A SURVEY ON SECURED WATERMARKING TECHNIQUES FOR JPEG IMAGES ON COMPRESSED-ENCRYPTED DOMAIN

Aparna Soni[1], **Deepty Dubey**[2]

Abstract— **In the digital world, the digital media is currently evolving at such a rapid pace, intellectual copyright protection is becoming increasingly important. Now a day, the digital media is available with various image formats, due to which they are simple to copy and resell without any loss of quality. A wide range of digital media is often distributed by multiple levels of distributers in a compressed and encrypted format. It is sometimes necessary to watermark the compressed encrypted media items in the compressed-encrypted domain itself for tamper detection or ownership declaration or copyright management purposes. The compression pack the information of raw media into a lower number of bits and an encryption process randomize the compressed bit stream. The encryption algorithm used was a stream cipher. While the technique embeds watermark in the compressed-encrypted domain, the extraction of watermark can be done in the encrypted and decrypted domain.**

Index Terms— **Compressed and encrypted domain watermarking, Decryption, Encryption, Watermark Embedding, Watermark Extraction etc.**

I. Introduction

Digital representation and distribution of data has increased the potential for misuse and theft and thus gives rise to the problems associated with copyright protection and the enforcement of these rights. The main technical approaches to address the challenge of intellectual copyright protection are digital watermarking techniques. In [1] and [2] it has been described that, the ease with which digital contents can be obtained, replicated, and distributed without any loss of quality has resulted in widespread illegal replication and distribution of digital content. Digital content by nature is very vulnerable to unauthorized distribution and use. For example, downloaded content at the user's side is easy to copy, so it is susceptible to illegal copying and has brought about a copy protection problem. Digital rights management (DRM) technologies were developed, to prevent users from unauthorized copying of digital content, to control the use of digital content, and to enable the development of digital distribution platforms on which innovative business models can be implemented. Hence, to prevent this and protect intellectual property rights, digital rights management (DRM) technologies have been developed. DRM uses cryptographic and digital watermarking techniques to prevent consumers from unauthorized copying of digital content, to control the use of digital content, and to enable the development of digital distribution platforms on which innovative business models can be implemented. Watermarking is a technique for embedding hidden data that attaches copyright protection information to digital information. This provides an indication of ownership of the digital data.

DRM systems with content owners has been introduced, multiple levels of distributors and consumers, the distributors do not have access to plain content (un-encrypted content). As they are distributors of content who distributes the encrypted content (in fact compressed encrypted content as most of the content would be compressed and then encrypted) and requests the license server in the DRM system to distribute the associated license containing the decryption keys to open the encrypted content to the consumers. In fact distributors do not need to have plain content as they are not consumers. However, each distributor sometime needs to watermark the content for media [3] and [4].

A. V. Subramanyam, et al. in [3] and [4], introduced the robust watermarking algorithm to watermark JPEG2000 compressed and encrypted images. The encryption algorithm used is a stream cipher. While the technique embeds watermark in the compressed-encrypted domain, the extraction of watermark can be done in the decrypted domain. It has been investigated in detail about the embedding capacity, robustness, perceptual quality and security of the proposed algorithm, using these watermarking schemes: Spread Spectrum (SS), Scalar Costa Scheme Quantization Index Modulation (SCS-QIM), and Rational Dither Modulation (RDM). Many scholars have published a ton of research work on JPEG compression techniques. In [5], Ricardo L. de Queiroz, presented the techniques that allow the processing of JPEG-compressed data. In [6], A. Alice Blessie1, et al. presents image compression scheme using 9/7 wavelet transform. In [7], Vijaya K. Ahire, et al. evaluated the robustness of image watermarking algorithm in transform domain using combined DWT-DCT. In [8], Omar Elkeelany, et al. implemented the RC5 algorithm for providing security to data by using a secret key both for encryption and decryption processes. In [9], S.Poongodi, et al. makes a comparative study of various transformations in Robust Watermarking Algorithms. In [10],[11],[12],[13] and [14], various watermarking techniques have been described, namely, Spread Spectrum, Scalar Costa Scheme-Quantization Index Modulation, Rational Dither Modulation, Singular Value Decomposition.

