code is defined by the range of candidate coefficients in a fixed low frequency band ($1 \le k \le$N) (this parameter N can be changed, and it is independent of the host image). In our experiments, 20 DCT coefficients per block are used in a given low frequency band ($1 \le k \le 20$), and then the total watermark bitstream length of a 256×256 image with 1024 8×8 blocks is 20×1024=20480.

5.1 Watermarking Capacity Without RA Coding

The secure watermarking scheme has a flexible watermarking capacity in a given host image by adjusting many parameters. Watermark bits are embedded into the image "Lena" at designated QF 50 in different low frequency bands ($1 \le k \le N$). All of the embedded watermark bits are equiprobably and independently generated with $p(1) = p(0) = 0.5$, and each result is the average over a large number of repeated tests. Table 1 reports the number of embedded watermark bits and corresponding PSNR of watermarked images after decryption. Note that the number of watermark bits reported here is actually the number of uncoded bits.

Table 1. The number of embedded watermark bits and PSNR with different parameters

QF=50	N=9		N=14		N=20	
Threshold t	Embed bits	PSNR (dB)	Embed bits	PSNR (dB)	Embed bits	PSNR (dB)
0	5450	39.41	7011	36.86	8051	34.76
1	3277	42.24	3828	40.78	4095	39.67
2	2382	43.86	2628	42.89	2724	42.24
3	1826	44.87	1948	44.28	1979	44.02
4	1438	45.85	1502	45.45	1511	45.33
5	1178	46.55	1208	46.29	1211	46.28

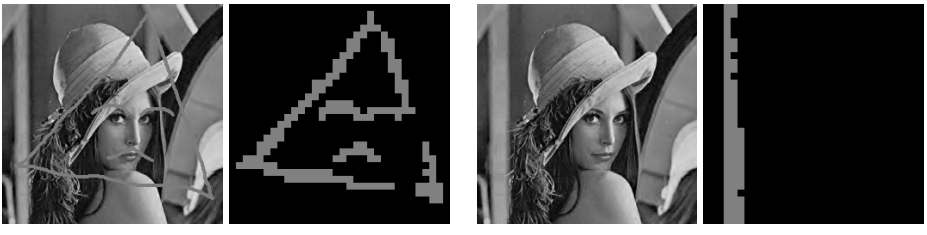
5.2 JPEG Compression Resistance

Since the previous watermarking scheme in the encrypted domain [12] is tuned to JPEG quantization table [16], the embedded watermark bits are efficient enough for free bit-error recovery against the JPEG compression less severe than the designated QF. As for the secure watermarking scheme, RA code can further improve the resistance against the JPEG compression more severe than the designated QF to a limited extent. For example, at RA coding rate 1/20, all the 1024-bit information in a watermarked image with parameters of QF=50, t=1, N=20 can be perfectly retrieved at the QF value of JPEG compression greater than 40, which is the same performance of the one with parameters of QF=25, t=3, N=14 in the previous watermarking scheme.

5.3 Image Tampering Tolerance and Detection

The secure watermarking scheme with RA coding can resist a limited amount of image tampering on the watermarked image and detect the tampered area in block level. If the watermarked image has undergone tampering, the tampered area in the watermarked image can be easily located. First, original information bits are retrieved by decoding the watermark bitstream from the tampered image. Second, the originally embedded RA bitstream is reconstructed by encoding the retrieved information bits again with the same parameters as original coding. Finally, by comparing the extracted watermark bitstream with the original RA bitstream, the tampered areas are indicated by where the errors exist.

In order to resist limited image tampering, the RA coding rate designated in watermark generation phase should be low enough to withstand limited erasures and errors and to decode information bits successfully. For example, at RA coding rate 1/40, all the 512-bit information in a watermarked image with the parameter of QF=50, t=1, N=20, PSNR=39.4083dB can withstand a global tampering with the gray value 128. In another case, at RA coding rate 1/32, all the 640-bit information in a watermarked image with the parameter of QF=50, t=1, N=20, PSNR=39.2729dB can withstand a local tampering with block shifting in an unobvious manner. Fig. 1 (a) and (c) display the watermarked images with global tampering (PSNR=24.8906) and local tampering (PSNR=26.9398) respectively. Fig. 1 (b) and (d) show the localization of tampered area in block level according to the tampered image.



