International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 4 • 2017

A Secure Watermarking Scheme for Compressed Images for Big Data Analytics

Ritu Gupta[1] and Abhilasha Singh[1]

[1.]Amity School of Engineering and Technology, Amity University, Uttar Pradesh, Emails: ritu4006@gmail.com, abhilashasingh28@gmail.com

Abstract: Free excess of data on internet raises grave security concerns. Social media applications like facebook, twitter, whatsapp etc are generating tons and tons of data every day. With the freely available huge data on cloud requires new innovative security applications to make data secure and feasible. Copyright protection is the biggest challenge in dealing with this data. Integration of social media data with other possible and related data is becoming more complex but challenging. Big data analytical tools generate new business opportunity in this scenario. Decision making without security and authentication of data becomes tough. Big data analytics offer a number of distinct advantages over other digital media like good quality, easy modifications and high fidelity copying. Several companies are eyeing various business opportunities based on big data like business forecasting. Due to its magnitude and importance, it created concerns over duplication and distribution anomalies has lead to the requirement of useful copyright protection tools. Different software based digital watermarking has been proposed in attempt to address these growing concerns of copyright protection of multimedia data. In present paper, a digital watermarking scheme to decide the legal rights of the digital images on cloud is proposed. A general hash algorithm is applied on host image to engender a hash value, which can be considered to be the fingerprint of the image. The secret key used in this case is the hash value for encryption techniques like Data Encryption Standard (DES). Then, standard encryption technique is used to encrypt consequential watermark. Finally, a Discrete Wavelet Transform based robust watermarking scheme is build to hide this encrypted watermark in the host image.

Keywords: Information, Watermarking, encrypted image, Copyright, Web.

1. INTRODUCTION

There is a hasty expansion in cloud based digital multimedia in the last few years and its processing becomes more and more complex. Security as well as ownership of the digital multimedia is great concerns to the users. Many researchers are working continuously for the better tool for the processing of these data. Due to its rapid growth, processing of the data becomes more complex. Integration of Data available with different agencies has raised new concerns of security and ownership. Copyright violation during authorization of and access of data is much more than normal data. Digital watermarking scheme is a topic of significant research concentration [1-3] in this concern. Watermarking based on bit model based

guarantees the authorized ownership of the image. Digital Image Watermarking schemes can be broadly categorized into two classes: spatial domain [4-61 and frequency domain [7-10]. In spatial domain techniques, watermark is hide into the LSBs (Least Significant Bit) of the host image. These schemes are generally fragile which means they cannot withstand general image processing attacks like lossy compression, filtering and scanning. Still, the watermark can easily be extracted. The frequency based methods have a number of types of transforms like Discrete Wavelet Transform (DWT), Contourlet Transform, Slantlet Transform, Discrete Cosine Transform (DCT) and so on. DCT [7-8] and DWT [9, 10, 14] based watermarking techniques are widely studied and used in literature. In DCT and wavelet based techniques the watermark is comparatively more robust. Also, they are often superior than the spatial domain techniques in robustness against general image processing exercises such as sharpening, noise distortion, cropping, compression, and so on. In recent times, N. P. Sheppard et. al. [11] and R. Barnett [15] raised a key concern of lawful possession of digital images. A counterfeit watermarking algorithm to permit several claims of lawful ownerships was presented by them. They proposed that to stay away from counterfeit attack, a non-invertible and non quasi-invertible watermarking method should be used by the owner and watermark should be a stream of bit from the host image generated by a one-way hash function. O.G. Guleryuz [11-16] presented a blind watermarking algorithm which does not require host images for extraction and can be used for determining legitimate ownerships of digital images. They declared that some significant signature should be used to generate watermark stream through one way hash function. Based on [21 - 24], a watermarking technique has been presented here which inserts significant information in a cover image. The watermark is encrypted with the help of block cipher algorithm RC6 with a secret key engendered from the hash value of the image.

2. ENCRYPTION OF THE WATERMARK

Security of multimedia data will be ensured by applying hash function. It is described as process given below:

1. Encrypt watermark logo by the process given in fig. 01 and get matrix (new) of LL.
2. Arrange LL matrix in a sequence of BBi, 0<i< N-1, where length N is equal to 2048.
3. Every image can produce fixed length hash value with condition that it is impossible to do H(a) of image for all hash values.
4. Hash value record the image will become key value.