II. METHODOLOGY

The image was treated with the concept of encryption and then the watermark embedding was performed. The watermark extraction/detection was also performed. In

Manuscript received Jan, 2013.

Aparna Soni*, Computer Science & Engineering, Chhatrapati Shivaji Institute of Technology,. Durg, Chhattisgarh, India..*

Deepty Dubey, *Computer Science & Engineering, Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India.,*

JPEG2000 encoder, the 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. The compressed byte stream is arranged into different wavelet packets based on resolution, precincts, components and layers[3]. Thus, it is possible to select bytes generated from different bit planes of different resolutions for encryption and watermarking.

A. Encryption

The security of multimedia data in digital distribution networks is commonly provided by encryption, i.e., the mathematical process that transforms a plaintext message into unintelligible cipher text.

In JPEG2000 images, the packetized byte stream X as JPEG2000 output is gained, where $X = \{x_i\}, x_i \in [0,255] \forall i = 0,1,\ldots,l-1$. l is the length of the message in bytes. In order to encrypt the message X , K was selected, a randomly generated key-stream using RC4, within the set $K = \{k_i\}$ where $k_i \in [0,254] \forall i = 0,1,\ldots,l-1$. Then the encryption is done byte by byte as given in equation (1), to get the ciphered signal S

$$S = F(X,K) = s_i$$

$$s_i = (x_i + k_i) \bmod 255 \forall i = 0,1,\ldots,l-1 \qquad (1)$$

where $F(\cdot)$ is the encryption function and the addition operation is arithmetic addition. Let $S_1 = F(X_1, K_1)$ and $S_2 = F(X_2, K_2)$. For $K = K_1 + K_2$ additive homomorphism property gives,

$$D(S_1 + S_2, K) = X_1 + X_2 \qquad (2)$$

Thus this stream cipher has additive privacy homomorphism property. Since the watermarking technique used is an additive one, the encryption algorithm must have privacy homomorphism property with addition. 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. Security of this stream cipher will be elaborated. Distributors in the distribution chain will be given this compressed encrypted byte stream S to distribute. They do not have access to the original image. Often distributors need to watermark S to prove their distributorship to the recipient or copyright violation detection purposes[15].

B. Watermark Embedding

Since the encryption algorithm is with additive privacy homomorphism property, any robust additive watermarking technique can be used. Use of spread spectrum technique for the purpose. For watermarking, the ciphered bytes from the less significant bit planes of the middle resolutions were considered, because inserting watermark in ciphered bytes from most significant bit planes degrades the image quality to a greater extent. Also, the higher resolutions are vulnerable to transcoding operations and lower resolution contains a lot of information, modifying which leads to loss of quality. The impact on quality of watermarking in the compressed-encrypted domain was studied. It was also experienced that how the watermark can be inserted in less significant bit planes of middle resolutions without affecting the image quality much.

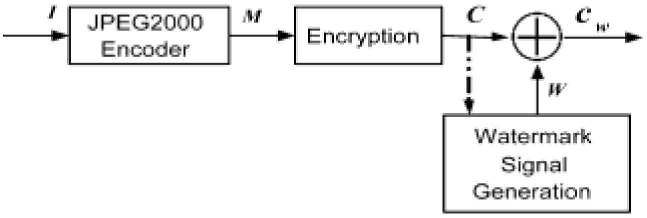

Fig. 1. Watermark Embedding

Let the watermark information bits be $y = \{y_i\} \forall i = 0,1,\ldots,n-1$, where $y_i \in \{-1,1\}$. This is then spread by a factor chip rate R , which gives

$$z_j = y_i, iR \leq j < (i+1)R \qquad (3)$$

The sequence z_j is then multiplied by a strength factor $\alpha > 0$ and PN sequence $P = \{p_j\}$ with zero mean and variance σ_p^2 ,where $p_j \in \{-1,1\}$. The watermark signal $W = \{w_j\}$, where,

$$w_j = \alpha a_j p_j \qquad (4)$$

The watermark signal generated in equation (4) is added to the encrypted signal B, to give the watermarked signal B_w ,

$$B_w = B + W = b_{w_i} = b_i + w_i \forall i = 0,1,..l-1$$

(5)

