International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Performance Analysis of JPEG2000 Images In a Compressed and Encrypted Domain Using Three Different Watermarking Techniques

Pallavi B[1], Sunil M P[2]

[1]Student, Department of Electronics & Communication Engineering, School of Engineering & Technology, Jain university Bangalore, Karnataka, India

[2]Assistant Professor, Department of Electronics & Communication Engineering, School of Engineering & Technology, Jain university Bangalore, Karnataka, India

Abstract: ***Digital Asset Management (DAM) systems generally involve the digital assets like images, graphics, logos, audio/video clips. These digital assets will contain some additional information and these files should be accessible only to the intended users .So these digital assets should be in a compressed and encrypted domain. The owner distributes the media to the consumers by multiple levels of distributors. Since the distributors are not the consumers they cannot have access to the original message. So before the owner distributes the message to the distributors, the message should be compressed and encrypted. Sometimes these compressed encrypted media items can be accessible to unwanted users so watermarking of these media items should be done. It is difficult to watermark such compressed encrypted streams since a small modification in the compressed and encrypted bit stream leads to degradation in the media quality. Thus we need to choose proper encryption algorithm which will allow secure watermarking in compressed-encrypted domain. The encryption algorithm used in this paper is stream cipher RC6.In this paper, we propose a robust watermark embedding technique for JPEG2000 compressed and encrypted images. The watermark embedding is done in the compressed encrypted domain; the extraction of watermark can be done either in decrypted domain or in encrypted domain. We investigate in detail the Peak Signal to Noise Ratio(PSNR) and the security of the proposed algorithm, using three watermarking schemes: Spread Spectrum (SS),Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM).***

Keywords: Watermarking, Compressed-encrypted domain, JPEG2000, DAM.

1. Introduction

Watermarking is the process of embedding data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object. The object may be an audio, image or video. A copy of a digital image is identical to the original. This has in many instances, led to the use of digital content with malicious intent. One way to protect multimedia data against illegal recording and retransmission is to embed a signal, called digital signature or copyright label or watermark that authenticates the owner of the data. Copyright protection becomes an important issue. As a potential and effective way to solve this problem, digital watermarking becomes a very active research area of signal and information processing, as watermarking is identified as a major technology to achieve copyright protection. Because of its growing popularity, the Discrete Wavelet Transform (DWT) is commonly used in recent watermarking schemes. In a DWT based scheme, the DWT coefficients are modified with the data that represents the watermark. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. Invisibility refers to the degree of distortion introduced by the watermark and its affect on the viewers or listeners. Robustness is the resistance of an embedded watermark against intentional attacks, and normal audio video processes such as noise, filtering (blurring, sharpening, etc.), re-sampling, scaling, rotation, cropping, and lossy compression. Capacity is the amount of data that can be represented by an embedded watermark. The need for copyright protection, ownership verification, and other issues for digital data are getting more and more interest nowadays. Among the solutions for these issues, digital watermarking techniques are used. A range of watermarking methods has been projected. Compression plays a foremost role in the design of watermarking algorithms. For a digital watermarking method to be effective, it is vital that an embedded watermark should be robust against compression. JPEG2000 is a new standard for image compression and transmission. JPEG2000 offers both lossy and lossless compression. The projected approach is used to execute a robust watermarking algorithm to watermark JPEG2000 compressed and encrypted images. For encryption it uses RC6 block cipher. The method embeds watermark in the compressed- encrypted domain and extraction is done in the decrypted domain. The proposal also preserves the confidentiality of substance as the embedding is done on encrypted data. On the whole 3 watermarking schemes are used: Spread Spectrum, Scalar Costa Scheme Quantization Index Modulation, and Rational Dither Modulation.

