ROBUST WATERMARKING OF AES ENCRYPTED IMAGES FOR DRM SYSTEMS

V.Chandra Prasad
PG Scholar, Department of EEE
Kongu Engineering College, Erode-638052, India
chandraprasad90@gmail.com

S.Maheswari
Assistant Professor, Department of EEE
Kongu Engineering College, Erode-638052, India
maheswari_bsb@yahoo.com

***Abstract*— Digital image capturing, processing and distribution has showed a remarkable growth over recent years. This media content is sometimes distributed in encrypted format and watermarking of these media items for proof of ownership, media authentication needs to be carried out in encrypted domain to improve image security. Therefore it is sometimes necessary to embed watermark in encrypted media items for ownership declaration or copyright management purposes. DRM system is one such example where there is a challenge to watermark these encrypted data as the encryption would have randomized the incoming data. In this paper, a block cipher called AES-128 bit key encryption algorithm and DCT combined with DWT based watermarking algorithm to watermark the encrypted image were proposed which increases robustness of the watermark. These method embeds the binary watermark in encrypted image and decryption is done after extraction of watermark.**

Keywords*—*Advanced Encryption Standard(AES), block cipher, DCT-DWT watermarking, Robustness, Symmetric Encryption.

I. INTRODUCTION

Digital Rights Management (DRM) is a class of access control technologies that are used by hardware manufacturers, copyright holders with the intent to limit the use of digital content after sale. DRM reduces the use of digital content that are not desired by the content provider.

Encryption is called as the process of transforming information(plaintext) using an algorithm(cipher) to make it unreadable to anyone except those possessing authorization. The result of the process is an output ciphertext. Symmetric encryption or secret key encryption uses a common key to encrypt or decrypt the message. Public key encryption, commonly known as asymmetric encryption which uses two different keys such as a public key known by all and a private key known only by the sender and the receiver. Advanced Encryption Standard (AES) is a symmetric block cipher and became the designated successor of the Data Encryption Standard(DES). Watermarking is a process which embeds data into digital contents such as text, images, video and audio without degrading the overall quality of the digital media. The possible domain for watermark embedding is that of the wavelet domain. The Discrete Wavelet Transform (DWT) separates an image into a lower resolution approximation image (LL) ,horizontal (HL), vertical (LH) and diagonal (HH) detail components.

Many research works are developed for encryption and watermarking based authentication. In [1], the algorithm proposed is based only on JPEG2000 compressed code streams, since the embedding is done in the compressed ciphered byte-streams. Here, the embedding position plays a crucial role in deciding the watermarked image quality. In [2], new hybrid approach of encryption-compression is proposed which is based on the AES encryption algorithm and compression is done by the Faber-schauder Multi-scale Transform (FMT), in which image quality is lost due to compression of the input data. While in [4], the encryption is performed on most significant bit planes while watermarking the rest of lower significant bit planes. Suppose if lesser number of bit planes are used for encryption, an attacker can easily manipulate the un-encrypted bit planes and further extract some useful information from the image which leads to loss in image quality. In the technique proposed in [5], 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 as they have only the encrypted content. Also the watermark embedders donot have the key to un-encrypt the plain text values to embed the watermark. Thus, watermarking in encrypted domain is very challenging.

II. PROPOSED SCHEME

The overall block diagram of the proposed method is shown in Figure1. The input image to be transmitted is separated into wavelet sub-bands using 1-level haar transform. AES encryption algorithm is proposed to encrypt the LL sub-band and Block DCT based watermarking algorithm is used to embed binary watermark in LH sub-band. Generally, frequency-based techniques are very robust against attacks like compression and filtering because the watermark is generally spread throughout image. So, to obtain better imperceptibility and also robustness, the addition of the watermark is done in a transformed domain. Inverse DWT is used for obtaining the Encrypted-Watermarked image which is to be transmitted at the transmitter side. At the receiver side, watermark recovery and decryption is performed in respective sub-bands .