(a) (b) (c) (d)

Fig. 1. Watermarked image with global tampering and local tampering

5.4 Other Attacks Resistance

The secure watermarking scheme presented in this paper can also resist many moderate attacks on the watermarked image after decryption. For example, additive noise, low-pass filtering, gaussian filtering, median filtering and image resizing. The lower RA coding rate designated in watermark generation phase, the higher ability to survive more intense attacks. However, this watermarking scheme fails to withstand several geometric attacks, such as rotation and cropping.

6 Conclusion

In this paper, we discuss some security aspects in the encrypted domain and propose a new method of homomorphism conversion for probabilistic public key cryptosystem with homomorphic property. Based on our previous work [12], a new secure watermarking scheme for watermarking protocol is presented, in which we employ a new embedding strategy in the encrypted domain. It simplifies embedding steps and provides another secret key. The El Gamal variant cryptosystem with additive homomorphic property is used to reduce the computing overload of watermark embedding in the encrypted domain. RA code deals with the synchronization issue and bit errors, and it also improves the robustness of watermarked image against many moderate attacks after decryption. As security analysis and experiment shows, the secure watermarking scheme is more suitable for implementing the existing watermarking protocols.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 90304008, the College and University Subject of Doctors Specific Scientific Research Foundation of China under Grant 2004071001, and the Graduate Innovation Fund of Xidian University 05017 and 05019.

References

1. Qiao, L., Nahrstedt, K.: Watermarking schemes and protocols for protecting rightful ownerships and customer's rights. Journal of Visual Communication and Image Representation 3, 194–210 (1998)
2. Memon, N., Wong, P.W.: A buyer-seller watermarking protocol. IEEE Trans. Image Processing 4, 643–649 (2001)
3. Lei, C.L., Yu, P.L., Tsai, P.L., Chan, M.H.: An efficient and anonymous buyer-seller watermarking protocol. IEEE Trans. Image Processing 12, 1618–1626 (2004)
4. Zhang, J., Kou, W., Fan, K.: Secure buyer-seller watermarking protocol. IEE Proceeding of Information Security 1, 15–18 (2006)
5. Kuribayashi, M., Tanaka, H.: Fingerprinting protocol for images based on additive homomorphic property. IEEE Trans. Image Processing 12, 2129–2139 (2005)
6. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM 2, 120–126 (1978)
7. Goldwasser, S., Micali, S.: Probabilistic encryption. Journal of Computer and System Sciences 2, 270–299 (1984)
8. El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory 4, 472–649 (1985)
9. Paillier, P.: Public key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)
10. Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 308–318. Springer, Heidelberg (1998)
11. Mao, W.: Modern Cryptography: Theory and Practice. Prentice-Hall, Englewood Cliffs (2003)
12. Tong, X., Zhang, J., Wen, Q.-Y.: New Constructions of Large Binary Sequences Family with Low Correlation. In: Lipmaa, H., Yung, M., Lin, D. (eds.) INSCRYPT 2007. LNCS, vol. 4318, Springer, Heidelberg (2007)
13. Solanki, K., Jacobsen, N., Madhow, U., Manjunath, B.S., Chandrasekaran, S.: Robust image-adaptive data hiding using erasure and error correction. IEEE Trans. Image Processing 12, 1627–1639 (2004)
14. Divsalar, D., Jin, H., McEliece, R.J.: Coding theorems for turbo-like codes. In: Proc. 36th Allerton Conf. Communications, Control, Computing, pp. 201–210 (1998)
15. Kschischang, F.R., Frey, B.J., Loeliger, H.-A.: Factor graphs and the sum-product algorithm. IEEE Trans. Inform. Theory 2, 498–519 (2001)
16. Wallace, G.K.: The JPEG still picture compression standard. Communications of the ACM 4, 30–44 (1991)