2. Literature Survey

Various DAM architectures have been proposed for digital content and license distribution for a typical two party scenario, where the owner and consumers are the only parties involved in the architecture. However the owner will

distribute the media content in a compressed-encrypted domain to consumers through various multilevel distributor channel. In such systems involves multiple levels of owners, distributors and consumers. Since the distributors are not the consumers they do not have access to plain content i.e original message. As they are distributors of media content distributes the encrypted content and requests the license server in the DAM system to distribute the associated licence which contains the decryption key in order to make the encrypted data available to the consumers. Sometimes it is necessary for the distributors to watermark the original media content for authentication purposes and for copy right violation detection.[1]-[4].Thus watermarking should be carried out in the compressed and encrypted domain. In this paper we are performing watermarking of JPEG2000 images which are compressed and encrypted, where the compression is a process which reduces the number of bits required to represent the image and encryption is a procedure which converts the plaintext into cipher text. Encryption is done on JPEG2000 compressed stream except headers and marker segments, which are left in plaintext for format compliance [5]. There is many such image watermarking techniques proposed till today. [6]–[11]. In [6],Deng et al. proposed 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 form using the plaintext features of the host signal and in [6], this is possible as the seller embeds the watermark. The ciphertext 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 are 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 distributors 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 unencrypt the ciphered text and get the plaintext values. Thus, watermarking in compressed-encrypted domain using the technique proposed in [11] is very difficult. In [12] Li et al. proposed a content-dependent watermarking technique, which embeds the watermark in an encrypted format, but the host signal is still in the plain text format. This algorithm cannot be applied when the content is in the encrypted domain because in such a case the distortion or noise introduced in the host signal may be large. In [13] Sun et al. proposed a semi fragile authentication system for JPEG2000 images. However, this scheme is not fully compressed and encrypted domain watermarking compatible as it derives the content based features for watermarking from the plain text. We propose a robust watermarking technique for JPEG2000 images in which the watermarking bits can be in a proper manner in a compressed and encrypted byte stream by using the homomorphic property, explained in Section 3 of the cipher scheme. The advantage of watermarking in a compressed and encrypted domain will save the computational complexity and also preserves the confidentiality of the media content. Although, some asymmetric schemes like RSA [14], Gold-wasser-Micali [15], Elgamel [16] and Paillier [17], with homomorphic property, can be used for encryption purpose, there are two main drawbacks using such schemes. Firstly, if the encryption is performed on a message size of few bits, the size of the ciphertext may expand which leads to loss of compression efficiency which inturn affect the image quality. For RSA and Goldwasser-Micali, expansion is caused due to the use of modulo $n_{p\,q}$ (a product of two large primes' p and q). For Paillier and Elgamel the expansion of ciphertext to plaintext is 2 [17], [16]. Secondly, if the encryption is per-formed on a large message size, say, few hundreds of bits, to compensate the loss in compression, the payload capacity de creases, where payload capacity is the number of watermark signal bits embedded per encrypted message. A secure sym-metric stream cipher with homomorphic property is preferred over secure asymmetric encryption with homomorphic prop-erty mainly due to the following two reasons. Symmetric ci-phers with homomorphism can be applied on a smaller mes-sage size (byte), without increasing the compressed data size and achieving a better payload capacity than asymmetric counterparts. So there is a tradeoff between security-compres-sion efficiency-payload capacities, which poses a challenge for deciding which cipher scheme to apply. Therefore we use the RC6 stream cipher with homomorphism property. This paper is organized as follows. Section III describes the proposed scheme. In Section IV, we discuss the key distribution, domain of encryption, security analysis of encryption and watermarking algorithm, and effect of scaling on RDM detection. The experimental results are discussed in Section V. Section VI concludes the paper.

3. Block Diagram

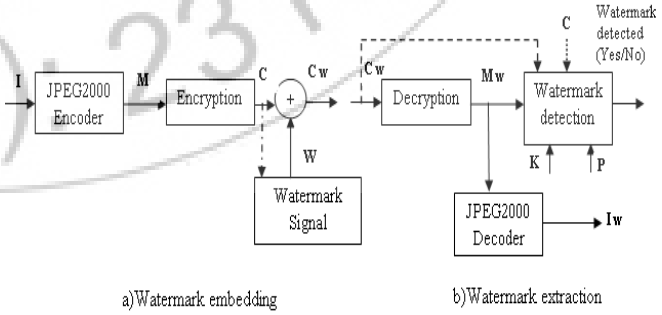


Figure 3.1: Basic block diagram

The proposed algorithm works on JPEG2000 compressed code stream. JPEG2000 compression process is divided into five different stages [18]. In the first stage the input image is

