IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014.
www.ijiset.com
ISSN 2348 – 7968

Robust Watermarking of Compressed and Encrypted JPEG2000 Images: Overview

Bhagyashri D. Shende[1], Prof. Mrs. R. J. Shelke[2]

[1] Department of M.E. Electronics, Walchand Institute of Technology, Solapur University, Solapur, Maharashtra, India

[2] Department of M.E. Electronics, Walchand Institute of Technology, Solapur University, Solapur, Maharashtra, India

Abstract

The need for copyright protection, ownership verification, and other issues for digital data are getting more and more importance nowadays. Among the solutions for these issues, digital watermarking techniques are used. A range of watermarking methods has been estimated. Compression plays a significant role in the design of watermarking algorithms. For a digital watermarking method to be efficient, it is very important that an embedded watermark should be robust against compression. JPEG2000 is a new standard for image compression and transmission. The proposed method is a robust watermarking algorithm to watermark JPEG2000 compressed and encrypted images (grayscale) of size 512×512. The encryption algorithm in this method uses stream cipher algorithm. While the projected technique embeds watermark in the compressed-encrypted domain, the extraction of watermark can be done in the encrypted domain. The proposed algorithm also preserves the secrecy of content as the embedding process can be done on encrypted data. The proposed method can investigate the PSNR and the security of the proposed algorithm, using the three watermarking schemes: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).

Keywords: *JPEG2000 Compression, Stream Cipher, Watermarking Techniques such as SS, SCS-QIM, RDM.*

1. Introduction

Digital watermarking is the process of embedding information into digital multimedia content such that the information which we call the watermark can later be extracted or detected for a variety of purposes including copy prevention and control. Basically Digital Asset Management System (DAMS) contain various assets like image, audio, video, logo etc. principally, DAMS means the grouping of hardware, software, professional services that provides central location for storing, managing, retrieving the digital assets [3]. These assets contain some additional information hence it is accessible to only intended users. The owner of multimedia content distributes these assets to consumer through multiple levels of distributers. As distributors are not consumers hence they cannot access the original message. Hence it is essential to compress and encrypt digital assets before its distribution. Sometimes there is possibility of losing the data hence watermarking should be done for copyright protection. [2] Therefore the proposed method introduces a robust watermarking technique for JPEG2000 images (grayscale) of size 512×512 in which watermark can be embedded in conventional manner in compressed an encrypted byte stream. This method uses JPEG2000 compression standard which provides lot of benefits over JPEG such as ROI capacity, transmission in noisy environment, high compression efficiency etc. As the compression provides less transmission time and less storage space hence compression can be done before encryption. The combination of encryption and watermarking provides robust security of image. This watermarking algorithm can be evaluated by investigating the watermarked image quality using one of these watermarking schemes: Spread Spectrum (SS) and Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), Rational Dither Modulation (RDM) [1].