According to SHA [19], this is a secure hash algorithm which processes the input information of 512 bits and provides output information of 160 bits which is then accumulated in five 32-bits. Suppose that a hash function H is applied onthe cover image for calculating D = H(I). Suppose CCA is a latest block

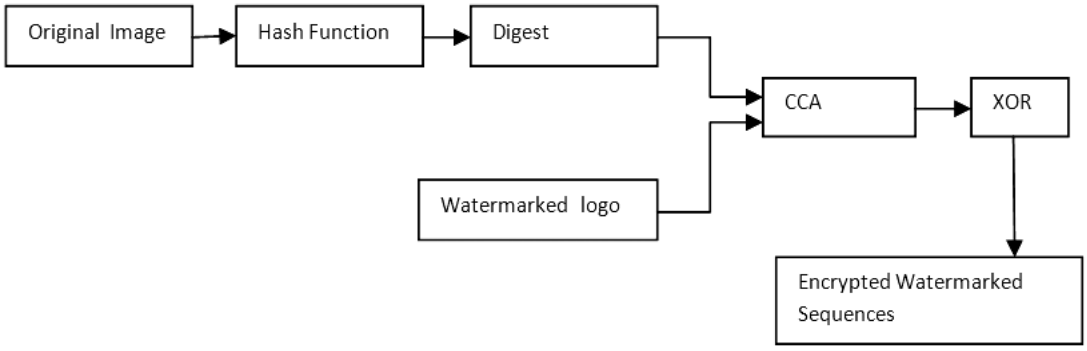


Figure 1: Encryption of Watermark

cipher. Digest D is used as a secret key for the block cipher CCA for generating a random binary sequence for encryption of the watermark W, the, which can be arranged as a mask B where B = CCA (W, D). To generate the random sequence for generation of the encrypted watermark sequence, XOR (Exclusive OR) function of the B and W is used.

3. PROPOSED ALGORITHM FOR WATERMARK EMBEDDING

In image processing the DWT (Discrete Wavelet Transform) [13, 17] has been extensively used. In wavelet transform, H and L symbolize the high pass filter and low pass filter, correspondingly. Each row is first transform by high pass and then each column with the low pass. The cover image is divided into four bans on application of DWT namely, LL, LH, HL and HH. This process can be repeated for all bands one by one. Fig 2, illustrate the 3 – level wavelet transform. We consider 3 – level wavelet transform and we will try to find out first N significant wavelet transform. At last we will embed the sequence with algorithm given below –

1. Decompose an image into sub bands.
2. Thresh hold value TT_i, 1<= i <= 5, is applicable for each sub band.
3. Considering the recent threshold TT_i examine all coefficients C_i (x, y) and select C_i (x, y)>TT_i to be significant.

   TT_i = 0.5 *max {C_i(x,y) ,

   1 <= x <= 64 * 2^{j-1}, 1 <= y <= 64 * 2^{j-1}, 1 <= I <=7, 1<=j<=3}.
4. Calculate in total the significant coefficients computed in Step 3 . If this count is less than the number N, modify Ti as:

   T_i =T*0.5, 1<= I <= 7.
5. Reiterate steps 3 and 4 till N. The considered coefficients are arranged in sequence of C_1, $C_{2, ...}$, C_n.
6. Watermark W is embedded for the considered coefficients as follows:

   $C = C_i (1 - W^{\alpha})$, if $W_i = 0$;

   $C = C_i (1 + W^{\alpha})$, if $W_i = 1$;
7. To reconstruct the watermarked image, the 3-level IDWT (Inverse Discrete Wavelet Transform) is used where á is a scaling factor and 1<= I<= N-1.

There are two methods to test existence of watermark in the image. First, by using visual assessment and the second, by using statistical examination using function NCC (Normalized Correlation Coefficient). Let C_i is the wavelet coefficient of the host image and C_i* is the wavelet coefficient of the modified image. The formula for extraction of watermark from modified image is:

$$W_{i+1}^{*} = (C_{i+1}^{*} - C_{i+1}) / \alpha + 1$$

If

$$W_i^{*} < 0,\ C_i^{*} < 0;\ \text{otherwise } W_i^{*} > 0,\ C_i^{*} = 1$$

where 1 < i < N-1. NCC is the parameter employed to determine the resemblance between the embedded watermark and the retrieved watermark.