Thus, watermark embedding is carried out in compressed encrypted domain. However, it is shown that the watermarked quality can be controlled in a predictable manner. Distributor distributes the compressed-encrypted watermarked image[4].

C. Watermark Extraction/Detection:

The objective of the extraction process is to reliably obtain an estimate of the original watermark from a possibly distortion version of the watermarked image The watermark is extracted from the possibly corrupted watermarked image using the host image, by applying the inverse procedure at each resolution level to obtain an estimate of the watermark. The received compressed-encrypted watermarked image is first decrypted using the equation (6), which defines the corresponding byte by byte decryption for the encryption defined in equation (1).

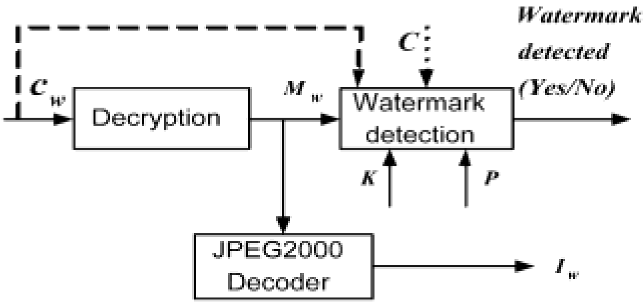

Fig. 2. Watermark Extraction/Detection

The key stream K can be generated as given in section of key stream generation. Let the watermarked image be denoted as $X_w = \{x_{w_i}\}$ where $x_{w_i} \in [0,255] \forall i = 0,1,\ldots,l-1$. Then the received signal B_w is decrypted to give X_w as,

$$\begin{aligned} X_w = D(B_w, K) &= (b_{w_i} - k_i) \bmod 255 \forall i = 0,1,..,l-1 \\ &= (b_i + w_i - k_i) \bmod 255 \\ &= x_i + w_i \\ &= x_{w_i} \end{aligned} \qquad (6)$$

where $D(.)$ is the decryption function. It can be seen from equation (6) that $x_{w_i} = x_i + w_i$, the watermarked compressed byte stream x_{w_i} is merely addition of compressed byte stream x_i and the watermark signal w_i. Thus by controlling the strength of w_i, choice of resolution levels and bit planes, the quality of the watermarked signal could be easily controlled. The watermarked quality would be poor if we pick up more number of resolution levels and bit planes to watermark, but the watermark embedding capacity would be high and vice versa. The embedded watermark information W can be estimated from X_w or B_w using correlation detector even without the knowledge of the corresponding originals X or B. In case of X_w it is multiplied by PN sequence P used for embedding, followed by summation over chip-rate window R, yielding the correlation sum H_i.

$$\begin{aligned} H_i &= \sum_R (x_{w_i} p_j) \\ &= \sum_R (x_j + w_j) p_j \\ &= \sum_R x_j p_j + \sum_R w_j p_j \end{aligned} \qquad (7)$$

The first term in equation (7) is zero if X and P are uncorrelated. However, this is not always the case for real data. To obtain better detection results, we can pre-filter X_w and remove most of the image content. Assuming that the first term in equation (7) is zero

$$H_i = \sum_R (w_j p_j) = \sum_R \alpha a_j p_j p_j = c_i \sigma_p^2 \alpha R \qquad (8)$$

Thus, the sign of H_i gives the watermark information bit

$$sign(H_i) = sign(c_i \sigma_p^2 \alpha R) = sign(c_i) = c_i \qquad (9)$$

It is also possible to detect the watermark in the compressed encrypted watermarked image $B_{w.}$ Since $B_w = B + W$, the correlation detector can be applied to B_w instead of X_w Thus, assuming zero correlation between B and P.