preprocessed by dividing it into non-overlapping rectangular tiles. The input image is a grayscale image.The image formats are uncompressed hence they are large. So compression should be performed to reduce the storage and the transmission bandwidth.The unsigned samples are then reduced by a constant to make it symmetric around zero and finally a multi-component transform is performed. In the second stage, the discrete wavelet transform (DWT) is applied.The purpose served by the Wavelet Transform is that it produces a large number of values having zeroed, or near zero, magnitudes. In the third stage quantization is performed.After the wavelet transforms, the coefficients are scalar-quantized to reduce the number of bits to represent them, at the expense of quality. The output is a set of integer numbers which have to be encoded bit-by-bit. The parameter that can be changed to set the final quality is the quantization step: the greater the step, the greater is the compression and the loss of quality. With a quantization step that equals 1, no quantization is performed.Multiple levels of DWT gives a multi-resolution image. The lowest resolution contains the low-pass image while the higher resolution contains the high-pass image. These resolutions are further divided into smaller blocks known as code-blocks where each code-block is encoded independently. Further, the quantized-DWT coefficients are divided into different bit planes and coded through multiple passes at embedded block coding with optimized truncation (EBCOT) to give compressed byte stream in the fourth stage. The 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. The pro-posed algorithm uses a symmetric stream cipher with additive homomorphic properties for encryption. In fact the distributors get JPEG2000 compressed stream cipher encrypted images for distribution. The distributors can then apply any robust additive watermarking technique to this compressed encrypted stream.

In this paper, we use three watermarking schemes, namely, Spread Spectrum (SS), Scalar Costa Scheme (SCS-QIM), and Rational Dither Modulation (RDM) for the purpose and study the bit error rate of detection and the quality versus payload capacity trade-off. Fig.3.1 shows the watermark embedding and detection pipelines. The watermark signal for SS is generated without using the host signal, whereas for SCS-QIM and RDM it is generated using C as shown with dashed-dotted line in the embedding block. The watermark detection can be done before and after the decryption but in the compressed domain as shown in Fig.3.1. For detection in encrypted domain, C w, instead of M w, is directly fed to the detection module, which is shown in dashed line in Fig.3.1. In the watermark extraction block C is given in dotted line to emphasize that it is not required for blind detection.

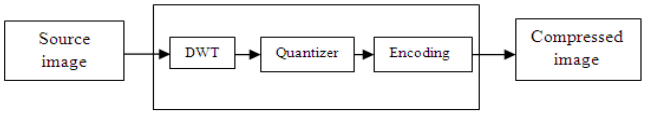


Figure 3.2: JPEG encoder

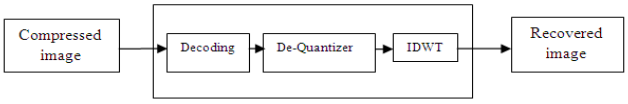


Figure 3.3: JPEG decoder

Notations:
- L= Length in bytes.
- M=Compressed byte stream
- Mw=Watermarked copy of M.
- C=Encrypted copy of M.
- Cw=Watermarked copy of C.
- b=Watermark information.
- E(.) and D(.)=Encryption and decryption function.
- K=Encryption key.
- r=chip rate in SS.
- α=Watermark strength factor in SS.
- P=PN sequence with zero mean and variance .
- Kqim=Random sequence.
- β=Scale parameter in SCS-QIM.
- Δ=Step size.
- q=Denotes the quantization error sequence.
- Lm=Number of the past watermarked samples in RDM
- γ=Shape parameter in RDM
- I,Iw =original and watermarked decompressed image.