978-1-4673-5036-5/13/$31.00 © 2013 IEEE

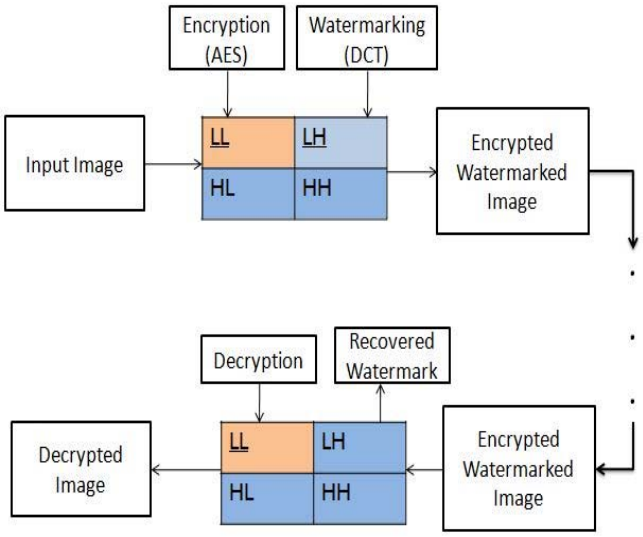


Figure1 Block diagram of the proposed scheme

III. AES ENCRYPTION

The input image to be transmitted is first separated into wavelet sub-bands and LL band is chosen for encryption since most of the image energy is concentrated at lower frequency sub-bands. AES-128(i.e.128 bit key) encryption algorithm is used for encrypting the LL sub-band. To reduce the computation time, particular region of the input image can be choosed encryption without doing it for whole image. AES-128 is used which has 10 rounds in order to minimize the number of if-then-else-conditions. The initial step of AES is to convert the input plaintext matrix into state matrix. State matrix is obtained calculating hexadecimal value of input matrix which is given as input to the forthcoming steps of encryption. The plaintext matrix is rearranged into state matrix and iteratively loops the state through 4 steps: Addroundkey, Subbytes, Shiftrows, and Mixcolumns.

The Addroundkey block performs bitwise xor of the state matrix and the round key matrix. The Subbytes block applies the S-box to one or more input bytes of input matrix. It performs the substitution function in which each byte of input matrix is replaced by the corresponding value in Sbox. The block shiftrows cyclically permutes (shifts) the rows of state matrix to the left. It takes the output matrix from subbytes step, cyclically shift the rows and give its output to next step. Polynomial matrices are used in the mixcolumns function, both matrices have the size of 4 × 4 and every row is a cyclic permutation (right shift) of the previous row. The mixcolumns transformation computes the new state matrix S0 by left multiplying the current state matrix S by the polynomial matrix P.The input parameters for encryption process are: the substitution table S-box, the key schedule w, and the polynomial matrix. The flowchart for AES encryption process is shown in Figure2.

A. Substitution tables

The substitution tables (S-boxes) are used by the expanded key schedule function, encrypting and decrypting functions to directly substitute a byte by another byte of the same finite field.

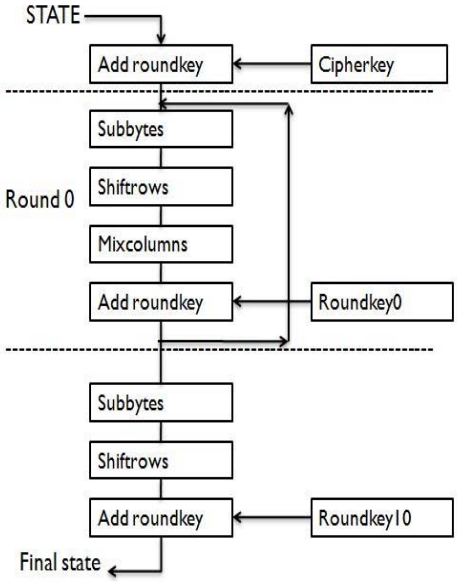


Figure2. AES Encryption Flowchart

S-box and Inverse S-box functions are the main blocks used by AES encryption. S-box is also used in Key expansion block. S-box generation process involves 2 steps in which first step is to search for multiplicative inverses of all elements and the second step of the S-box creation process is to perform affine transformation which consist of a polynomial multiplication with a specific constant.

B. Key Expansion

The round constant matrix is used in the key expansion scheme, which is a 10×4 matrix of zeros except for the first column which contains byte-conform powers of 2.The key expansion function takes the user supplied 16 bytes long key and utilizes the previously created round constant matrix and the substitution table S-box to generate a 176 byte long key schedule 'w', which will be used during both encryption and decryption processes.

C. Decryption

Decryption is to be done at receiver side for the same sub-band which is used for encryption. AES is a symmetric cipher, so key is common for both encryption and decryption. As in encryption process, but in the opposite order, it takes nine identical rounds of row shifting, byte substituting and column mixing and a final tenth round to get reshaped plaintext matrix. As encryption is combined with watermarking, security of the overall system could be greatly improved.