ISSN 2348 – 7968

2. Related Work

Digital media content creation/capturing, processing and distribution have witnessed a phenomenal growth over the past decade. This media content is often distributed in compressed and encrypted format and watermarking of these media for copyright violation detection, proof of ownership or distributorship, media authentication, sometimes need to be carried out in compressed-encrypted domain. There have been several related image watermarking techniques proposed. The DAMS (Digital Asset Management System) generally consist of multiple levels of owners, distributors and consumers. But the distributors are not the consumers hence they cannot access the original data. Sometimes it is necessary to watermark the original message for the purpose of not only authentication but also copy right violation detection. [1]-[4]. Thus watermarking should be done after compressing and encrypting the data. In this paper, digital asset is considered as image (grayscale). First image is compressed using JPEG2000 standard; compression can be done because it reduces the storage space requirement. Compression can be done because it provides less storage space. Then compressed image can be encrypted using stream cipher algorithm. Here encryption refers to the complete ciphering of compressed bit stream. And then watermarking technique can be applied [5]. The various image watermarking techniques are projected now days. [6]-[11]. In [6],Deng et al. projected an efficient buyer-seller watermarking protocol based on composite signal representation given in [7]where the host signal and the embedding signal are represented in a composite format. However, the watermark embedder can access the content only in encrypted form, then the embedding scheme proposed in [6] will not be applicable since the host and watermark signal are represented in composite signal from using the plaintext features of the host signal and in [6], this is possible as the seller embeds the watermark. The cipher text has an expansion of 3.8 times that of plaintext. In [8] and [9], lower resolution sub-bands encrypted while higher resolution sub-bands are chosen for watermarking. While in [10], on the most significant bit planes encryption is performed. While on the rest of the lower significant bit planes watermarking is performed. An attacker can manipulate the unencrypted sub-bands/bit planes and extract some useful secret information from the image if lesser number of sub-bands/bit planes is used for encryption, even if the image is not of good quality. On the other hand, it can be possible for an attacker to remove the watermarked sub-bands/bit planes if more sub-bands/bit planes are encrypted and only rest few sub-bands/bit planes are watermarked. Prins et al. in [11] proposed a robust quantization index modulation (QIM) watermarking technique. This technique embeds the watermark in the encrypted domain. In the technique proposed in [11], based on the value of the quantized coefficients the addition or subtraction of a watermark bit to a sample is done. However, in the proposed algorithm, the distributor who embeds the watermark bits does not have access to the plain text. Only compressed and encrypted content is available to them. Also the distributors do not have the key to unencrypted the ciphered text and get the plaintext values. Thus, watermarking in compressed-encrypted domain using the technique proposed in [11] is very difficult. Hence there is a need of robust watermarking scheme. The proposed system introduces the robust watermarking scheme of compressed and encrypted JPEG2000 images as watermarking in compressed-encrypted content saves the computational complexity [1]

3. Proposed Scheme

In the proposed algorithm, the image is compressed using JPEG2000 standard and encrypted, the watermark is embedded on the compressed and encrypted image and extraction of watermark is done from encrypted domain.[1] Consider the following figure which gives overall idea about the proposed scheme.

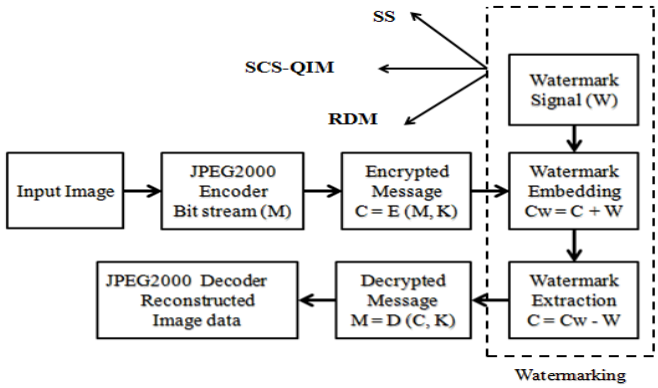

Fig: 1: Block Diagram of Proposed Scheme

Considering the above scenario of proposed system, first image can be taken (grayscale) and it is compressed using JPEG2000 standard. After that, the image is encrypted using stream cipher algorithm. The encrypted image is

ISSN 2348 – 7968

given to the block embedding watermark as an input. The watermark is embedded in the encrypted image using one of the three different watermarking techniques: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM). After embedding a watermark in an encrypted image, the watermark can be detected from the encrypted watermarked image then the image can be decrypted to get the original image. The detail description of each block is explained in following section.

3.1 JPEG2000 Compression

JPEG 2000 is an image compression standard and coding system. It was created by the Joint Photographic Experts Group committee in 2000 with the intention of superseding their original discrete cosine transform-based JPEG standard with a newly designed, wavelet-based method. The standardized filename extension is .jp2. This new standard has been developed to meet the demand for efficient, flexible, and interactive image representations. JPEG2000 is much more than a compression algorithm, opening up new paradigms for interacting with digital imagery [1], [13]. The following figure shows the functional block diagram of JPEG2000 encoder and decoder.

