Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.856 – 862

RESEARCH ARTICLE

Encryption of JPEG2000 Images using Watermarking

Renuga Devi.J[1], Priyadharshini.K[2], Umamaheswari.V[3]
[1]P.G Scholar, [2]P.G Scholar, [3]P.G Scholar
[1,2,3]Department of Computer Science and Engineering
[1,2,3]P.S.R.Rengasamy College of Engineering for Women, Sivakasi
[1] rdsweety1@gmail.com, [2] priyavijayagopalan@gmail.com, [3] umavarshni@gmail.com

Abstract— ***The proposed system aims to secured jpeg2000 images using digital image watermarking technique. The watermarking scheme is robust against noise, scaling and filtering attack. The jpeg2000 image encryption and decryption using RC4 stream cipher. In watermark, embedding and extraction has been done using robust watermarking technique. The watermarking techniques are Spread Spectrum, Scalar Costa Scheme and Rational Dither Modulation. The proposed work is analyzed by Peak Signal to Noise Ratio (PSNR), which is calculated using Mean Square Error (MSE).***

Keywords— ***Watermark Embedding, Watermark Extraction, Compressed and Encrypted, JPEG 2000***

I. INTRODUCTION

In practice, it is required that a signal is accurately hidden into image data in such a way to result very difficult to be perceived but also very difficult to be removed. Another important characteristic is blindness i.e., the watermark decoder must not require the original non watermarked image for extracting the embedded code. A research field whose results could undoubtedly help in the design of a watermarking algorithm is image compression. The goal of image compression can be described as one of removing from images all the data which are perceptually irrelevant. Similarly the problem of image watermarking is one of adding, to images, data which are perceptually unimportant a widely used technique exhibiting a strong similarity to the way the HVS processes images is the Discrete Wavelet Transform (DWT). As a matter of fact, the next-generation image coding standard JPEG2000 will strongly rely on DWT for obtaining good quality images at low coding rates. When the content is accessible only in encrypted form to the watermark embedder, the embedding scheme proposed in [6] might not be applicable as the host and watermark signal are represented in composite signal form using the plain text features of the host signal and in [6], this is possible as the seller embeds the watermark. Also, there is a cipher text expansion of 3.7 times that of plaintext. In [8] and [9], some sub-bands of lower resolutions are chosen for encryption while watermarking the rest of higher resolution sub-bands. While in [10], the encryption is performed on most significant bit planes while watermarking the rest of lower significant bit planes. In case lesser number of sub-bands/bit planes is used for encryption, an attacker can manipulate the un-encrypted sub-bands/bit planes and further extract some useful information from the image, although the image may not be of good quality. On the other hand, if more sub-bands/bit planes are encrypted and only rest few sub-bands/bit planes are watermarked, it might be possible for an attacker to remove the watermarked sub-bands/bit planes while maintaining the image quality. Robust quantization index modulation (QIM) based watermarking technique, which embeds the watermark in the encrypted domain. In the technique proposed in [11], the addition or subtraction of a watermark bit to a sample is based on the value of quantized plaintext sample. However, in our algorithm, the watermark embedder does not have access to the plain text values. They have only compressed-encrypted content. Also the watermark embedders do not have the key to UN-encrypt and get the plain text compressed values. Thus, watermarking in compressed-encrypted domain using the technique proposed in [11] is very challenging.

II. RELATED WORK

A.Subramanyam,S. Emmanuel, and M. Kankanhalli (2010) proposed the compressed encrypted domain jpeg2000 image watermarking [1]. In digital rights management (DRM) systems, digital media data is distributed by multiple levels of distributors in a compressed and encrypted format. In this paper, has proposed a robust watermark embedding technique for JPEG2000 compressed and encrypted images. The proposed technique embeds watermark in the compressed encrypted domain, and the extraction of watermark can be done either in decrypted domain or in encrypted domain. The encryption and decryption site using RC4 cipher. In watermark, embedding and watermark detection using spread spectrum watermarking technique. The algorithm is simple to implement as it is directly performed on the compressed-encrypted domain. This scheme also preserves the confidentiality of content in embedding as well as extraction. In their work, analyzed the relation between payload capacity and quality of the image for different resolutions.