IV. WATERMARKING SCHEME

Watermarking in the DCT domain is usually performed on the middle or lower band frequency bands, as compressing the image leads to loss in higher frequencies. As DWT have excellent multi-resolution characteristics the idea of applying two transforms may lead to improved performance. It is based on the fact that drawbacks of both methods could be compensated by combining them which results in an effective watermarking.

A. Watermark Embedding

DCT watermarking can be done either for an entire image or blockwise on an image. In block-wise DCT method, the image is transformed into its DCT coefficients and the watermark is added to it. Finally the watermarked coefficients are inverse-transformed into the spatial domain thereby spreading the watermark throughout the block of the image. Here binary watermark of size 19x52 is used to embed it in original image of 512x512. In general most of the image energy is concentrated at the lower frequency sub-band so embedding watermarks in these sub-bands may degrade the image significantly. Also, changing the high frequency sub-band HH is not generally sensitive to human eye. So, many DWT-based watermarking algorithm uses middle frequency sub-bands LH and HL to embed the watermark where acceptable performance of imperceptibility and robustness could be achieved. In proposed scheme, to embed the watermark first step is to select the high frequency sub-bands in which human visual system is most sensitive. i.e. LH band and second step is to process the selected band in blocks. Transform each block using DCT and swap them according to the bit of the watermark.

B. Watermark Extraction

At receiver side, watermark is extracted by selecting the respective sub-band which contains watermark. Correlation value between original and recovered watermark will show quality of recovered watermark. The block diagram for embedding the watermark in wavelet sub-bands is shown in Figure. 3.

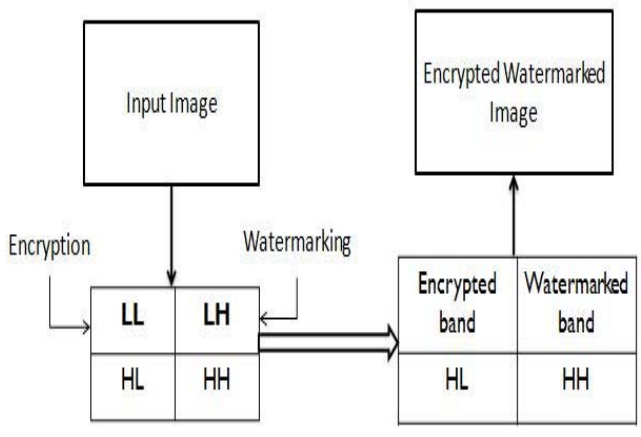


Figure3. Embedding watermark in sub-band

V. RESULTS

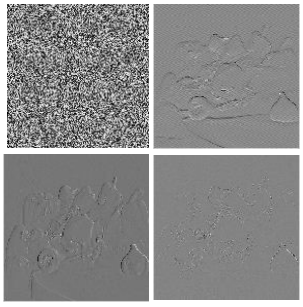
In this section, experimental results for various standard test images after encryption and watermark embedding on transmitter side, watermark extraction and decryption on receiver side are presented.

A. Encryption

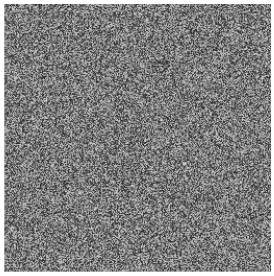
At the transmitter side, the original image is encrypted using AES-128(16 byte key) block cipher. As it performs on 16 bytes of data, 4x4 blocks are considered for encryption. Whole image or particular part of the image can be encrypted by iteratively looping it over that particular region. Here we chose entire LL sub-band to improve the overall security of the image as shown in Figure4 and Figure5.