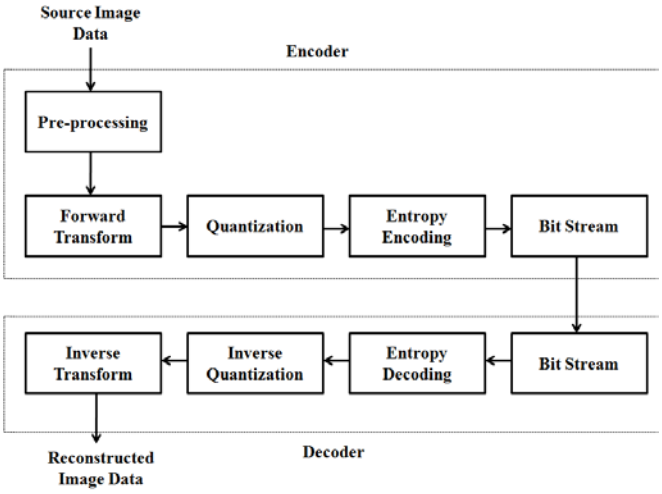

Fig: 2: JPEG2000 Encoder and Decoder

In jpeg2000 encoder stage, the input source image data is grayscale image of size 512×512 which is given to the pre-processing phase. In pre-processing, two types of operations are performed such as tiling and DC level shift. In tiling, the input source image is partitioned into a number of rectangular non overlapping blocks if the image is very large. Each of these blocks is called a tile. All the tiles have exactly the same dimension except the tiles at the image boundary if the dimension of the image is not an integer multiple of the dimension of the tiles. The tile sizes can be arbitrary up to the size of the original image. For a grayscale image, the tile has a single component. After that DC level shifting operation is performed. Originally, the pixels in the image are stored in unsigned integers. For mathematical computation, it is essential to convert the samples into two's complement representation before any transformation or mathematical computation starts in the image. The purpose of DC level shifting is to ensure that the input image samples have a dynamic range that is approximately centered on the zero. The DC level shifting is performed on image samples that are represented by unsigned integers only. All samples $Ii(x,y)$ in the ith component of the image (or tile) are level shifted by subtracting the same quantity $2Ssizi-1$ to produce the DC level shifted sample $Ii'(x,y)$ as follows, $Ii'\ x, \leftarrow Ii\ x, -2Ssizi-1$ Where $2Ssizi-1$ is precision of image samples signaled in the SIZE (image and tile size) marker while the higher resolution contains the high-pass image. The next step is Quantization. After transformation, all coefficients are quantized. Quantization is the process by which the coefficients are reduced in precision. This operation is lossy, unless the quantization step is 1 and the coefficients are segments in the compressed bit stream. The output of pre-processing unit is given to the forward transform. In JPEG 2000 Discrete Wavelet Transform (DWT) is used to decompose each tile component into different sub bands. The transform is in the form of dyadic decomposition and use biorthogonal wavelets. Multiple levels of DWT give a multi-resolution image. The lowest resolution contains the low-pass image integers, as produced by the reversible integer 5/3 wavelet. Each of the transform coefficients $a_b(u,v)$ of the sub band b is quantized to the value $q_b(u,v)$ according to

$$q_b(u,v) = \text{sign}\left(a_b(u,v)\right)\left[\frac{|a_b(u,v)|}{\Delta_b}\right]$$

Where, $q_b(u,v)$ = Quantized value
$a_b(u,v)$ = Transform coefficients of subband b
Δb = Quantization step size

The quantization step-size Δb is represented relative to the dynamic range of sub band b. After that encoding process occurred. These entropy encoders then compress data by

ISSN 2348 – 7968

replacing each fixed length input symbol with the corresponding variable-length prefix-free output codeword. In JPEG 2000 Huffman Encoding is used for encoding the quantized coefficients. Huffman coding is based on the frequency of occurrence of pixel in images. The principle is to use a lower number of bits to encode the data that occurs more frequently and larger number of bits to encode data that occur less frequently. This compressed byte stream is arranged into different wavelet packets based on resolution, precincts, components and layers in the fifth and final stage. Thus, it is possible to select bytes generated from different bit planes of different resolutions for encryption and watermarking. [18].