The extracted watermark has high resemblance with the original watermark if MN is a large and

$$MN = \sum_{i=0}^{i=n-1} \left(W_i^*\right)\left(W_i\right) / \sqrt{\sum_{i=1}^{i=n-1} \left(W_i^*\right)^2 \sum_{i=1}^{i=n-1} \left(W_i\right)^2}$$

Where 0 <= i <= N-2;

A hash function is applied on the original to create the digest of an image, in order to examine the extracted watermark visually. To encrypt the original watermark sequence, the digest is utilized as the secret key for the block cipher to produce the mask B**.** It can be checked that whether the extracted watermark is a significant information or not by calculating the logic XOR between B and W*.

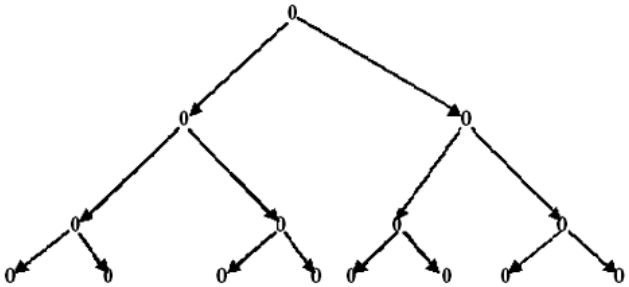


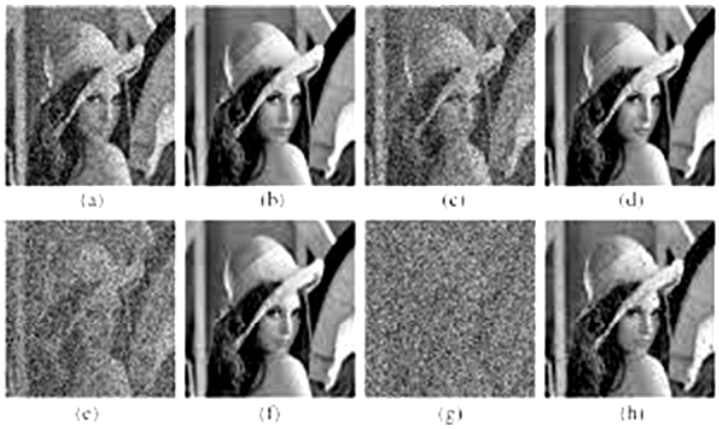
Figure2 : (a) Hierarchical wavelet tree

4. SIMULATION RESULTS

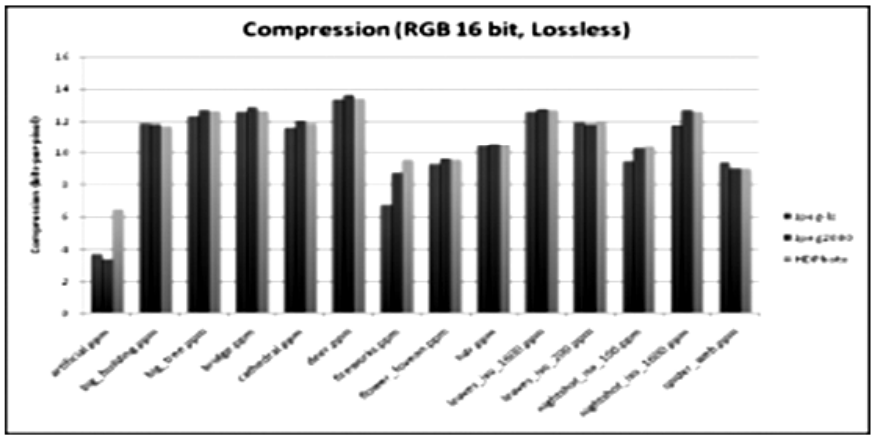
Image LL, a binary 64x64 image, has been used as the watermark. PSNR is used to measure the similarity between the cover image and the watermarked image. Figure 3 shows the original image, watermarked