$$H_i = \sum_R (b_{w_j} p_j) = \sum_R (b_j + w_j) p_j = c_i \sigma_p^2 \alpha R$$

(10)

Here again, the sign of H_i gives the watermark information bit as derived in equation (9). In case of copyright violation detection purpose, since the distributors have B, they can apply the non-blind detection technique, i.e., subtract away B from B_w to remove the correlation effect completely. Thus get a better watermark detection rate. However, the distributors can also use pre-filtered (semi-blind) detection technique. In case of ownership proving applications the pre-filtered (semi-blind) detection technique may be required[4].

The output obtained here after applying the concepts of Watermarking in compressed-encrypted domain was experienced in Fig.3.

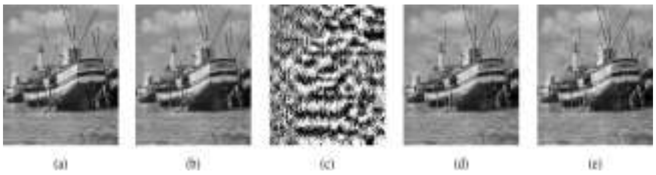

Fig. 3. (a) Original image. (b) Unwatermarked-decompressed image (45.08 dB). (c) Encrypted image. (d)Watermarked image (resolutions 1, 2, and 3) (32.80 dB). (e) Watermarked image (all resolutions) (31.15 dB).

III. Discussion

A. ***Spread Spectrum (SS):*** In spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth. Similarly, the watermark is spread over very many frequency bins so that the energy in any one bin is very small and certainly undetectable. Spreading the watermark throughout the spectrum of an image ensures a large measure of security against unintentional or intentional attack: First, the location of the watermark is not obvious. Furthermore, frequency regions should be selected in a fashion that ensures severe degradation of the original data following any attack on the watermark. This method uses the frequency hopping spread spectrum in order to determine positions for watermark embedding in an original image.

B. ***Scalar Costa Scheme-Quantization Index Modulation (SCS-QIM):*** In this scheme, given watermark strength, a quantiser is being chosen from an ensemble of quantizers to embed the watermark. It is all related to the quantizers. Watermark is estimated by quantizing the received signal to the nearest data in the codebook. The properties of the quantiser ensemble can be related directly to the performance parameters of rate, distortion, and robustness.

C. ***Rational Dither Modulation (RDM):*** The Rational Dither Modulation are vulnerable against value-metric scaling, it only needs that the features hosting the watermark are scaled by an unknown gain factor, to embed correct decoding of the watermark. RDM is an essentially scalar algorithm, since each feature ratio is quantised by itself, by means of a scalar quantiser. The detection of watermark is performed by the minimum distance criteria using the following equation. The distance is computed corresponding to both the quantizers and the one which gives minimum distance gives the watermark bit.

D. ***Singular Value Decomposition (SVD):*** The basic idea behind the SVD-based watermarking techniques is to find the SVD of the cover image or each block of the cover image, and then modify the singular values to embed the watermark. There are two main properties to employ the SVD method in the digital-watermarking scheme:

1) When a small perturbation is added to an image, large variation of its singular values does not occur.
2) Singular values represent intrinsic algebraic image properties.

From the perspective of image processing, an image can be viewed as a matrix with nonnegative scalar entries. The SVD of an image I with size $v \times v$ is given by $I = UVG^T$, where U and G are orthogonal matrices, and $V = diag(\lambda_i)$ is a diagonal matrix of singular values $\lambda_i, i = 1,.....,v,$ which are arranged in decreasing order. The columns of U are the left singular vectors, whereas the columns of G are the right singular vectors of image I [13].