3.2 Encryption and Decryption

A secure symmetric stream cipher with homomorphic property is used for encryption here. It is mainly due to the following two reasons. Symmetric ciphers with homomorphism can be applied on a smaller message size, like a byte, without increasing the compressed data size and achieving a better payload capacity than asymmetric counterparts. So there is a tradeoff between security-compression efficiency-payload capacities, which poses a challenge for deciding which cipher scheme to apply. [4], [5]. Therefore it uses the RC4 stream cipher with homomorphism property. It uses a variable sized key that can range between 8 and 2048 bits in multiples of 8 bits. Since it is a stream cipher Byte by Byte encryption is done. A typical stream cipher encrypts plaintext one byte at a time; although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time. In this, a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are apparently random. A pseudorandom stream is one that is generated by an algorithm but is unpredictable without knowledge of the input key. The output of the generator, called a key stream, is combined one byte at a time with the plaintext stream using the bitwise exclusive-OR (XOR) operation.[10][14].

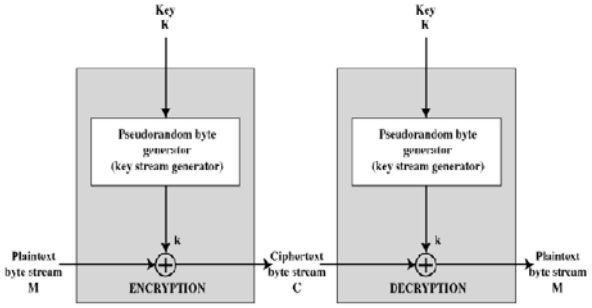

Fig. 3: Stream Cipher basic structure

RC4 is a stream cipher using a symmetric key. The key stream is generated from a variable length key using an internal state composed of the following elements:

1. A 256 bytes array (denoted S) containing a permutation of these 256 bytes
2. Two indexes i and j, used to point elements in the S array (only 8 bits are necessary for each index since the array only have 256 elements)

Once the S array has been initialized and "shuffled" with the key-scheduling algorithm (KSA), it is used and modified in the pseudo-random generation algorithm (PRGA) to generate the key stream. RC4 algorithm has got 2 stages. [16][17].

3.2.1 Key scheduling algorithm

The key-scheduling algorithm is used to generate the permutation array. The first step of this algorithm consist in initializing the S table with the identity permutation: the values in the array are equal to their index.

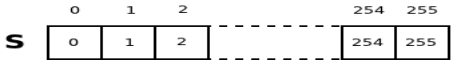

Fig.4: S Table

Once the S array is initialized, the next step consists is shuffling the array using the key to make it a permutation array. To do so, we simply iterate 256 times the following actions after initializing i and j to 0:

Compute j = j + S[i] + key [i mod key length]
Swap S[i] and S[j]
Increment i

ISSN 2348 – 7968

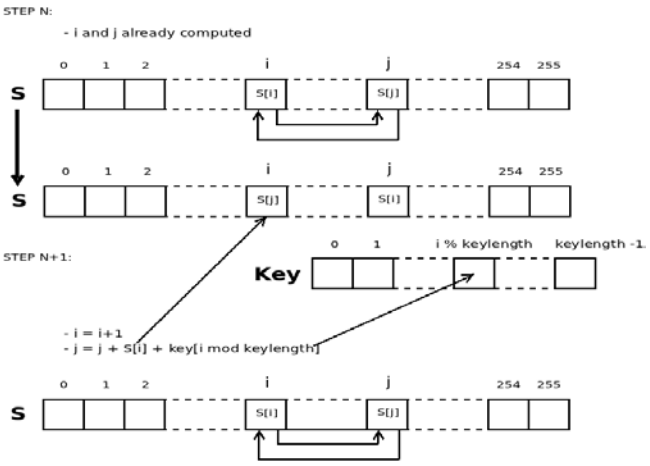

Fig.5: Key Scheduling Algorithm

Once i have reached 256, the S array has been properly initialized. Here is some pseudo-code corresponding to the key-scheduling algorithm:

for i from 0 to 255
S[i] := i
endfor
j := 0
for i from 0 to 255
j := (j + S[i] + key[i mod keylength]) mod 256
Swap values of S[i] and S[j]
endfor

Now that the S array is generated, it is used in the next step of the RC4 algorithm to generate the key stream.

