International Research Journal of Computer Science (IRJCS)
Volume 1 Issue 4 (December 2014)
ISSN: 2393-9842
www.irjcs.com

Invisible Data Hiding on Compressed & Encrypted JPEG2000 Images

Krishna P. Tayade
Dept. Of Computer Engineering,
MIT Pune, University of Pune.

Mrs. Sarika S. Bobde
Dept.Of Computer Engineering,
MIT Pune, University of Pune

Abstract— Rational Dither Modulation (RDM) is an efficient method of invisible watermarking. In the digital world, images are available in various formats. They are simple to copy, resell & distribute without any loss of quality in the content. The digital data is distributed in compressed and encrypted form in the system called as Digital Asset Management System (DAMS). It becomes necessary to watermark this form of data to copyright management purpose and ownership declaration. By watermarking the compressed and encrypted data, there is degradation of an image quality. In the proposed scheme, using JPEG2000 compression, the information of raw data is packed and RC6 encryption block cipher algorithm ciphered the compressed byte stream. Rational Dither Modulation encodes watermark in the compressed and encrypted domain and extraction of watermark can be done in encrypted and compressed domain. Using JPEG2000 compression, it becomes easy for transmission. RC6 encryption provides security & confidentiality to the data while transmitting. RDM invisible watermarking provides copyright management & ownership declaration. Invisible watermarking is having advantage over visible watermarking as it is very difficult to remove from the content. The digital media data is normally distributed by multiple levels of distributors in encrypted and compressed form. The invisible watermarking scheme, Rational Dither Modulation investigates robustness & security.

Keywords— Rational Dither Modulation, Digital Asset Management System, JPEG2000, RC6 Block Cipher, Copyright Management, Ownership Declaration.

I. INTRODUCTION

Now a day's business is changed, multiple distributors are involved in between sellers & buyers. Different business models are used to complete the operation of delivery of digital content. Two parties (Buyer & Seller) business models are replaced by Multiparty Multilevel Digital Right Management (MPML-DRM) architectures. To make the working of business model efficient, the digital content should be secured, compact & confidential. In order to achieve the above properties, the digital content have to be in compressed & encrypted form. A digital asset management system (DAMS) normally works on media data in a compressed and encrypted form. Now the question is, is it possible for the compressed & encrypted data to provide the copyright management, ownership declaration & tamper detection? Hence there is need of watermarking.

To watermark these compressed encrypted byte streams is a challenge, as the compression process would have packed the information of raw media into a low number of byte stream and encryption would have randomized the compressed byte stream. It's not easy to perform embedding & extracting watermark on the compressed and encrypted data. There are different types of watermarking algorithms available which falls into two categories as visible watermarking & invisible watermarking. In visible watermarking, the data which is to be watermark would be visible & in invisible watermarking, the data which is to be watermark is in hidden form. It's very difficult to remove the hidden watermark from the content. It helps the watermark embedding party by being robust against malicious agent.

The E-commerce applications are very popular for purchasing. In that actual seller is unknown to buyer. Buyer can identify only lower level distributor. If there any fault may occurs then buyer can complaint it to lower level distributor. The one then forward the complaint to higher level distributor in multilevel distributor system. The complaint should be resolved; seller might accept his mistake only when the object is the one which is sent by him. Otherwise he can deny exchanging it. A third party authority should judge the things genuinely. The same system is applicable for media content which are spread through Internet. There should be proper system which resolve the issues between client & seller effectively & perform smooth & healthy business environment.

After content is downloaded, no further protection is provided on that content which raises Intellectual property issues. DRM (Digital Rights Management) technologies were developed to ensure the protection of digital information. It involves two party systems which contain the owner and consumers. For scalability of business, it is important to add levels of distributors and sub-distributors who can distribute and promote the content in regions unknown to the original owner. A visible watermarking can be easily identified & removed as compared to invisible watermarking. Invisible watermarking is robust against brute-force attack. For copyright management & ownership declaration, the watermarking is essential. To make digital data secure, it should be encrypted. To increase transmission rate, the data should be in compressed form.

In the system, the image is first compressed using standard JPEG2000 compression which include discrete wavelet transform then the output after compression is encrypted using RC6 block cipher. The output from the

encryption process is then watermarked with invisible scheme i.e. Rational Dither Modulation. The compressed encrypted watermarked data is then sent to receiver through network where it loses its image format totally. It's not easy to identify about transmitted data as it is in streamed form. From the streamed data watermark signal is detected by receiver then it is decrypted using key of RC6 cipher. Then it is uncompressed with JPEG2000 decoder.

.

II. Literature Survey

A. Digital Asset Management System (DAMS)

Digital asset Management System uses protocol for grouping, archiving, optimizing, downloading, maintaining, reforming and sending files in encrypted and compressed type. [2] It consists of management tasks and choices encompassing the uptake, annotation, storage, retrieval and distribution of digital assets. Digital pictures, animations, videos and music exemplify the target areas of digital plus management.