(a) **(b)** **(c)**

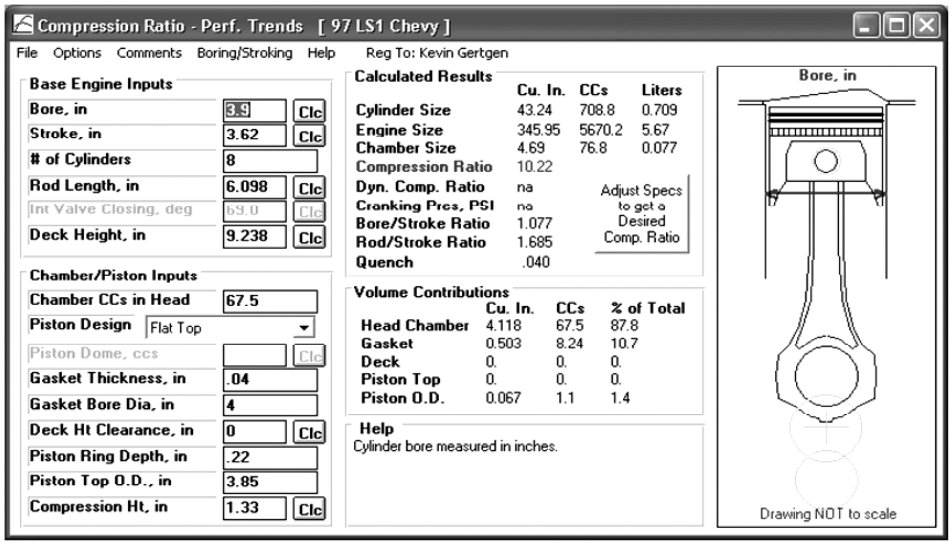
Figure 3: (a) Original image (Lena) (b) Watermarked image, PSNR = 33.72 db (c) Extracted watermark, NCC=0.8441

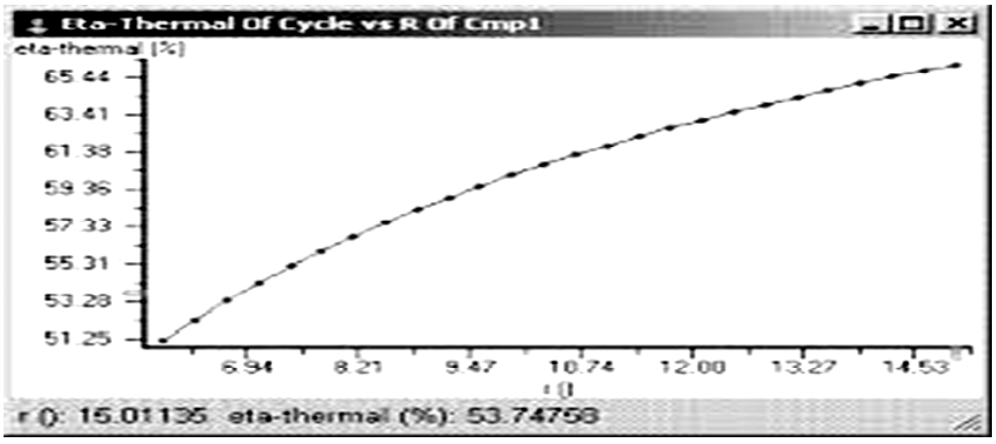


(a)



(b)





(c)

Figure 4: (a) distorted version by uniform noise; the noise are 15%, 20%, 25%, 30% and 35% (b) The jpeg compression factor is 40, 50, 60, 70 and 80. (c) The compression ratio are 6:1, 12:1, 18:1, 26: l and 32: l

image and the extracted watermark. They are visually of the same kind to the original images as the PSNR of the watermarked image is fairly high. Figure 4 shows the extracted watermarks and the NCC (Normalized Correlation Coefficients) when a number of attacks are applied to image Lena. From fig. 3 and fig. 4, it is evident that the proposed method can be utilized to extract the important information from the watermarked image with high NCC (Normalized Correlation Coefficients) even under a range of attacks.

5. CONCLUSIONS

In this paper, an algorithm with robust features has been proposed and it is applicable for JPEG compressed data in the cloud and other areas. Although noise level of the compressed data in cloud is much more in comparison to the normal data available but with this algorithm it's very easy to watermark image or logo and protect the copyright of the system. The main purpose of the algorithm is to save and identify the rights of the digital images by visual inspection and statistical detection. Proposed technique has been tested on various parameters and has shown successful results in terms of efficiency. Experimental observations reveal that the proposed watermarking algorithm shows robustness and is secure for image authentication in cloud images.

REFERENCES

[1] A.L.Jeeva1, V. Palanisamy and K. Kanagaram, "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun, 3033-3037, 2012

[2] C. Shannon, "Communication Theory of Secrecy Systems," Bell Systems Technical Journal, 28, 656-715, 1949.