- **3.2.2 Key stream generation algorithm**

This step of the algorithm consists in generating a key stream of the size of the message to encrypt. This algorithm enables us to generate a key stream of any size. To do so, we first initialize the two indexes to 0 and we then start the generation of the key stream one byte at a time until we reached the size of the message to encrypt. For each new byte to compute we do the following actions:

1. Compute new value of i and j
   i := (i + 1) % 256
   j := (j + S[i]) % 256
2. Swap S[i] and S[j] to have a dynamic state (it makes it obviously harder to crack than if the state was computed only once and use for the generation of the whole key stream)
3. Retrieve the next byte of the key stream from the S array at the index
   S[i] +S[j] % 256

Here is some pseudo-code corresponding to the pseudo-random generation algorithm:

i := 0; j := 0
while GeneratingOutput:
i := (i + 1) mod 256
j := (j + S[i]) mod 256
swap values of S[i] and S[j]
K := S[(S[i] + S[j]) mod 256]
output K; endwhile

3.3 Watermarking Schemes

After compressing and encrypting an image the watermarking process is applied on it. There are three different watermarking schemes such as Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM) which are described in following section.[1], [4], [7].

3.3.1 Spread Spectrum (SS)

The watermark signal is generated by using watermark information bits (b), chip rate (r) and PN sequence (P). [1]. The watermark information bits $b_i = \{b_i\}$, where, are spread by (r). The watermark signal W = {wj},

Where

$$Wj = \alpha * aj * Pj. \qquad \text{Where } Pj = \{1,-1\}$$

And Watermarked Signal (C_W) is given by

$$C_w = C + W = C_{wi} \qquad \text{where } i = 0, 1... L-1.$$

The received encrypted-watermarked (C_W) signal is applied to the detector. It is multiplied by PN (P) sequence used for embedding, followed by summation over chip-rate window (r), yielding the correlation sum (S_i)

$$S_i = \sum_r C_{wj} P_j = \sum_r (C_j + W_j) P_j = b_i \sigma_p^2 \alpha r$$

The sign of S_i gives the watermark information bits: Sign (S_i) = Sign (b_i) = b_i

3.3.2 Scalar Costa Scheme Quantization Index Modulation (SCS-QIM)

In this scheme, given watermark strength, we choose a quantizer from an ensemble of quantizer to embed the watermark. [19]. for a binary watermark W {0, 1} the quantizer can be chosen as

$$U = (l + k_{qim_i})\beta\Delta + w\beta\Delta/2 \quad \forall i = 0, 1, \ldots, L-1.$$

The embedding scheme is given by

ISSN 2348 – 7968

$$q_i = Q_\Delta\left(c_i - \Delta\left(\frac{w_i}{2} + k_{qim_i}\right)\right) - \left(c_i - \Delta\left(\frac{w_i}{2} + k_{qim_i}\right)\right) \quad \forall i = 0, 1, \ldots, L-1$$

The watermark sequence is then given by

$$\boldsymbol{W} = \beta \mathbf{q}$$

And the embedding is done as

$$\boldsymbol{C}_W = \boldsymbol{C} + \boldsymbol{W}.$$

Watermark is estimated by quantizing the received signal to the nearest data in the codebook.

$$\hat{w} = Q_\Delta\left(c_{w_i}\right) - c_{w_i} \quad \forall i = 0, 1, \ldots, L-1.$$

3.3.3 Rational Dither Modulation (RDM)

It is based on the quantization of the ratio of the host signal to a function g (.). [20]. The quantizer is given by

$$Q\text{“}\ \Delta = 2\Delta + w\Delta/2$$

w= {-1, 1} is the information that is to be embedded into the host element. The embedding is done by:

$$cwi = g(cwi\text{-}1)\ Q\text{“}\ \Delta\ (ci/\ g(cwi\text{-}1))$$

Hence $wi = (cw_i - c_i)$ gives the additive nature of watermark. The detection of watermark is performed by the minimum distance criteria using the following equation, as given:

$$\hat{w} = \arg\min_{1,-1}\left(\frac{c_{w_i}}{g\left(\boldsymbol{c}_{w_{i-1}}\right)} - Q'_\Delta\left(\frac{c_{w_i}}{g\left(\boldsymbol{c}_{w_{i-1}}\right)}\right)\right)^2 \quad \forall i = 1, \ldots, L-1.$$

