International Journal of Students Research in Technology & Management
Vol 1 (05), September 2013, ISSN 2321-2543, pg 547-554

A SECURED AUTHENTICATED WATERMARKING TECHNIQUE

Priyanka U, Remya K R, Reenu R and Sai Subha V
M.Tech students, Department of Computer Science and Engineering,
Mohandas College of Engineering and Technology, Thiruvananthapuram
priyankayou@yahoo.in, remykr@gmail.com,
reenu.rahman@gmail.com, saisubhav@gmail.com

Abstract

Whenever media contents transmitted through the network, compressed and encrypted media data is used so it is important to give proper protection to the data items to avoid unauthorized access and for that we need to enhance media authentication and for that the compressed encrypted media data which is used to distribute through the network is watermarked for providing proof of ownership or distributorship. For doing compression JPEG 2000 compression and while doing compression the data is packed to low number of bits and to this data encryption is applied so stream cipher technique is used for avoiding media quality degradation and also this technique allow to do watermarking in a predictable manner. And a robust watermarking algorithm is used for watermarking this compressed and encrypted media data.

Keywords: Watermarking, JPEG2000.

1. INTRODUCTION

Image compression is to reduce irrelevance and redundancy of the image data in order to be able to store or transmit data in an efficient form. An image is essentially a 2-D signal processed by the human visual system. The signal representing images are usually in analog form. However, for processing, storage and transmission by computer applications, they are converted from analog to digital form. A digital image is basically a 2-Dimensional array of pixels. Image compression addresses the problem of reducing the amount of data required to represent a digital image. JPEG is commonly used method of lossy compression for digital photography. The JPEG compression algorithm is at its best on photographs and paintings of realistic scenes with smooth variations of tone and color. For web usage, where the amount of data used for an image is important, JPEG is very popular. On the other hand, JPEG may not be as well suited for line drawings and other textual or iconic graphics, where the sharp contrasts between adjacent pixels can cause noticeable artifacts.

In this paper, JPEG 2000 compression is used to compress the media content which is created, captured and processed is in distribution.

While there is a modest increase in compression performance of JPEG 2000 compared to JPEG, the main advantage offered by JPEG 2000 is the significant flexibility of the code stream. The code stream obtained after compression of an image with JPEG 2000 is scalable in nature. Another difference, in comparison with JPEG, is in terms of visual artifacts: JPEG 2000 produces ringing

artifacts, manifested as blur and rings near edges in the image, while JPEG produces ringing artifacts and 'blocking' artifacts, due to its 8×8 blocks. The aim of JPEG 2000 is not only improving compression performance over JPEG but also adding (or improving) features such as scalability and edit ability. JPEG 2000's improvement in compression performance relative to the original JPEG standard is actually rather modest and should not ordinarily be the primary consideration for evaluating the design. Very low and very high compression rates are supported in JPEG 2000. The ability of the design to handle a very large range of effective bit rates is one of the strength of JPEG 2000.

Here, the compressed image content to be transmitted is then encrypted using stream cipher technique. The Digital asset management systems use media data in a compressed and encrypted form. The encryption here means the ciphering of the complete Jpeg 2000 stream expect the headers and marker segments. Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys. In a stream cipher technique each plaintext digit is encrypted one at a time with the corresponding digit of the key stream, to give a digit of the cipher text stream.

Here, this compressed-encrypted image is watermarked for tamper detection or ownership declaration or copyright management purposes. A watermark is a visible embedded overlay on a digital photo consisting of text, a logo, or a copyright notice. The purpose of a watermark is to identify the work and discourage its unauthorized use. Though a visible watermark can't prevent unauthorized use, it makes it more difficult for those who may want to claim someone else's photo or art work as their own. So in this paper, the watermarking of image in a compressed and encrypted domain is implemented. This paper is organized as follows. Section II describes the related works. In Section III specifies the proposed scheme then in Section IV includes experimental results and Section V includes conclusion of the paper.

2. RELATED WORK

One of the weaknesses of all encryption systems is that the form of the output data (the cipher text), if intercepted, alerts the intruder to the fact that the information being transmitted may have some importance and that it is therefore worth attacking and attempting to decrypt it. This

Cipher text transmission can be used to propagate disinformation, achieved by encrypting information that is specifically designed to be intercepted and decrypted. In this case, system assume that the intercept will be attacked, decrypted and the information retrieved.