H. Wu and D.Ma (2000) proposed efficient and secure schemes for jpeg2000 in their work successfully developed efficient and secure encryption schemes for JPEG 2000 [1]. The secure encryption algorithm RC4 stream cipher and AES block cipher can be used in this scheme. These schemes are efficient and introduce only extremely small amount of extra computation. The schemes are highly secure and it is proved that they perfectly protect 99.15% of the information of an image. The algorithm uses a stream cipher to generate a key stream for encryption and decryption. The “modulo 0xFF” can be effectively implemented, so the encryption and decryption algorithms introduce only a few extra operations for each byte and will not incur delay in real-time delivery. In a block cipher the encryption algorithm may not be a full block. In that case, cipher text stealing technique to preserve the length of the message. If cipher text stealing is used in the encryption process, the decryption of the last two blocks should be adjusted accordingly. The RC4 and AES are used in the experiments. Both schemes provide the same security protection. The schemes are very computationally efficient. The schemes are also very secure since they protect 99.15% of the information of an image.

M. Deng, T. Bianchi,A. Piva, and B. Preneel (2009) proposed buyer seller watermarking protocols integrate watermarking techniques with cryptography, for copyright protection [3]. An efficient buyer seller watermarking protocol based on homomorphism public-key cryptosystem and composite signal representation in the encrypted domain. A composite signal representation allows us to reduce both the computational overhead and the large communication bandwidth which are due to the use of homomorphism public-key encryption schemes. Composite representation of signals permits to group several signal samples into a single word and to perform basic linear operations on them. This representation to solve the problems related to the data expansion from the plaintext to the encrypted representation of signals.

Shiguo Lian, Zhongxuan Liu, Ren Zhen, and Haila Wang (2006) proposed a commutative watermarking and encryption scheme is used for media data protection [4]. In this scheme, the partial encryption algorithm is adopted to encrypt the significant part of media data, and other part is watermarked. The commutative property brings practical applications in secure media transmission or distribution. Digital watermarking embeds identification information into media data imperceptibly, which protects media data's ownership. Media data's are first watermarked, and then encrypted. However, in this scheme, the encrypted media data should be decrypted before the watermark can be extracted or another watermark can be embedded. Media data's are encrypted with the Advanced Encryption Standard and Quantization Index Modulation method is used as the watermark algorithm. This method can be combined with JPEG2000. Based on the scheme, analyze the trade-off between security and robustness was analyzed. The encryption or watermarking algorithm can be combined with JPEG2000 code, which is time-efficient compared with the compression process.

T. Bianchi, A. Piva, and M. Barni (2010) proposed the signal processing tools working directly on encrypted data could provide an efficient solution to application scenarios where sensitive signals must be protected from an untrusted processing device [5]. The data expansion required to pass from the plaintext to the encrypted representation of signals, due to the use of cryptosystems. The proposed representation permits to speed up linear operations on encrypted signals via parallel processing and to reduce the size of the encrypted signal. The advantage brought by the composite representation is therefore twofold: Firstly, it permits to speed up computation via parallel processing; Secondly, it reduces the size of the encrypted signals. Composite representation can be a viable solution to the problems of both data expansion and increased complexity arising from the processing of encrypted data, it can be more convenient to use simpler processing algorithm like filtering through convolution.

Z. Li, X. Zhu, Y. Lian, and Q. Sun (2007) proposed as a solution to overcome the potential estimation attack aiming to recover and remove the watermark from the host signal [6]. It has also been used for the application of content authentication. The watermarking embedding and detection using spread spectrum technique. In this paper, a novel approach to construct secure CDWM with the aid of homomorphic encryption and dirty paper precoding. The intuitive idea is to introduce a decryption module before watermark detection such that only those who know how to decrypt is able to detect the watermark. improving watermarking security by using homomorphic cryptography to facilitate a distributed watermark detection and centralized decryption. By integrating watermarking with cryptography would improve the security of the cryptographic schemes.

III. PROPOSED SCHEME

Project Goal	**Description**
Functional Goals:	
Confirmation of sender	Sender confirmation using Watermarking.
Maintaining Confidentiality	Check if third party is decrypting the data.
Technological Goals:	
Use of effective Watermarking Technique	Reduce the Bit Error Rate, Noise and Scaling attack.