E. ***Key Stream Generation:*** The key stream is generated at the encryption and decryption site using RC4 cipher. For encryption, a secret seed O is applied to RC4 cipher which in turn generates the key stream K. In order to generate the same key K at the decryption site, the seed O must be delivered to the decryption site through a secret channel. Once the seed O is received, it can be applied to RC4 cipher to generate the key stream K [3].

F. ***Security of Watermarking Algorithm*****:** The security and robustness of the watermarking algorithm depends on the various watermarking techniques and the encryption standards used. The attacks to retrieve or destroy the watermark can be performed either in encrypted or decrypted compressed domain. However, attacks in encrypted domain may result into a random decrypted stream which degrades the image quality. Hence, decrypted-compressed content provides a better domain to attack. These attacks can be protected using the encryption as well as watermarking approaches. And to very increased level the security must be provided in this case. The most important uses of watermarks include copyright protection and ownership authentication for the multimedia data that flourish at the advent of the Internet.

IV. Conclusion

In this survey paper, a technique is studied to embed a robust watermark in the JPEG2000 compressed encrypted images. The algorithm is simple to implement as it is directly performed on the compressed-encrypted domain i.e. it does not require decrypting or partial decompression of the content. The scheme also preserves the confidentiality of content as the embedding is done on encrypted data. The homomorphic properties of the cryptosystem are exploited, which allows us to detect the watermark after decryption and control the image quality as well. The various techniques of Digital Watermarking were studied in which how a watermark will be embedded in images has been described.

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]. 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.

[3]. A. V. Subramanyam, Sabu Emmanuel and Mohan S. Kankanhalli, “Robust Watermarking of Compressed and Encrypted JPEG2000 Images”, IEEE *Transactions on Multimedia*, Vol. 14, no. 3, June 2012.

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

[5]. Ricardo L. de Queiroz, “Processing JPEG-Compressed Images and Documents,” *IEEE Trans on Image Processing*, Vol. 7, no. 12, Dec 1998.

[6]. A. Alice Blessie, J. Nalini and S.C.Ramesh, “Image Compression Using Wavelet Transform Based on the Lifting Scheme and its Implementation,” *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 3, No. 1, May 2011.

[7]. Vijaya K. Ahire, Vivek Kshirsagar, “Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images,” *IJCSNS International Journal of Computer Science and Network Security*, Vol.11 no.8, Aug 2011.

[8]. Omar Elkeelany, Adegoke Olabisi, “Performance Comparisons, Design, and Implementation of RC5 Symmetric Encryption Core using Reconfigurable Hardware,” Journal of Computers, Vol. 3, no. 3, March 2008.

[9]. S.Poongodi, B.Kalaavathi, “Comparative Study of Various Transformations in Robust Watermarking Algorithms” *International Journal of Computer Applications (0975 – 8887*) Vol 58 no.11, Nov 2012.

[10]. F. Hartung and B. Girod, “Watermarking of uncompressed and compressed video,” *Signal Process.*, vol. 66, no. 3, pp. 283–301, 1998.

[11]. 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.

[12]. 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.

[13]. Chih-Chin Lai and Cheng-Chih Tsai, “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition,” IEEE Trans. on Instrumentation and Measurement, Vol. 59, no 11, Nov 2010.

[14]. B.Chandra Mohan and S. Srinivas Kumar, ” A Robust Image Watermarking Scheme using Singular Value Decomposition,” *Journal of Multimedia*, Vol. 3, no. 1, May 2008.

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

Aparna Soni, received the B.E. degree in Computer Science & Engineering from Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India, in 2009. Currently she is pursuing MTech from Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India.

Her current research interests are in Cryptography and Watermarking Techniques.

Deepty Dubey, received the B.E. degree in Computer Science & Engineering from Shri Shankaracharya College of Engineering & Technology, Bhilai, Chhattisgarh, India, in 2005, the MTech. degree in Computer Science & Engineering, Rungta College of Engineering & Technology, Bhilai, Chhattisgarh, India., in 2010.

She is currently an Assistant Professor in Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India. Her current research interests are in Cryptography and Cloud Computing.