4. Algorithm Implementation

A. Encryption Algorithm

JPEG2000 gives out M, a packetized byte stream as output. In order to encrypt the message M, we use RC6 encryption scheme. RC6 algorithm supports a block size of 64 bits and a key size of 256 bits. The encryption and decryption of RC6 makes cipher text and plain text after carrying out twenty rounds continually with cipher text and plain text in the four storages (A, B, C, and D) per 32bit word. After doing four words round function, it operates left / right rotate per word with parallel operation as shown in the pseudo code.

Input: Plain text stored in four w-bit input registers A, B, C, D
Number of r rounds,w-bit round keys S[0,…,2r + 3]
Output: Cipher text stored in A, B, C, D
Procedure: B = B + S [0];
D = D + S [1];
For (i=1; i<r; i++)
{ t = (B × (2B + 1)) ⋘log w;
u = (D× (2D + 1)) ⋘ log w; A = ((A ⊕ t) ⋘ u) + S [2i];
C = ((C ⊕ u) ⋘ t) + S [2i+1];(A, B, C, D) = (B, C, D, A);
} A = A + S [2r+2]; C = C + S [2r+3];

B. Decryption Algorithm

In decryption operation, the round key of encryption is used with the inverse order. Thus, RC6 has a Feistel structure; however the operation between encryption and decryption is diverse. RC6 does not have a non-linear transformation s-box.

Input: Cipher text stored in four w-bit input registers A, B, C, D
Number of r rounds, w-bit round keys S[0,…,2r + 3]
Output: Plain text stored in A, B, C, D

Procedure: C = C + S[2r+3]; A = A + S[2r+2];
for(i=r; i>=1; i--)
{ (A, B, C, D) = (D, A, B, C);
u = (D × (2D + 1)) ⋘ log w; t = (B × (2B + 1)) ⋘ log w;
C = ((C – S [2i+1]) ⋙ t) ⊕u; A = ((A – S [2i]) ⋙ u) ⊕ t;
} D = D - S[1]; B = B - S[0];

C. Embedding Algorithm

1. SS

Hartung et al. in [20] proposed a spread spectrum watermarking scheme. The embedding process is carried out by first generating the watermark signal W, by using watermark information bits, chip rate and PN sequence P. For watermarking, an aj sequence of watermarking bits has to be embedded into the image, aj = {-1, 1}. The signal is spread by a factor called chip rate, to obtain the spread sequence, bi= aj where bi = {1,-1}. The spread sequence is amplified with a locally adjustable amplitude factor and then modulated by a pseudo-noise sequence, Pi.The modulated signal (SS watermark signal)

$$Wi = \alpha * aj * Pi. \quad (1)$$

The watermark signal generated is added to the encrypted signal.

2. SCS-QIM

In [21], Eggers et al. projected SCS scheme for watermark embedding. In this method, given watermark strength, we choose a quantizer from an group of quantizers to embed the watermark. The quantizer is chosen by:

$$U = (1+ kqimi) \beta\Delta + w \beta\Delta/2 \quad (2)$$

where w= {0,1} and 1 is different sets of quantizers.For making the codebook secure a random sequence kqimi can be chosen. The embedding is done by:

$$qi = Q\Delta(ci–\Delta(wi/2+kqimi))–(ci-\Delta(wi/2+kqimi)) \quad (3)$$

where QΔ (.) denotes scalar uniform quantization with step size Δ. The watermark sequence is given by

$$W=\beta q. \quad (4)$$

The watermark signal generated is added to the encrypted signal.

3. RDM

It is based on the quantization of the ratio of the host signal to a function g (.). This scheme was proposed by Gonzalez et al [22]. The quantizer is given by

$$Q^{\alpha}\ \Delta = 2\Delta + w\Delta/2 \quad (5)$$

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

$$cwi = g(cwi-1)\ Q^{\alpha}\ \Delta\ (ci/\ g(cwi-1)) \quad (6)$$

where cwi and cwi-1 are the current and previous watermarked samples. cwi is an amplitude enhanced version of scaled-quantized . Thus we can write

$$wi = cwi - ci \quad (7)$$

gives the additive nature of watermark.