B. Digital Right Management (DRM)

It is the system of distribution of media content during a compressed & encrypted format to consumers through hierarchical distributor network. Digital rights management (DRM) design involving many levels of distributors in between associate owner and a consumer has been advised as an alternate business model to the standard two-party (buyer-seller) DRM design for digital content delivery. [4] In the two-party DRM design, techniques are used for secure delivery of the data. The protocol which is implemented in the two-party case for secure content delivery may be directly applied to the multiparty structure case.

C. Buyer Seller Watermarking Protocol

It is based on composite signal illustration where content is accessible solely in encrypted type to the watermark embedder & the watermark signal are depicted using features of plain text. Watermarks have recently been projected for the needs of copy protection and replica deterrence for multimedia content.[9] In copy deterrence, an owner (seller) embed a novel watermark into a duplicate of the content before it's sold to a client. If the customer sells unauthorized copies of the watermarked content, then these copies are derived to the unlawful reseller (original buyer) using a watermark detection formula.

D. Semi Fragile Authentication System

This scheme isn't totally compressed and encrypted domain watermarking compatible because it derives the content primarily based features for watermarking from the plain text. Semi-fragile image authentication deals with substantiating authenticity of a received image whereas permitting some acceptable manipulations. In an exceedingly semi-fragile authentication watermarking solution was projected for JPEG images. JPEG-specific invariant features are identified and used for image signature generation and embedding. Semi-fragile authentication of JPEG2000 images under a generic framework that ought to pass authentication are outlined based on concerns of some target applications.

E. Quantization Index Modulation

In this technique, the addition or subtraction of a watermark bit to a sample is predicated on the worth of measure plaintext sample. The watermark embedder doesn't have access to the plain text values. They need solely compressed-encrypted content & don't have the key to un-encrypt and obtain the plain text compressed values. Copyright notification, authentication and applications like digital audio broadcasting are examples of emerging multimedia system applications for digital watermarking.

F. 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.

I. Scalar Costa Scheme - Quantization Index Modulation (SCS-QIM)

The watermark signal can be detected before and after decryption in the compressed domain which is a suboptimal technique using scalar embedding and reception functions. Eggers et al. proposed SCS scheme for watermark embedding. In this scheme, given a watermark strength, quantizer is used to ensemble of quantizers to embed the watermark. [7]

J. Rational Dither Modulation

It is a quantization-based data-hiding technique that is basically liable to amplitude scalings and modifies it in such a way that the result becomes invariant to realize attacks. [6] 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. 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 is 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. [1]

III. System Design

System Architecture consist of six modules as follows

At Sender Side-

1. JPEG2000 Encoder
2. RC6 Encryption
3. RDM Encoder

At Receiver Side-

4. RDM Decoder
5. RC6 Decryption
6. JPEG2000 Decoder

A. *JPEG 2000 Compression*

At sender side, the original image is first compressed with JPEG2000 Encoder. It is divided into five different stages. In the first stage the input image is preprocessed by dividing it into non-overlapping rectangle tiles, the samples are then reduced by a constant to create it bilaterally symmetrical around zero and eventually a multi-component transform is performed. Within the second stage, the distinct wavelet transform (DWT) is applied followed by quantization within the third stage. Multiple levels of DWT provide a multi-resolution image. In that the lower resolution contains the low-pass image whereas the highest resolutions contain the high-pass image. These resolutions are more divided into smaller blocks called code-blocks wherever every code-block is encoded separately. After that the quantized DWT coefficients are divided into completely different bit planes and coded through multiple passes at embedded block coding with optimized truncation (EBCOT) to present compressed byte stream within the fourth stage.[8][1] In the fifth stage compressed byte stream is managed into completely different wavelet packets based on resolution, elements and layers. RC6 uses output obtained from all above stages for encryption process.

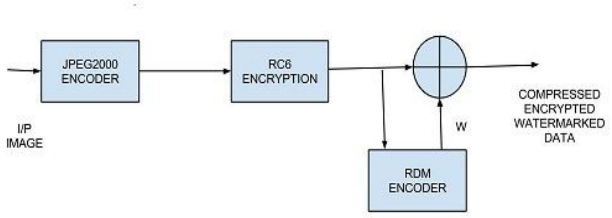

Fig.1 Watermark embedding

B. *RC6 Encryption Algorithm*

JPEG2000 gives out packetized byte stream as its output. In order to encrypt the message, RC6 encryption is used. A version of RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a positive number of rounds r and b denotes the length of the encryption key in bytes. Where w = 32 and r = 20. For all variants, RC6-w/r/b performs on units of four w-bit words using the following basic operations.