Quality Goals:	
Non-repudiation	No one other than sender can claim about the sent data.
Security	The data should be
Constraints:	
Encryption Algorithm	RC4 is having some limitations

A. Problem definition

To implement watermarking using Spread Spectrum (SS), Scalar Costa Scheme (SCS) and Rational Dither Modulation (RDM) on compressed and encrypted data.

B. Scope

To give a watermarking scheme is robust against noise attack and scaling attack. To secure data in compressed format and to minimize Bit Error Rate of watermarked signal. It provides necessary mechanism for traitor tracing, copyright management and distributor protection against false implication.

C. *Goal*

Goal of proposed system is to secure the digital data by using watermarking technique along with embedding capacity, robustness and perceptual quality.

D. *Objective*

1. To give a watermarking scheme is robust against noise attack and scaling attack.
2. To secure data in compressed format.
3. To minimize Bit Error Rate of watermarked signal.
4. To provide necessary mechanism for traitor tracing, copyright management and distributor protection against false implication.

IV. RESEARCH METHODOLOGY

A. Encryption and Decryption Algorithm:

JPEG2000 gives out packetized byte stream M as its output. In order to encrypt the message M, K is chosen, a randomly generated key-stream using RC. Then the encryption is done byte by byte to get the ciphered signal C:

$$C = E\ (M, K) = Ci$$

$$C = (mi + ki\ ) \bmod 255$$

Where, the addition operation is arithmetic addition. Here, mod 255 is required to preserve the format compliancy of JPEG2000 bit stream. In JPEG2000 bit stream, the header syntax occurs as a value greater than 0xff89. This value corresponds to two consecutive bytes having values 255 and higher than 137 in decimal bases. If mod 256 is used, it may generate a value 255 and the consecutive byte value greater than 137, which corresponds to syntax and is undesirable. So to prevent the generation of header segments, the value mod 255 is used.

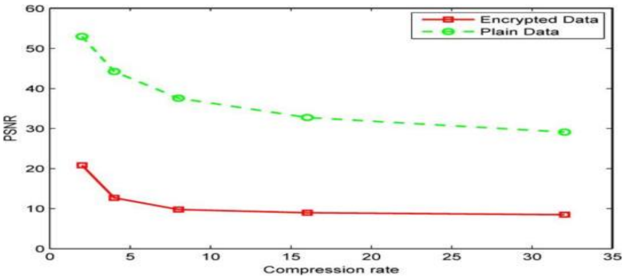

Fig 1 PSNR vs. Compression Rate

Let
C1= E (M1, K1) and
C2 = E (M2, K2).
For K= K1+K2,
Additive homomorphism property gives
D (C1+C2, K) = M1+M2

Here, M1 has been preprocessed by the owner. The owner does the preprocessing by limiting the values as M1 | M1 ε [α, 255 – (α + 1)], where α is a positive integer. However, the preprocessing is not applied when M1 = 255 and M1i+1 > 137, because this case indicates the presence of a header segment which should be preserved to preserve the bit stream compliance. Thus the stream cipher has additive privacy homomorphism property. The privacy homomorphism property will make it possible to detect the watermark from the decrypted content and also help us to control the watermarked image quality easily.

The security of the cryptosystem lies on the underlying stream cipher used. RC4 is a stream cipher and its security has been investigated in depth. The compressed encrypted byte stream C is given to distributors to distribute. They do not have access to the original image. Often distributors need to watermark C to prove their distributorship to the recipient or copyright violation detection purposes.

B. Watermark Embedding and Extraction

1) Spread Spectrum: The watermark signal for SS is generated without using host data. In the context, security is known because the issue of estimating the secret parameters of the embedding function supports the observation of watermarked signals. On the theoretical aspect, the security is quantified from an information-theoretic purpose of point by means of the equivocation about the key parameters. The main results reveal basic limits and bounds on security and provide insight into different properties like the impact of the embedding parameters, and the tradeoff between strength and security. On the practical side, executable estimators of the key parameters are projected and on paper analyzed for a range of situations, providing a comparison with previous approaches, and showing that the protection of the many schemes employed in practice are often fairly low. The protection of spread-spectrum-based data-hiding strategies has been investigated from theoretical and practical points of view.

