International Journal of Engineering & Technology, 7 (4.6) (2018) 39-41

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A lightweight buyer-seller watermarking protocol based on time-stamping and composite signal representation

Ashwani Kumar[1]*, Paras Jain[2], Jabir Ali[3], Shrawan Kumar[4] G. John Samuel Babu[5]

[1]*Department of Computer Science & Engineering Vardhaman College of Engineering Shamshabad, Hyderabad, Telangana, India*
[2]*Department of Computer Science & Engineering, Sree Chaitanya Institute of Technological Sciences, Karim Nagar, Telangana, India*
[3]*Department of Computer Science & Engineering, Jaypee University of information & Technology, Waknaghat, Solan, H.P, India*
[4]*Department of Computer Science & Engineering Vardhaman College of Engineering Shamshabad, Hyderabad, Telangana, India*
[5]*Department of Computer Science and Engineering MLR Institute of Technology, Hyderabad*
**Corresponding author E-mail: ashwani.kumarcse@vardhaman.org*

Abstract

The protocol allows a content provider to detect duplicate copy of a digital content and restrict the content provider who blames the innocent customer. This paper, proposed a lightweight protocol, which uses composite signal representation and time-stamping for watermark embedding and extraction. We have used timestamp, which tells at what time the digital content was created, signed or verified to digital watermarking algorithms and uses the composite signal representation for minimizing the overhead and bandwidth due to the use of composite signals. The suggested protocol uses composite signal representations and timestamp based methods with digital watermarking scheme for content authentication. Our watermark embedding and detection algorithm achieves a balance between robustness and image visual quality. Simulation results demonstrate that the algorithm used by proposed protocol has an increase robustness and good quality of watermark images as well and withstand against various image-processing attacks.

Keywords: *Linear operation; encrypted signal; composite signal representation; time-stamp; public key cryptosystem;*

1. Introduction

Increase growth of internet requires a digital copyright-based method to control the flow of multimedia data over internet. Digital watermarking [1-2] is an effective method to protect the rights for the participant involving in e-commerce. These concepts are used by different watermarking scheme for protecting the intellectual property law and digital right for audios, pictures, and other multimedia content [3]. Time stamp based methods [4-5] are used to identify on which time a certain digital content was created, signed or verified. However, digital content can very easily reproduce by the owner of the digital content because he knows where the exact watermark bits are embedded into the cover media. Time stamp based scheme is used to protect copyright with the help of time stamp.

Our protocol allows the content provider to insert the watermarked bits along with key. The content provider uses a WCA that is trusted third party that issues a valid signature contain the credentials of content provider and uses a time-stamp i.e. at what time the digital content was created, signed or verified.

The remainder of this paper is structured as follows. In the Section 2, we have shown related work. Section 3 represents the various requirements for the protocol. Section 4 elaborates our proposed scheme. In section 5 we have shown the security analysis. Section 6 shows result analysis. Section 7 represents conclusion of our research paper.

2. Related Work

In this section, we have shown the related work of this field. There are many digital watermarking protocols proposed in history, they uses cryptography techniques for embedding and extracting watermark. The digital watermarking scheme focuses to improve the robustness of the watermark and imperceptibility of the watermarked image and it reduces the complexity of the underlying scheme.

Haber and Stornetta [6] proposed a time-stamp based protocol with watermark certificate authority.

$$S = sig_{TSS}(n, t_n, ID_n, X_n, L_n) \quad (1)$$

3. Requirements for proposed protocol

Here, we have shown the various requirements of proposed protocol.

Requirement for cryptographic operation

The BSWP [7-14] should solve the problems, which exist in traditional protocol.

Image processing requirements

In general, a good watermarking [7,10] system should contain kerckhoffs principle, robustness, imperceptibility and effectiveness.

Composite signal representation

Signal representation is a technique, which enables us to increase the speed of linear operations on encrypted domain. Due to the nature of composite signal representation, the size of the encrypted signals can be reduced as well.