[3] D.R. Stinson, Cryptography Theory and Practice, CRC Press, Boca Raton, 1995.

[4] F. Hartung, M. Kutter, "Multimedia Watermarking Techniques," Proceedings of the IEEE, 87(7), 1079-1107, July 1999.

[5] Ferguson, N., Schneier, B., and Kohno T., "Cryptography Engineering: Design Principles and Practical Applications". New York: John Wiley and Sons (2010).

[6] G. Coluccia and E. Magli, "A novel progressive image scanning and reconstruction scheme based on compressed sensing and linear prediction," in IEEE Int. Conf. Multimedia Expo 2012, Melbourne, Australia, Jul., 866–871, 2012.

[7] G. Jiang, M. Yu, S. Shi, X. Liu, and Y. D. Kim, "New Blind Image Watermarking in DCT Domain" In Proceedings of the 6th International Conference on Signal Processing, volume 2, 1580 – 1583, Aug 2002.

[8] H. Cheng and X. Li, "Partial encryption of compressed images and video," IEEE Trans. on Signal Processing, vol. 48(8), 2439–2451, Aug. 2000.

[9] Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, Vol 1, Issue 2, December, 6-12, 2011.

[10] M. D. Swanson, B. Zhy A.H. Tewfik, "Multiresolution Scene-Based Video Watermarking Using Perceptual Models" IEEE Journal on Selected Areas in Comm., Vol.16, Issue 4,1108- 1126, May 1998.

[11] N. P. Sheppard, R. S. Naini, and P. Ogunbona, "On Multiple Watermarking" In Proceedings of the ACM Multimedia workshops on multimedia and security: new challenges, 3–6, 2001.

[12] O.G. Guleryuz, "Nonlinear approximation based image recovery using adaptive sparse reconstructions," Proc. IEEE Int. Conf. Image Processing, vol. 1, 14–17, Sept. 2003.

[13] P. Jessop, "The Business Case for Audio Watermarking," IEEE International Conference on Acoustics, Speech, and Signal Processing, 2077-2074, 1999.

[14] R. B. Wolfgang, C. I. Podlchuk and E. J. Delp, "Perceptual watermarks for digital images and video." Proceedings of the IEEE, Vol. 87, No. 7, July, 1999.

[15] R. Barnett, "Digital Watermarking: Applications, Techniques, and Challenges," Electronics and Communication Engineering Journal, 11(4), 173-183, August 1999.

[16] S. Soni, H. Agrawal, M. Sharma, "Analysis and comparison between AES and DES Cryptographic Algorithm", International Journal of Engineering and Innovative Technology, Vol 2, Issue 6, December, 362-365, 2012.

[17] Y. T. Pai, S. J. Ruan, and J. G¨otze, "Energy-Efficient Watermark Algorithm Based on Pairing Mechanism" In Lecture Notes in Computer Science (LNCS), KES (1), 1219–1225, 2005.

[18] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," IEEE Trans. Multimedia, vol. 5(1), 118–129, March 2003.

[19] W. Stallings, "Cryptography and network security: principles and practice, 2nd Edition." Prentice Hall, 1999.

[20] Z.M. Lu, D. G. Xu, and S. H. Sun, "Multipurpose Image Watermarking Algorithm based on Multistage Vector Quantization" IEEE Transactions on Image Processing, 14(6): 822–831, June 2005.

[21] Ritu Gupta, Sarika Jain, "A Review on Watermarking Techniques for Compressed Encrypted Images", in International IEEE Conference MEDCOM 2014 on 7-8th November,2014 at G.L.Bajaj Institute of Technology, Greater Noida.

[22] Ritu Gupta, Sarika Jain, Anurag Mishra, "Watermarking System for Encrypted Images at Cloud to check reliability of Images" in IEEE Conference in NGCT-2015, 4-5 September, 2015, UPES, Dehradun.

[23] Abhilasha Singh, Malay Kishore Dutta, "Wavelet Based Reversible Watermarking System for Integrity Control and Authentication in Tele-Ophthalmological Applications", Int. J. of Electronic Security and Digital Forensics, Vol.8, No.4, pp.392 – 411, 2016

[24] Abhilasha Singh, Malay Kishore Dutta, Jiri Pirinosil, Kamil Riha, "Wavelet based robust watermarking scheme for copyright enforcement and integrity control in tele-ophthalmology", 8th International Conference on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT),pp. 408-413, 2016