(a) Input Image

(b) Original Watermark



(c) Encrypting & Watermarking



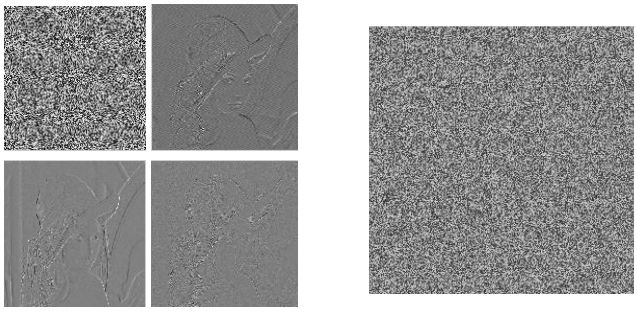
(d) Encrypted watermarked image

Figure4. Encryption: (a) Input Image (b) Original Watermark

B. Watermark embedding

Binary watermark of size(19x52) is embedded into the incoming image of size greater than the size of watermark. Encryption was done in low frequency sub-band LL and watermarking is to be done in middle frequency bands which achieves robustness. The input image is splitted into 4-sub-bands LL,LH,HL,HH using 1-level Haar Wavelet transform and watermark is embedded using DCT algorithm in LH,HL bands to improve robustness as shown in Figure4 and Figure5. Performance improvements could be obtained by combining DWT with DCT since these combined transforms could avoid the drawbacks of each other, resulting in effective and secured watermarking. Watermark capacity generally depends on both size of the image and size of watermark. In these proposed scheme capacity of watermark can be increased by embedding different watermarks in both LH and HL sub-bands.

(a) Input Image (b) Original Watermark



(c) Encrypting & Watermarking (d) Encrypted watermarked image

Figure 5. Encryption: (a) Input Image (b) Original Watermark c) Encrypting & Watermarking (d) Encrypted watermarked image

C. Watermark extraction

At receiver side, watermark is recovered from LH sub-band by comparing the swapped coefficients of the original sub-band. Correlation between original and recovered watermark is computed. Without any noise interruption at transmitter side, the recovered watermark at receiver side is shown in Figure 6.

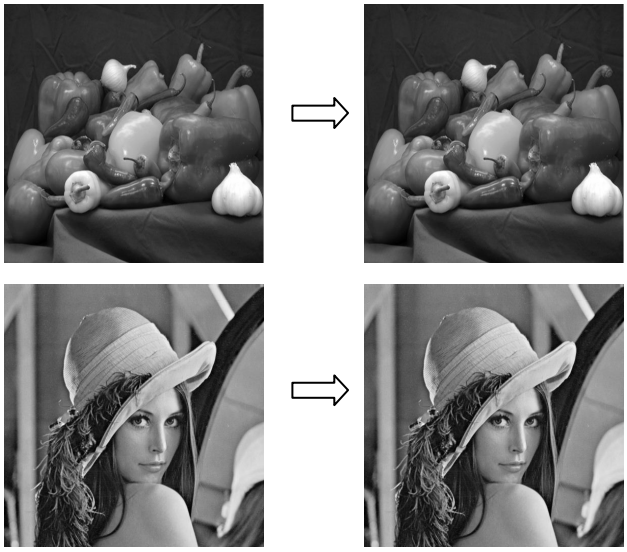
(a) Original image (b) Recovered Watermark

Figure 6. Watermark extraction: (a) Original image (b) Recovered Watermark

We achieve good correlation value for standard test images without any noise interference. Correlation between original and recovered watermark by considering noises such as Salt & Pepper, Gaussian, Poisson are also indicated.

D. Decryption

Decryption is to be done at the receiver side from LL sub-band. As encryption is done by considering LL sub-band and watermarking is performed on LH sub-band, the problem of random decryption is reduced when compared to decryption after watermarking the entire image as shown in Figure 7.



(a) Original image (b)Decrypted image

Figure. 7 Decryption: (a) Original image (b)Decrypted image

Peak Signal-to-Noise Ratio(PSNR) is the ratio between maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Imperceptibility of watermarked image by considering various test images are analyzed by calculating PSNR values between original and watermarked image as shown in Table1.

Table1 PSNR between Original and Watermarked image

IMAGE	PSNR(db) Value
Peppers.png	43.19
Lena.bmp	42.80
Cameraman.tif	43.01
Rice.png	42.84
Circuit.tif	43.50
Pout.tif	43.61
Coins.png	42.87

Imperceptibility of overall encrypted-watermarked image is analyzed by calculating PSNR between original and encrypted-watermarked image as shown in Table1. Less PSNR values

indicates that encryption is good enough to protect the transmitted images.

Table2 PSNR between Original and Encrypted-Watermarked images

IMAGE	PSNR(db) Value
Peppers.png	29.64
Lena.bmp	27.59
Cameraman.tif	27.90
Rice.png	28.36
Circuit.tif	30.18
Pout.tif	28.92
Coins.png	29.55

Robustness of recovered watermark is analysed by considering correlation values between original and recovered watermark as shown in Table2. Here correlation values without considering noises and after considering various noises are compared.