The 'key' to this approach is to make sure that the cipher text is relatively strong and that the information extracted is of good quality in terms of providing the attacker with 'intelligence' that is perceived to be valuable and compatible with their expectations, i.e. information that reflects the concerns/ interests of the individual and/or organization that Encrypted the data. This approach provides the interceptor with a 'honey pot' designed to maximize their confidence especially when they have had to put a significant amount of Work in to 'extracting it'. The trick is to make sure that this process is not too hard or too easy. 'Too hard' will defeat the object of the exercise as the attacker might give up; 'too easy', and the attacker will suspect a set-up. The disadvantage of existing systems is that this system allows limited participation to avoid traffic flow and from attack. It provides more security and is also applicable for authentication of e-documents. It is important for securing certificates, personnel documents, bond papers that are send via email.

In H Wang [8], for protection the commutative watermarking and encryption is proposed for media data. Here a partial encryption algorithm is adopted to encrypt the significant part of media data, while some other part is watermarked. These partial encryption algorithms encrypt only significant frequency bands that mean some significant part of the media contents. In [12] Li et al proposed constructing secure content based watermarking technique, in which watermarking is applied in an encrypted format and here distortion occurs in the host signal, it cause large effects in degradation of quality. In [11] J.Prins discussed about Anonymous fingerprinting with robust QIM watermarking technique, here the compressed and encrypted content only access no plain text can be accessed by the watermarking embedders through decryption .In [10] M. Cancellaro proposed a joint digital watermarking and encryption method, here the most significant bits is used for encryption and the lower bit is used for watermarking. But it is vulnerable because an attacker can easily extract useful information from the image. Because lesser number of bit planes are used for encryption so attacker can manipulate the unencrypted bit planes and the quality of image may be degraded.

3. PROPOSED SYSTEM

This system presents a method of 'hiding' encrypted information in a color digital image. In principle, any cipher can be used to do this providing it consists of floating point (or decimal integer) numbers that are ideally, uniformly distributed. The scheme allows for the authentication and self-authentication of documents such as letters, certificates and other image based data. The figure below shows the architecture of the proposed system.

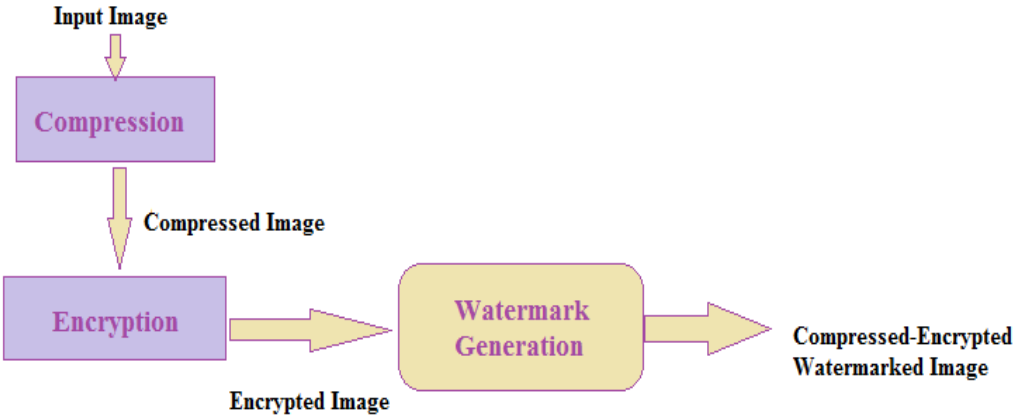

Fig 1 Watermark Generation

In this architecture, at first the input image is given to the JPEG 2000 Encoder, here the image is converted to editable format and then the compression of image takes place, later the compressed image is given for encryption and a ciphered content is obtained. Later watermarking is applied to this compressed encrypted image and Fig 1 gives the block diagram of watermark embedding and watermark extraction.

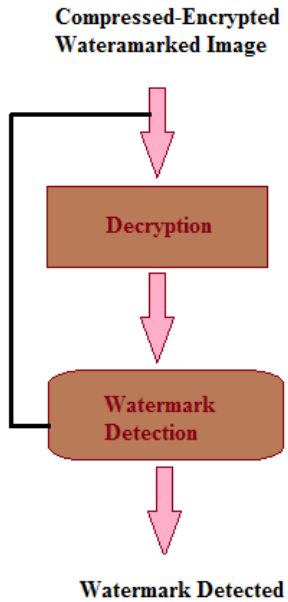

Fig 2: Watermark Detection.

During the watermark extraction phase the ciphered image can be decrypted and watermark can be detected and without decrypting also the watermarking can be done, this paper supports both provisions. Here after doing compression it may lead to the degradation of image quality therefore the

watermark applying position should be selected carefully then only degradation rate decreases. In the case of encryption also lead to quality variation because already the encrypted data means the data is scrambled so to that scrambled data again watermarking is applied so the distortion due to embedding should be controlled for avoiding picture quality degradation.

