Watermarking of Compressed imageswithImproved Encryption

Deepa L C
Department of Computer Science, CUSAT
TKM Institute of Technology
Kollam,Kerala,India
deepa08111989@gmail.com

Meerakrishna G H
Department of Computer Science, CUSAT
TKM Institute of Technology
Kollam,Kerala,India
meerakrishna1410@gmail.com

***Abstract*—Media data generally Handles In compressed and encrypted form. It is necessary To watermark these compressed encrypted media Items in the compressed encrypted domainitselffortamperdetectionorownershipdeclaration orcopyrightmanagement purposes. It is a challenge to watermark this media data in compressed and encrypted domain because of security and visual quality problems. The watermarking in encrypted domain gives double security. Thus it is necessary to choose a watermark embedding and encryption scheme for maintaining both security and visual quality. In this work, a robust approach for watermarking images in compressed and encrypted domain is presented. The encryption algorithm here used is Rijndael encryption algorithm. While the proposed technique embeds watermark in the compressed-encrypted domain, the extraction of watermark can be done in the decrypted domain. The watermark embedding technique used is Rational Dither Modulation (RDM).**

***Keywords*— Compressed and Encrypted domain watermarking, copyright, Visual cryptography, RDM**

I. INTRODUCTION

Watermarking has an important role in the digital media content distribution. It is necessary to watermark these compressed encrypted media items in the compressed encrypted domain itself for tamper detection or ownership declaration or copyright management purposes. Digital Right management system is an example, where the owner of multimedia content, distribute it in a compressed and encrypted format to consumers through multilevel distributor network, each distributor sometime needs to watermark the content for media authentication, traitor tracing or proving the distributorship. Watermarking has an important role in DRM systems. It helps publishers; copyright protectors etc to keep track their digital data after sale. It helps the developers to transfer the media data securely in this domain. In DRM systems there are multiple levels of distributers and consumers. The distributors don't have access to the plain text. This paper focus on the watermarking of compressed encrypted images, where the encryption refers to the ciphering of complete compressed stream. Watermarking in compressed-encrypted content saves the computational complexity as it does not require decompression or decryption, and also preserves the confidentiality of the content because it doesn't need decryption at the time of watermark embedding.A V Subramanyam (2012) [1] proposed a robust watermarking algorithm to watermark jpeg2000 compressed encrypted images.The technique here used was spread spectrum. But the problem was that this technique has only low number of bit capacity. GaoHai-ying, Liu Guo-qiang, and XuYin(1993) [2] proposed a new robust watermarking algorithm for JPEG2000 images. Here the watermark information is embedded by modifying the wavelet coefficients in pairs after quantization of the original image. The main problem of this work was image quality degradation and the lack of ability to resist attacks. To overcome this problem Kan Li and Xiao-Ping Zhang(2001) [3] proposed a robust adaptive watermarking scheme .It was a compression degree adaptive method .Here the watermark will be embedded in to the middle frequency wavelet coefficients after quantization. But this approach couldn't overcome the security problems. Roland Schmitz (2006) [4] proposed a commutative watermarking encryption method. It was designed by combining histogram based watermarking scheme with a permutation cipher. Here the permutation cipher is used toencrypt the multimedia data. The disadvantage of this work was that it was not a secure method. Zhi Li and Yong Lian (2007) [5] introduced a method for content dependent watermarking and authentication. It had been proposed as a solution to overcome the potential estimation attack aiming to recover and remove the watermark from the host signal. A watermarking scheme based on TCQ quantization scheme was proposed by D.Goudia(2009) [6]. The main contribution is that this system allows both quantization of wavelet coefficients and watermark embedding by using the same quantization module.

In this paper we focus on watermarking of compressed-encryptedimages, where the encryption refers to the ciphering of images in compressed stream. The aim of watermarking is to provide the digital media content creator with the ability to keep track of their media data after sale. Watermarking is a data hiding method. This technique is mainly used in one to many communications. Watermarking can be done in encrypted domain or compressed domain. The problem of watermarking in encrypted domain is that changing a single bit

may lead to random decryption and there is no strong security in compressed domain. So here we choose the compressed and encrypted domain. In our algorithm the watermark embedder only have compressed encrypted content. Also the watermark embedders do not have the key to unencrypt and get the plain text compressed values. However the proposed system faces the following challenges.