D. Watermark Detection Algorithm

Encrypted Domain Detection

1. SS

The received signal is applied to a detector and then multiplied by the PN sequence, P used for embedding and summing it with chip rate, r.

$$Si = bi * r* \alpha*\sigma p^2 \quad (8)$$

$$Sign\ (Si) = bi \quad (9)$$

Resulting in extraction of watermark information bits.

2. SCS-QIM

The watermark is estimated by quantizing the received signal to the in close proximity data in the code book.

$$\dot{w} = Q\Delta\ (cwi) – cwi \quad (10)$$

3. RDM

The watermark is detected by performing minimum distance criterion by means of

$$\dot{w} = argmin\ (1,-1)\ [cwi/g(cwi-1) - Q^{\alpha}\ \Delta\ (cwi\ /\ g(cwi-1))]^2 \quad (11)$$

$Q^{\alpha}\ \Delta$ give the 2 quantizers belonging to bits 1 and -1.The distance is computed consequent to both the quantizers and the one which gives minimum distance gives the watermark bit.

Decrypted Domain Detection:

$$Mw=D\ (Cw,K)=(c_{wi} – k_i) mod\ 255= m_{wi} \quad (12)$$

1. SS

For SS detection, the embedded watermark information W can be estimated from Mw using correlation detector even without the knowledge of the corresponding originals M or C. Therefore to obtain better detection results, we can encryptMw with K which gives Cw and removing C gives

$$Si = bi * r* \alpha*\sigma p^2 \quad (13)$$

Thus, the sign of Si gives the watermark information bit

$$Sign\ (Si) = bi \quad (14)$$

2. SCS-QIM and RDM

For SCS-QIM the decrypted message Mw along with cipher key K is fed to the watermark extraction module. The signal Mw is encrypted with the key K.Thus, we get the ciphered-watermarked signal Cw and the watermark is detected using (10) and (11).

5. Results and Discussion

Experiments have been carried out for a grayscale image of size 512X512.Table 5.1 shows the PSNR of the watermarked and watermark detected images using three watermarking schemes SS, SCS-QIM, RDM are calculated and the performance of the three techniques are analysed.Thus from the results we can conclude that the RDM scheme of watermarking provides better image quality with higher value of PSNR.PSNR can be calculated using the following equation

PSNR = 10*log10(255^2/MSE)

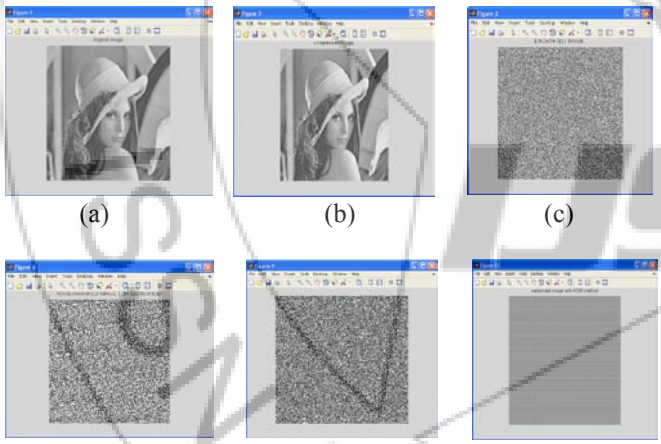
Where Mean Square Error (MSE) is given by

MSE = (1/m*n)*sum(sum(I(i,j)- I_w(i,j))^2),Where I is the original image and Iw is the watermarked image.

Table 5.1: PSNR (db) of watermarked and watermark detected image

Scheme	*Watermarked image PSNR(db)*	*Watermark detected image PSNR(db)*
SS	11.10	10.62
SCS-QIM	10.83	10.36
RDM	12.19	12.76