Time-Stamping technique

Time-stamping [5] based methods are applicable to identify when a digital signature was created, signed or verified.

4. Proposed Lightweight Buyer-Seller Watermarking Protocol(BSWP) Based On Time-Stamping And Composite Signal Representation

In this section, we propose a lightweight protocol for secure distribution of digital content. We proposed a hybrid and efficient watermark embedding technique for encryption. The scheme is based on a public key cryptosystem, judge, trusted third party, and time-stamping services. We have used tamper resistance device and time-stamp to make our approach better for enhancing the security to the buyer and seller. Tamper resistance device is used to reduce the overhead on WCA and time-stamp are used keep the records of transaction done by customer and content provider. Figure 1 shows the proposed protocol.

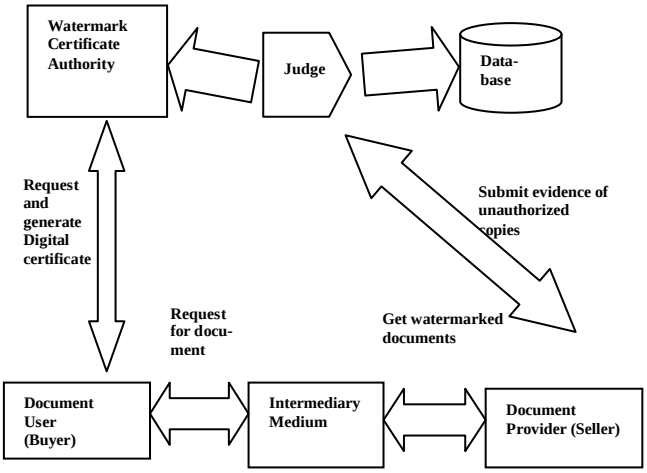

Fig. 1: Proposed lightweight protocol

Our proposed protocol consists two sub-protocols, i.e. registration protocol and watermark insertion and detection protocol. Here, we have used time-stamp based public key cryptosystem and has five different roles i.e. buyer, seller, watermarking certificate authority, judge and intermediary.

4.1 Registration protocol

This protocol is executed between the buyer and certificate authority. The customer randomly selects a pair of key, if a customer wants to hide his identity then this protocol can be skipped.

4.2 Watermark generation and extraction protocol

This protocol uses secure and robust digital watermarking scheme to generate and extract the watermark. We have used wavelets and principal component analysis methods for doing this.

5. Security Analysis

Underlying security of the protocol relays on the watermarking embedding and detecting scheme and cryptosystem, which we have used for secure communication between buyer and seller. Table 1 shows the security of the proposed protocol is examined and compared with previously published work [14] [3] [2] and [6]. Table 1 shows encryption, decryption, homomorphism and signing operation used by cryptosystem which we have used in proposed protocols.

Table 1. Comparison of Computation Cost with Existing Protocol.

	[14]	[3]	[2]	[6]	[Our]
Encryption operation	3	2k+1	2	3	1
Decryption operation	1	4	1	1	1
$\oplus$ operation	2	2	2	2	2
Signing Operation	1	k	2	2	1

In the above table k is the number of watermarks. The proposed protocol solves all the problems which exist in previously published buyer-seller watermarking protocol. Anonymity is resolved because we have used registration protocol, which contains credentials of all buyers. Unbinding problem is solved because underlying time-stamp and composite signal representation based method give the purchase information and there is one time interaction between buyer and seller.

6. Result Analysis

In this section, we have given the result analysis of our proposed protocol. In history, the traditional proposed protocol uses Cox method to gain robustness and imperceptibility. In our approach we have used wavelet coefficient and PCA based methods with time-stamp to achieve robustness. Here, we have taken Cameraman, Barbara, Lena and Man test images for showing the result. In figure 2 we have represented the original images and watermarked images. In figure 3 we have shown the various watermark logos which are embedded into the original images. We have chosen watermark logos i.e. JNU logo and copyright logo for embedding into the cover media. We have used PSNR and NCC parameters for analyzing the quality of watermarked images. The presented method is implemented in MATLAB 10.