1) *Compressed Domain Watermarking:* A small modification in the compressed data may lead to the degradation of decoded image. Thus we have to find the place for embedding the data very carefully, so we can reduce the visual quality degradation.

2) *Encrypted Domain Watermarking and Watermark Retrieval:* In an encrypted piece of content, changing even a single bit may lead to a random decryption; therefore the encryption should be such that the distortion due to embedding can be controlled to maintain the image quality. It should also be possible to detect the watermark correctly even after the content is decrypted. Also, the compression gain should not be lost as encryption may lead to cipher text expansion.

This paper is organized as follows. Section II describes the proposed scheme. In section III we discuss the encryption algorithm, watermark embedding and extraction algorithm .The experimental results are discussed in Section IV. Section V concludes the paper. The theoretical analysis and derivations are given in the Appendix.

II. PROPOSED SCHEME

Overview

At first blue region detection is performed on input image using HSV color space.Secondly cover image is transformed in frequency domain. (DWT) This is performed by DWT on image leading to four subbands.Then payload (number of bits in which we can hide data) is calculated. Then secret data embedding is performed in one of the high frequency sub-band by tracingblue area pixels in that band.Then extract it.

Plain Text (In form of Image)

↓

Encryption (Creating shares)

↓

Channel (Cover image , Dither Modulation)

↓

Extraction

↓

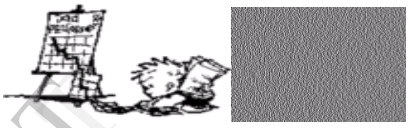
Decryption

A. *Image Compression*

The image compression is divided into five stages. In the first stage the input image is preprocessed by dividing it into non-overlapping rectangular tiles, 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 followed by quantization in the third stage. Multiple levels of DWT gives a multi-resolution image. The lowest resolution contains the low-pass image while the higher resolutions contain 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.

B. *Encryption Algorithm*

The encryption method we are using here is Visual cryptography&Rijndael. The secret image will be divided into two shares


Share 1


Share2

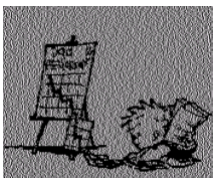

Stacking the shares reveals the secret.

Fig 1:Visual cryptography

Visual cryptography scheme in computer representation using n×m matrix is as follows:

Orginalpixel : 1 0

Share 1 (S^1) :

Share 2 (S :

$$S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

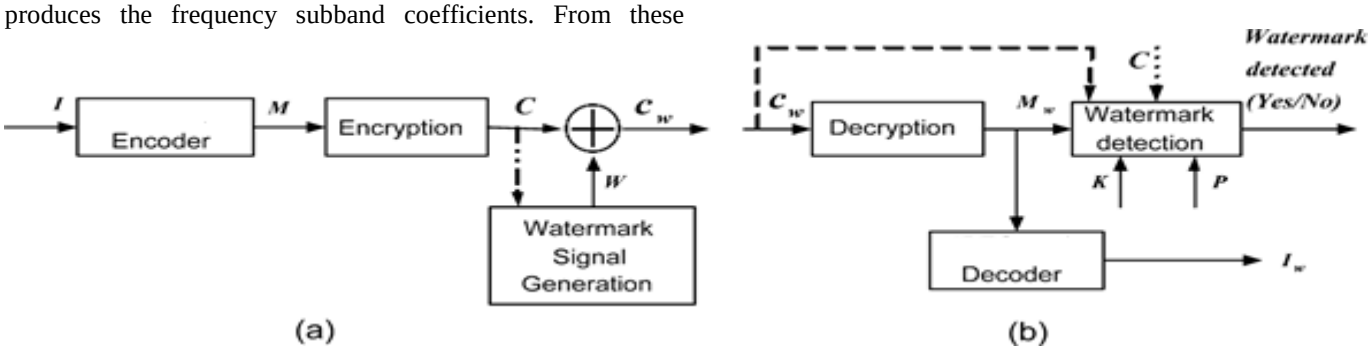
$$S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

Using the permutated basis matrices, each pixel from the secret image will be encoded into two sub pixels on each participant's share. A black pixel on the secret image will be encoded on the *ith* participant's share as the *ith* row of matrix *S1*, where a 1 represents a black sub pixel and a 0 represents a white sub pixel. Similarly, a white pixel on the secret image will be encoded on the *ith*participant's share as the *ith* row of matrix *S0*.