- A+B integer addition modulo 2w
- A-B integer subtraction modulo 2w
- A⊕B bitwise exclusive-or of w-bit words
- A*B integer multiplication modulo 2w
- A<<< B rotation of the w-bit word A to the left by the amount given by the least significant lg w bits of B
- A>>> B rotation of the w-bit word A to the right by the amount given by the least significant lg w bits of B
- (A,B,C,D) = (B,C,D,A) parallel assignment.

In decryption, the round key of encryption is applied in reverse order. Thus, RC6 has Fiestel structure

1. RC6 Encryption Algorithm:

Input: Plain text stored in four w-bit input registers A, B, C, D
r- no. of 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 xor t) <<< u) + S[2i];
C= ((C xor u) <<< t) + S[2i+1];
```

```
                (A,B,C,D) = (B,C,D,A);
        }
                A = A + S[2r+2];
                C = C + S[2r+3];
```

2. RC6 Decryption Algorithm:

```
Input: Cipher text stored in four w-bit input registers A,  B, C, D
  r- no. of rounds
 w-bit round keys S[0,…..,2r+3]
Output: Cipher 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) xor u;
                A = ((A – S[2i] >>> u) xor t;
        }
                 D = D - S[1];
                 B = B - S[0];
```

C. Watermarking Algorithm RDM

Watermarking may be described as a way for embedding information into another signal. just in case of digital images, the embedded watermark may be either visible or hidden from the user. The system concentrates on hidden watermarks. Typical usage scenarios for watermarking are copyright management & ownership declaration. Since the embedding is done compressed ciphered byte stream, the embedding position plays a vital role when deciding the watermarked image quality.

1. RDM Encoder: Gonzalez et al. proposed a watermarking scheme based on quantization of the ratio of host signal to a function g (.). The quantizers are given by

$$Q'\Delta = 2\Delta + w\Delta/2$$

where w ε { -1, 1} is the watermark information to be embedded in the source element. The embedding rule can be defined as

$$C_{wi} = g(C_{wi-1})\ Q'\Delta\ \ (C_i / g\ (C_{wi-1}))$$

where C_{wi-1} and C_{wi} are the previous and current watermarked samples. Notice that C_{wi} is an amplitude enhanced version of scaled-quantized C_i. Thus following equation is possible,

$$W_i = C_{wi} - C_i$$

which gives the additive nature of watermark. The function g (.) is chosen such that the scheme is robust against amplitude scaling attacks and is given by

$$g(C_{wi-1}) = \left(\frac{1}{L_m}\sum_{j=i-L_m}^{i-1}\left|C_{wj}\right|^{\gamma}\right)^{\frac{1}{\gamma}}$$

One of the drawbacks with this scheme is that the watermarked sample may differ from the original sample to a large extent due to the function g (.) used for quantization. So, g (.) is scaled by a constant factor known at both encoder and decoder to control the amount of watermark added. Thus, watermark embedding is carried out in compressed-encrypted domain, and the watermarked content is then distributed by the distributors.

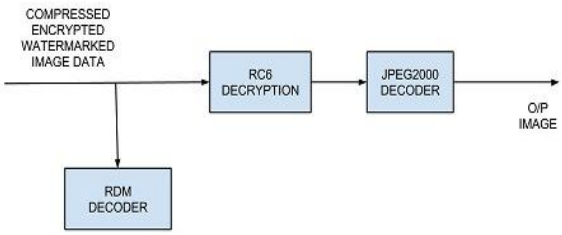

Fig.2 Watermark extraction

2. RDM Decoder: The watermark can be detected in encrypted & compressed domain. In encrypted domain, C_W is directly given to the watermark extraction module and the detection process is as follows. The detection of watermark is performed by the minimum distance criteria using the below equation,

$$w = \arg\min_{i=1} \left({C_{W_i}}/{g(C_{W_{i-1}})} - Q^i \left({C_{W_i}}/{g(C_{W_{i-1}})} \right) \right)^2$$

$\forall i$ = 1, ….L-1

Here, gives two quantizers belonging to bits 1 and -1. The distance is computed corresponding to both the quantizers and the one which gives minimum distance gives the watermark signal.

IV. RESULTS AND DISCUSSIONS