Watermark Embedding

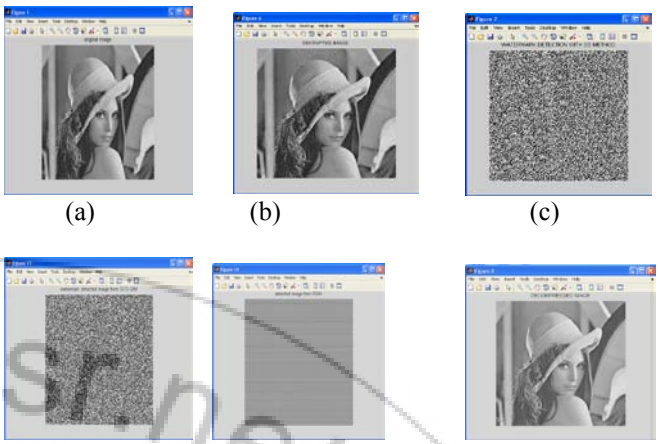


(a) (b) (c)

(d) (e) (f)

Fig.5.1. a) Original image b) Compressed image (101db) c) En -crypted image (10.98db) d)SS in encrypted domain (11.10db) e)SCS-QIM in encrypted domain (10.83db) f)RDM in encrypted domain(12.19db)

Watermark Extraction



(a) (b) (c)

(d) (e) (f)

Figure 5.2: a) Original image b) Decompressed image (275db) c) Decrypted image (48.13db) d) SS in decrypted domain (10.62db) e)SCS-QIM in decrypted domain (10.36db) f)RDM in decrypted domain(12.76db)

6. Conclusion and Future scope

In this paper we propose an algorithm to embed a robust watermark in the JPEG2000 compressed encrypted images using three different existing watermarking schemes i.e. SS, SCS-QIM, RDM. The algorithm is simple to implement as it is directly performed in the compressed-encrypted domain, it does not involve decryption or decompression. Our proposal also preserves the confidentiality of content as the embedding is done on encrypted data. The encryption algorithm used is RC6 which uses homomorphic property which allows us to detect the watermark after decryption and manage the image quality.The detection is carried out in compressed or decompressed domain. in case of decompressed domain, the non-blind detection is used. We Analyze the performance of all the three watermarking techniques in terms of Peak Signal to Noise Ratio(PSNR in db).Experimental results shows that using RDM watermarking technique higher PSNR value of 12.19 db(embedding) and 12.76db(detection) can be obtained which in turn provides better image quality compared to other two watermarking techniques. Future work aims at extending the proposed scheme to video watermarking with modification in the proposed algorithm.

References

[1] S.Hwang, K.Yoon, K.Jun,and K.Lee, "Modeling and implementation of digital rights," J. Syst. Softw., vol. 73, no. 3, pp. 533–549, 2004.

[2] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli, "Privacy preservingmultiparty multilevel DRMarchitecture," in Proc. 6th IEEEConsumer 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.WuandD.Ma,"Efficient and secure encryption schemes for JPEG2000," 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] 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.
[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," inProc. 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] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in Proc. 2nd Annu.Int. Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005), 2005, pp.
[20] F. Hartung and B. Girod, "Watermarking of uncompressed and compressed video," Signal Process. vol. 66, no. 3, pp. 283–301, 1998.
[21] 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.
[22] 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. 2005.

Author Profile

Ms. Pallavi B is a student in the Department of Electronics and Communication Engineering, School of Engineering, Jain University, Bangalore. She obtained her Bachelor degree in Electronics and Communication Engineering from SBMJCE, Bangalore in 2012, Visvesvaraya Technological University, Belgaum and she is pursuing M.Tech (SP and VLSI) in Electronics and Communication Engineering, Jain University Bangalore. My research interest includes VLSI and DSP.

Mr. Sunil M P, currently working as an assistant professor in the Department of Electronics & Communication Engineering, School of Engineering and technology, Jain University, Karnataka, India. He has received Bachelor degree in Electronics and Communication from VTU in 2009. He has received M.Tech degree in Electronics design and Technology from National Institute of Technology, Calicut, Kerala in 2011. His research interests include embedded systems design, Analog and mixed signal VLSI design, Ultra-thin gate insulators for VLSI Technologies, RF VLSI design, Microelectronics system packaging, Microelectronics, Micro/Nano sensor technology, High-speed CMOS analog/RF-wave integrated circuits and Systems.