C..*Embedding Algorithm*

The embedding algorithm uses color image as cover and grayscale image as watermark. The color image is decomposed into Luminance, Intensity and Hue channels. The DWT is applied on the Luminance channel of color image, which produces the frequency subband coefficients. From these subband coefficients the highest texture energy subband is selected. On this subband apply *DWT* to obtain the second level decomposition. From this again select a subband having hightexture energy. Before embedding the watermark into selected subbands, the watermark image is split into two shares by applying (2, 2)−*V CS* scheme using *AOD* . Out of these two shares one share is embedded into selected subband and other share is kept secret.

The details of the algorithm is as follows:
Algorithm: Watermark Embedding Algorithm.
Input : Cover (Color) image, Watermark (gray-scale) image.
Output : Watermarked color image.
1) Read the cover (color) image *I* of size $N \times N$ and watermark (gray-scale)image*W*of size $M \times M$
2) Decompose the color image into Luminance (*Y*), Intensity (*I*) and Hue (*Q*) channels of size $M \times M$
3) Split the watermark by applying *V CS* using *AOD* is kept secret and *S*1 is used for embedding.
4) Apply *DWT* on Luminance (*Y*) channel to get subband coefficients (*LL*1, *LH*1, *HL*1 and *HH*1).
5) Extract the texture property *Energy* for each subband coefficient
6) Select the subband frequency coefficients (*LL*1 or *LH*1 or *HL*1 or *HH*1) which is having high energy.
7) Apply the *DWT* on selected subband to get second level decomposition (*LL*2, *LH*2, *HL*2 and *HH*2).
8) Extract the vector of texture property *Energy* for each subband of second level decomposition
9) Select the subband which is having high energy from second level decomposition (*LL*2,or*LH*2 or *HL*2 or *HH*2).
10) Embed the share *S*1 produced in Step 3 into the selected subband coefficients of Step 9 using following steps.
for*i*= 1 to *M* do
for*j*= 1 to *M* do
$Y\_(i, j) = (|Y(i, j)| + \alpha)S1(i, j)$
end for
end for



Where $Y\_(i, j)$ represents the modified frequency coefficient of subband, $Y(i, j)$ represents the original frequency coefficient of subband, α represents the watermark scaling factor.
11) The value of α is adjusted such that the texture properties of embedded subband are changed by negligible value
12) Replace the modified subband coefficients into its initial location and apply twice inverse DWT to get the watermarked Luminance channel.
13) Combine the watermarked Luminance (*Y*) channel with Intensity (*I*) and Hue (*Q*) to get watermarked color image.

D. *Extraction Algorithm*

Extraction algorithm is of type blind extraction which uses only watermarked color image as input. The watermarked color image is decomposed into Luminance, Intensity and Hue channels. The DWT is applied on the Luminance channel of watermarked color image, which produces the frequency subband coefficients. From these subband coefficient the highest texture energy subband is selected. On this subband apply DWT to obtain the second level decomposition. From this againselect a subbandhaving high texture energy. The watermark is extracted from these selected subband coefficients. After extracting the watermark, the watermark image is superimposed with secret share using *V CS* scheme as explained in Section 3. The output of superimposition produces the extracted watermark. The details of the extraction algorithm are explained below.

Algorithm: Watermark Extraction Algorithm.