Table2 Correlation between Original and Recovered watermark

IMAGE	Without Noise	Salt & Pepper Noise	Gaussian Noise	Poisson Noise
Peppers	1	0.38	0.51	0.99
Lena	1	0.41	0.60	1
Cameraman	1	0.40	0.50	0.98
Rice	1	0.41	0.58	0.99
Circuit	1	0.36	0.58	1
Pout	1	0.40	0.52	1
Coins	1	0.41	0.54	1

PSNR between original and decrypted images is shown in Table3. Decryption is almost perfect as we have high Peak Signal-to-Noise ratio.

Table3 PSNR between Original and Decrypted image

IMAGE	PSNR(db) Value
Peppers.png	43.58
Lena.bmp	43.14
Cameraman.tif	43.40
Rice.png	43.21
Circuit.tif	43.93
Pout.tif	44.06
Coins.png	43.30

VI. CONCLUSION

In this paper, a robust watermarking algorithm is proposed to embed the watermark in encrypted image. AES algorithm improves the security of system even though it is symmetric and security of these algorithm can be further improved simply by adding more rounds into it at the cost of increase in computation time. The proposed method also prevents the confidentiality of content since encryption is combined with watermarking. Correlation between embedded and recovered watermark for various images were analyzed. Decryption after watermark extraction was done which is very challenging since the embedded watermark could alter the pixel values. Experimental results for decryption after watermarking provides good results.

REFERENCES

[1] A.V.Subramanyam, S.Emmanuel, 'Robust watermarking of compressed and encrypted JPEG2000 IMAGES', *IEEE Transaction on multimedia,* vol.14, no.3, pp.130-142, 2012.

[2] M.Benabdellah, M.M.Himmi, 'Encryption-Compression of Images Based on FMT and AES Algorithm', *Applied Mathematical Sciences*, vol.1, no.45, pp.203-219, 2007.

[3] Maheswari, S. and Rameshwaran**,** K**.**, "A robust blind image watermarking based on Double Haar Wavelet Transform (DHWT)", *Journal of Scientific and Industrial Research*, Vol. 71, No.5, pp. 324-329, May 2012.

[4] H.K.Varma,"Robustness of the Digital Image Watermarking Techniques against Brightness and Rotation Attack", International Journal of Computer Science and Information Security, vol. 5, no. 1, 2009 .

[5] Santi P. Maity, Malay K. Kundu, "A Blind CDMA Image Watermarking Scheme In Wavelet Domain," *International Conference on Image Processing,* vol. 4, pp. 2633-2636,2004.

[6] M.Cancellaro, M.Battisti, M.Carli, 'A joint digital watermarking and encryption method', *in Proc. SPIE Security, Forensics, Steganography, and Watermarking of Multimedia Contents*, vol. 68, pp.191–194, 2008.

[7] J.Prins, Z.Erkin, 'Anonymous fingerprinting with robust QIM watermarking techniques', *EURASIP J. Inf. Security, vol.1*. pp.13-17, 2007.

[8] Maheswari, S. and Rameshwaran, K., "Robust Blind Complex Double Haar Wavelet Transform Based Watermarking Algorithm for Digital Images", International Journal of Engineering and Technology, Vol.3, No.6, pp. 638-645, December 2011.

[9] 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, 2010.

[10] F.Battisti, M.Cancellaro, G.Boato, and M.Carli, 'Joint watermarking and encryption of color images in the Fibonacci-Haar domain', *EURASIP J. Adv. Signal Process.*, vol.4, pp.261-269, 2009.

[11] Maheswari, S. and Rameshwaran**,** K**.**, "3-D DWT based Multiple watermarking algorithm for spectral images", *IET International Conference on Sustainable Energy and Intelligent System*, pp. 780-784, July 2011.

[12] J.Eggers, R.Bauml, 'Scalar costa scheme for information embedding', *IEEE Trans. Signal Process.*, vol.51,no.4, pp.1003–1019, 2003.

[13] A.Klien, 'Attacks on the RC4 stream chiper', *Designs, codes, cryptography,* vol.48, no.3, pp. 269-286, 2008.

[14] 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,* pp. 627–630, 2007.

[15] S.Fluhrer, and I.Mantin, 'Weaknesses in the key scheduling Algorithm of RC4', *Lecture Notes in Computer Science,* pp.1–24, 2001.

[16] S.Lian, Z.Liu, R.Zhen, 'Commutative watermarking and encryption for media data', *Opt. Eng.,* vol. 45, pp. 1–3, 2006.

[17] C.Shanon, 'Communication theory of secrecy systems', *MD Comput.*, vol.15, no. 1, pp. 57–64, 1998.