2) SCS: Research on data hiding techniques has received substantial attention because of its potential application in multimedia system security. Digital watermarking is an information hiding technique wherever the embedded information is powerful against malicious or accidental attacks, may provide new potentialities to enforce the copyrights of multimedia system data. The initial knowledge isn't available to the decoder. For Gaussian data, in 1983, Costa projected a scheme that in theory achieves the capability of this communication situation. [12] But, Costa's scheme isn't practical. Thus, many analysis teams have projected suboptimal practical communication schemes based on Costa's plan. The goal of scheme is to present an entire performance analysis of the scalar Costa scheme (SCS) that may be a suboptimal technique using scalar embedding. Information theoretic bounds and simulation results with progressive committal to writing techniques are measured. Further, amplitude scaling attacks and the invertibility of

SCS embedding square measure investigated. Information embedding into IID original data and an attack by AWGN has been analyzed. The decoder has no access to the original data. This situation may be considered to be communication with side information at the encoder that a theoretical communication scheme has been derived by Costa in 1983.

3) Rational Dither Modulation: It is a quantization-based data-hiding technique that is basically liable to amplitude scaling and modifies it in such a way that the result becomes invariant to realize attacks. [11] This technique retains most of the simplicity of the traditional dither modulation (DM) scheme. RDM is predicated on employing a gain-invariant adaptive approximation step-size at each encoder and decoder. This causes the watermarked signal to be asymptotically stationary. Mathematical tools are used to verify the stationary probability density function that is later used to assess the performance of RDM in Gaussian channels. RDM is compared with improved spread-spectrum methods, showing that the previous can do a lot of higher rates for an equivalent bit error probability. RDM could be a novel data-hiding technique that's invariant to fixed gain attacks and doesn't need estimating the step-size, as most existing methods do. RDM constructs a gain-invariant domain in which quantization takes place, and it will so in a very simple manner, amounting to minor modifications of the quality DM technique.

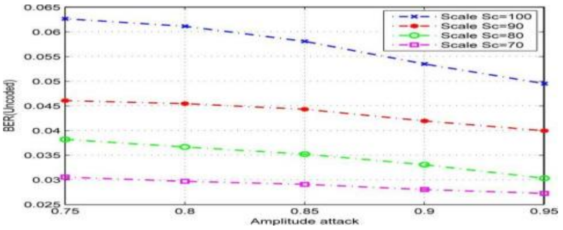

Fig 2 BER vs. Amplitude Scaling Proposed scheme

V. CONCLUSION

The proposed a novel technique to embed a robust watermark in the JPEG2000 compressed encrypted images using three different existing watermarking schemes. The algorithm is 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. Our scheme also preserves the confidentiality of content as the embedding is done on encrypted data. The homomorphic property of the cryptosystem, it allows us to detect the watermark after decryption and control the image quality as well. The watermark detection is carried out in compressed or decompressed domain.

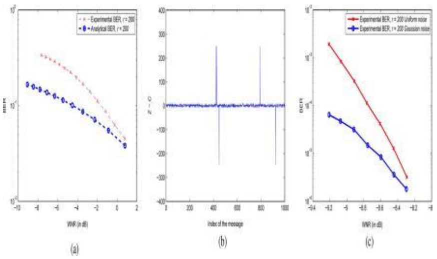

Fig 3 (A) BER Vs. Experimental. (B) Values of Z-C versus Index of the Message. (C) BER after Removal of the Peaks.

In case of decompressed domain, the non-blind detection is used. We analyze the relation between payload capacity and quality of the image (in terms of PSNR and SSIM) for different resolutions. Experimental results show that the higher resolutions carry higher payload capacity without affecting the quality much, where the middle resolutions carry lesser capacity and the degradation in quality is more than caused by watermarking higher resolutions. However, higher resolutions might be truncated to meet the bandwidth requirements and in that case middle resolutions provide a good space for embedding.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

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

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

[10] 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.

[11] 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.

[12] 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.