Input : Watermarked (Color) image.
Output : Extracted watermark.
1) Read the watermarked color image I of size $N \times N$
2) Decompose the watermarked color image into Luminance (Y), Intensity (I) and Hue (Q) channels of size $M \times M$
3) Apply *DWT* on Luminance (Y) channel to get subband ($LL1$, $LH1$, $HL1$ and $HH1$).
4) Extract the texture property *Energy* for each subband coefficients.
5) Select the subband frequency coefficients ($LL1$ or $LH1$ or $HL1$ or $HH1$) which is having high energy.
6) Apply the *DWT* on selected subband to get second level decomposition subbands($LL2$, $LH2$, $HL2$ and $HH2$)
7) Extract the texture property *Energy* for each subband of second level decomposition.
8 Select the subband frequency coefficients which is having high energy from second level ($LL2$,or$LH2$ or $HL2$or$HH2$).
9) Extract the share $S1$ from selected subbandcoefficientsof Step 9 using following steps.
for$i$= 1 to M do
for$j$= 1 to M do
if$Y$ _ _ 0 then
$S_1(i, j) = 1$;
else
$S(i, j) = 0$;
end if
end for
end for
10) Superimpose extracted share $S_1$with secret share $S0$using *V CS*

III. RESULTS AND DISCUSSION

Security of Encryption Algorithm

To verify the effectiveness of the proposed scheme, a series of experiments were conducted. By keeping the cipher structure simple, it becomes accessible to a larger set of people for evaluation. The simplistic structure also plays a part in performance and security. The security of the cipher is amplified by the simple structure. For instance, the rate of diffusion is improved by several simple steps in the round: integer multiplication, the quadratic equation, and fixed bit shifting. The data-dependent rotations are improved, as the rotation amounts are determined from the high-order bits in *f(x)*, which in turn are dependent on the register bits. The security has been evaluated to possess an "adequate security margin"; this rating is given with familiarity of theoretical attacks, which were devised out of the multiple evaluations. The AES-specific security evaluations provide ample breadth and depth to how RC6 security is affected by the simplicity of the cipher.

Table 1 : Algorithm comparison

Algorithm	**Key Size**	**Block size**	**Algorithm structure**	**Rounds**	**Existing cracks**
Rijndael	128,192,256 bits	128	Substitution ,permutation	10,12 or 14	Side channel attacks
Twofish	128,192,256 bits	128	Feistel Network	16	Truncated differential cryptanalysis
Blowfish	32-448 bit	64	Feistel Network	16	Second order differential attacks
RC4	Variable	Variable	Stream	Unknown	Weak key schedule
RC2	8- 128 bit	64	Heavy Fiestel Network	16	Related key attacks
TripleDES	112 or 168 bits	64	Feistel Network	48	Theoritically possible
DES	56 bits	64	Feistel Network	16	Brute force attacks

IV. CONCLUSION

This paper provides double security through encryption and watermarking. Encryption provides security by hiding the content of secret information; while watermarking hides the existence of secret information. Earlier works were concentrated on encrypted or compressed domain only.The proposed system helps to embed a robust watermark in the compressed encrypted images using the watermarking scheme spread spectrum. 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. This scheme also preserves the confidentiality of content as the embedding is done on encrypted data. The homomorphic property of the cryptosystem is exploited, which allows us to detect the watermark after decryption and control the image quality as well.

ACKNOWLEDGEMENT

This workwassupportedin partbythe Departmentof ComputerScience&Engineering, TKMIT,andKollam.We wouldliketoshow ourgratitudetoProfP.Mohamed Shameem&Asst.Prof.Meerakrishna G Hfortheirvaluable guidance.

REFERENCES

[1] A.V.Subramanyam,SabuEmmanuel,"Robustwatermarkingof compressed encrypted JPEG 2000images," IEEEtransactions on multimedia, vol. 14, no.3, june 2012.

[2] Guo-quang,LiuGuo-qiang and Xuyin,"A New Robust watermarking algorithm for JPEG2000 images,".

[3] KanLiand Xiao-Ping Zhang, "Reliable Adaptive Watermarking Scheme Integrated with JPEG2000,"Proceedings **of** the **3rd** International Symposium on **Image** and Signal Processing and Analysis (2003).

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