In the base paper, the encryption is applied using RC4 cipher. As it is a stream cipher, grayscale images can be encrypted easily. Grayscale image is having less data than color image. While implementing encryption on color images, its parameter should be considered. Each color image pixel is having three bytes data of RGB planes. In order to encrypt it effectively block cipher is appropriate. Block cipher works on 128 bit block size in AES. It becomes easy in case of color images to encrypt using block cipher as image data is large in number compared to grayscale image. We focus on parameters of image & its compatible algorithm which can be easily implemented on color images. On Java platform, its format compliancy is not maintained which gives more confidentiality as it cannot be easily identified as an image. The output from encryption stage is more compatible to the Rational Dither Modulation Encoder as it takes input in one dimensional array format. At every stage it gives more confidentiality to the data.

Experiments are conducted on color images of different sizes & resolutions. The graph is plotted of Bit Error Rate (BER) versus Watermark to Noise Ratio (WNR). It shows that as WNR increases BER stabilizes at 10^{-2} order which means that watermarked byte capacity increases without increase in BER. The BER becomes constant though there are higher no. of watermark bytes are embedded. It shows that image quality cannot be affected by no. of watermarked bytes.

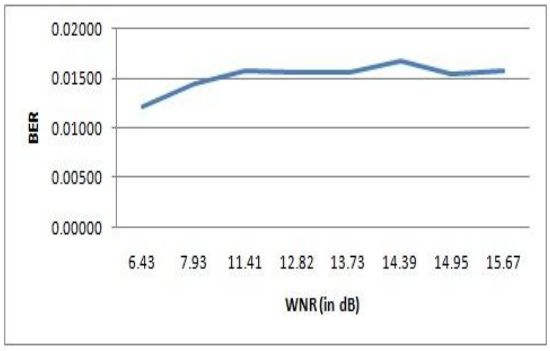

Fig.3 BER Vs WNR

The graph is plotted of Peak Signal to Noise Ratio (PSNR) versus Payload of compressed encrypted image & compressed encrypted watermarked image. It shows that as Payload capacity increases, PSNR increases when there is constant BER while embedding watermark.

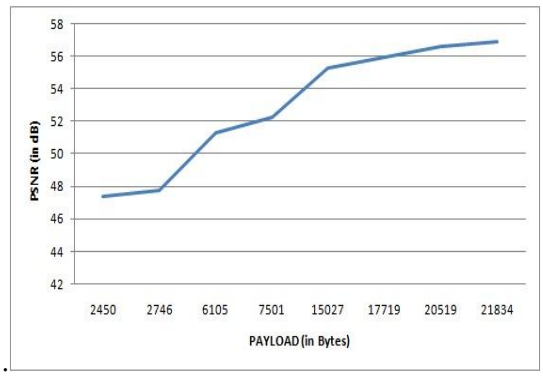

Fig.4 PSNR Vs Payload

V. CONCLUSION

The system gives business model for distribution of digital media in compressed & encrypted form along with copyright management & ownership declaration. It maintains the confidentiality of the content as the embedding is done on encrypted data. The system controls the image quality while applying different operations on the image while achieving goals of project. RDM provides robustness against brute force attack as watermark signal cannot be removed due to of its hidden form.

VI. FUTURE WORK

The RDM scheme implemented in the system is scalar in nature; using vector quantization better performance can be obtained. The proposed scheme can be applied on video.

REFERENCES

[1] A. V. Subramanyam, Sabu Emmanual and Mohan S. Kankanhalli, "Robust Watermarking Of Compressed & Encrypted JPEG2000 Images", *IEEE Trans. On Multimedia*, vol. 14, no. 3,Jun. 2012.

[2] 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.

[3] 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.

[4] 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.

[5] Arvind Kumar Parthsarathy and Subhash Kak, "An Improved Method of Content Based Image Watermarking", *IEEE Trans. On Broadcasting*, Vol 53, No.2, Jun 2007.

[6] 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.

[7] 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.

[8] YiweiWang, John F. Doherty, Robert E. Van Dyck "A Wavelet-Based Watermarking Algorithm for Ownership Verification of Digital Images", *IEEE Trans. on Image processing* , Vol. 11, No. 2, Feb 2002.

[9] N. Memon and P. Wong, "A buyer-seller watermarking protocol", *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[10] Khalid Sayood, "Introduction to Data Compression", 3rd ed.

[11] Chih-Wei Tang and Hsueh-Ming Hang, "A Feature-Based Robust Digital Image Watermarking Scheme", *IEEE Transactions on Signal Processing*, vol. 51, no. 4, April 2003.

[12] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic, and Christian Roux, "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 5, September 2012.

[13] Xiangyang Wang, Jun Wu, and Panpan Niu, "A New Digital Image Watermarking Algorithm Resilient to Desynchronization Attacks", IEEE *Transactions on Information Forensics and Security*, vol. 2, no. 4, December 2007.

[14] Qibin Sun and Shih-Fu Chang, "A Secure and Robust Digital Signature Scheme for JPEG2000 Image Authentication", *IEEE Transactions on Multimedia*, vol. 7, no. 3, June 2005.

[15] Chun-Shien Lu, Shih-Wei Sun, Chao-Yong Hsu, and Pao-Chi Chang, "Media Hash-Dependent Image Watermarking Resilient Against Both Geometric Attacks and Estimation Attacks Based on False Positive-Oriented Detection", *IEEE Transactions on Multimedia*, vol. 8, no. 4, August 2006.