In this proposed system, during compression the input image of formats such as png16, png24, gif, jpeg are analyzed and processed. The analyzing is based on their current file size, pixel ratio, RGB color values etc that means the attributes of the image file and there are some unwanted attributes such as file additional title, creation of date and time user details etc these are removed and these are the first stage of processing and this time small amount of file size is reduced.

To this JPEG 2000 image compression is applied, here at first the image is converted to bit map because windows default file format is in bit map so the processing of the particular image will be easier. After that it is converted to pure binary format, it is possible to convert the initially processed image to binary format but windows need additional support for that.

Thus the binary formatted image file is processed after that by decreasing the corner position binary values to fully null and rest 50 percent of image is also reduced, below 50 reductions is not applied because it will affect the image quality. After that it is converted back to bit map format. After doing compression the next is encryption, here a random key is generated and this key is converted to binary format and this key is stored as an image attribute in the bitmap image and the message to be encrypted also converted and stored as the image attribute. After encryption the bit map image is converted to the original input image format. And this is decrypted for viewing the message and the decryption is done by getting the image file and getting the data with the help of some attribute such as time of recent creation and attribute addition. And the last phase is watermarking.

In this paper, it can be done after and before decryption. For doing watermark, at first the image is taken and its predefined particular area is selected and this pixel area is converted to pure binary data and also the text used for watermarking is also converted to pure binary form and both are appended and it is then converted to original format of image.

4. EXPERIMENTAL RESULTS

This section includes the experimental results of simple and effective watermarking technique on JPEG 2000 compressed and encrypted images. The Fig 3 and 4 gives the representations of two images which are watermarked after doing JPEG 2000 compression and encryption. Fig 2 (a) represents the input image; Fig 3 (b) represents the compressed and encrypted form of the input image. Fig 3 (c) represents the image after applying compression, encryption and watermarking. Similarly the same process is done to watermark the image given in Fig 4 (a).

5. CONCLUSION

In this paper, I proposed a robust watermarking in the JPEG2000 compressed encrypted images. The scheme preserves the confidentiality of content and the algorithm is simple to implement as a embedding is done on encrypted data. Here the main advantage is using JPEG 2000 compression because it maintains image quality with greater compression ratio. The aim of JPEG 2000 is not only improving compression performance over JPEG but also adding (or improving) features such as scalability and edit ability. JPEG 2000's improvement in compression performance relative to the original JPEG standard is actually rather modest and should not ordinarily be the primary consideration for evaluating the design and the encrypted data can be decrypted only with this application. The algorithm is performed in compressed-encrypted domain and the detection is also carried out in compressed or decrypted domain.

(a) (b) (c)

Fig 3: Representing Watermarking of Compressed-Encrypted Image. (a) Input Image, (b) Compressed and Encrypted Image and (c) Watermarked Compressed-Encrypted Image.

(a) (b) (c)

Fig 4: Representing Watermarking of Compressed-Encrypted Image. (a) Input Image, (b) Compressed and Encrypted Image and (c) Watermarked Compressed-Encrypted Image.

(a) (b) (c)

Fig 5: Representing Watermarking of Compressed-Encrypted Image. (a) Input Image, (b) Compressed and Encrypted Image and (c) Watermarked Compressed-Encrypted Image.

REFERENCE

1) A. V. Subramanyam, Sabu Emmanuel, Member, IEEE, and Mohan S. Kankanhalli, "Robust Watermarking of Compressed and Encrypted JPEG2000 Images" VOL. 14, NO. 3, JUNE 2012.

2) A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli, "Privacy preserving multiparty multilevel DRM architecture," in *Proc. 6th IEEE Consumer Communications and Networking Conf., Workshop Digital Rights Management*, 2009, pp. 1–5.

3) 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.

4) 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.

5) 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.

6) 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.

7) 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.

8) S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," *Opt. Eng.*, vol. 45, pp. 1–3, 2006.

9) 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.

10) A. 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.

11) J. Prins, Z. Erkin, and R. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," *EURASIP J. Inf. Security*, vol. 2007.

12) Z. Li, X. Zhu, Y. Lian, and Q. Sun, "Constructing secure contentdependent watermarking scheme using homomorphic encryption," in *Proc. IEEE Int. Conf. Multimedia and Expo*, 2007, pp. 627–630.

13) Q. Sun, S. Chang, M. Kurato, and M. Suto, "A quantitive semi-fragile JPEG2000 image authentication system," in *Proc. Int. Conf. Image Processing*, 2002, vol. 2, pp. 921–924.

14) R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978

15) S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

16) 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

17) P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *Lecture Notes in Computer Science*, pp. 223–238, 1999.