4. Conclusion

The proposed method introduces a robust watermarking technique. This watermarking algorithm can be simple to implement as it is directly performed in the compressed-encrypted domain, i.e., it does not require decrypting or partial decompression of the content. The proposed scheme also preserves the privacy of content as the embedding is done on encrypted data. The homomorphic property of the cryptosystem can be broken, which allows us to detect the watermark after decryption and control the image quality as well. The proposed scheme can examine the relation between payload capacity and quality of the image for different resolutions. The performance of the watermarking algorithm can be evaluated by determining the watermarked image quality using the three different watermarking schemes: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).

References

[1] A. V. Subramanyam, Sabu Emmanuel, Member, IEEE, and Mohan S. Kankanhalli, Senior Member, IEEE," Robust Watermarking of Compressed and Encrypted JPEG2000 Images" IEEE Trans. on multimedia, vol. 14, no. 3, june 2012, pp.703 - 716

[2] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli, "Privacy preserving multiparty multilevel DRM architecture," in Proc. 6th IEEE Consumer Communications and Networking Conf., Workshop Digital Rights Management, 2009, pp. 1–5.

[3] T. Thomas, S. Emmanuel, A. Subramanyam, and M. Kankanhalli, "Joint watermarking scheme for multiparty multilevel DRM architecture," IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 758–767, Dec. 2009.

[4] A. Subramanyam, S. Emmanuel, and M. Kankanhalli, "Compressed encrypted domain JPEG2000 image watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, 2010, pp. 1315–1320.

[5] H. Wu and D.Ma, "Efficient and secure encryption schemes for JPEG 2000," in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, 2004, vol. 5, pp. 869–872.

[6] M. Deng, T. Bianchi,A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.

[7] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage- efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[8] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," Opt. Eng., vol. 45, pp. 1–3, 2006.

[9] Deepa L , Meerakrishna G ,Vinitha ,Febeena," Compressed Image Watermarking using Visual Cryptography", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.

[10] F. Battisti, M. Cancellaro, G. Boato, M. Carli, and A. Neri, "Joint watermarking and encryption of color images in the Fibonacci-Haar domain," EURASIP J. Adv. Signal Process., vol. 2009.

[10] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. De Natale, and A. Neri, "A joint digital watermarking and encryption method," in Proc. SPIE Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008, vol. 6819, pp. 68 191C–68 191C.

ISSN 2348 – 7968

[11] J. Prins, Z. Erkin, and R. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," EURASIP J. Inf. Security, vol. 2007.

[12] Z. Li, X. Zhu, Y. Lian, and Q. Sun, "Constructing secure content dependent watermarking scheme using homomorphic encryption," in Proc. IEEE Int. Conf. Multimedia and Expo, 2007, pp. 627–630.

[13] Q. Sun, S. Chang, M. Kurato, and M. Suto, "A quantitive semi-fragile JPEG2000 image authentication system," in Proc. Int. Conf. Image Processing, 2002, vol. 2, pp. 921–924.

[14] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.

[16] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[17] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," Lecture Notes in Computer Science, pp. 223–238, 1999.

[18] M. Rabbani and R. Joshi, "An overview of the JPEG 2000 still image compression standard," Signal Process.: Image Commun., vol. 17, no. 1, pp. 3–48, 2002.

[19] J. Eggers, R. Bauml, R. Tzschoppe, and B. Girod, "Scalar costa scheme for information embedding," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 1003–1019, Apr. 2003.

[20] F. Perez-Gonzalez, C. Mosquera, M. Barni, and A. Abrardo, "Rational dither modulation: A high-rate data-hiding method invariant to gain attacks," IEEE Trans. Signal Process., vol. 53, no. 10, pt. 2, pp. 3960–3975, Oct. 200