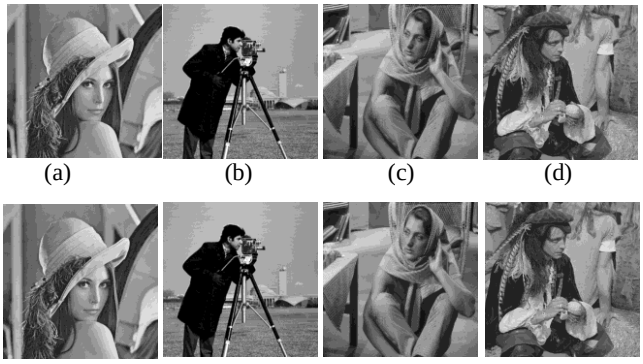

Fig. 2. Original images (a-d) watermarked images (e-h).

Fig. 3. Watermark images (i-l).

For calculating the performance of the proposed scheme, we have applied various types of noises to the watermarked images. In figure 4, we have shown the various extracted watermarks. For an instant, we only take Lena and Barbara image for producing the result. Our scheme performs well when tested against various

types of attacks the value of PSNR and NCC are given in table 2 respectively.

Table 2. PSNR values and Normalized correlation coefficient of all watermarked images and extracted logos after attacks.

Images	**Lena**		**Cameraman**	
Attacks	**PSNR**	**NC**	**PSNR**	**NC**
Gaussian Noise	40.59	0.8463	39.25	0.8131
Salt & pepper Noise	39.63	0.6338	35.10	0.5321
Speckle Noise	39.72	0.7842	37.61	0.6541
Median Filter	41.01	0.9762	40.49	0.9153

7. Conclusion

We proposed a lightweight protocol based on composite signal representation and time-stamping for multimedia data distribution. In addition, we make use of a time-stamp based techniques, which is used to store the information about time at which the digital content or signal was created, signed or verified. Our proposed protocol uses digital watermarking algorithms with composite signal based methods for minimizing the overhead. Our protocol uses a robust watermark embedding and extracting schemes this lead to higher demand for multimedia data like images with high visual quality. These aspects make our proposed protocol really secure, feasible and efficient.

References

[1] F. Mintzer., G. W. Braudaway.: If one watermark is good, are more better?, in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '99), 4, pp. 2067–2069, (1999).

[2] P. W. Wong., N. Memon.: Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Transactions on Image Processing, 10 (2001).

[3] C.-L Lei., P.-L.Yu., P.-L.Tsai., M.-H. Chan.: An efficient and anonymous buyer–seller watermarking protocol, IEEE Trans. Image Process, 13 pp. 1618–1626, (2004).

[4] A. Buldas., P. Laud., H. Lipmaa., J. Villemson.: Time-stamping with binary linking schemes, in: Advances in Cryptology—CRYPTO98, pp. 486–501, (1998).

[5] M.S. Hwang., K.F. Hwang., C.C. Chang.: A time-stamping protocol for digital watermarking. Appl Math Comput 169 pp. 1276–1284, (2005).

[6] S. Haber., W.S. Stornetta.: How to time-stamping, Journal of Cryptology 3 pp. 99–111, (1991).

[7] A. Kumar., M.D. Ansari., J. Ali., K. Kumar.: A New Buyer-Seller Watermarking Protocol with Discrete Cosine Transform. In: Das, V.V., Stephen, J., Chaba, Y. (eds.) CNC (2011).

[8] A. Kumar., V. Tyagi., M.D. Ansari., and K., Kumar.: A Practical Buyer-Seller Watermarking Protocol based on Discrete Wavelet Transform. International Journal of Computer Applications, 21(8), pp. 46-51. (2011).

[9] A. Kumar., S.P. Ghrera., V. Tyagi.: Implementation of wavelet based modified buyer-seller watermarking protocol (BSWP), WSEAS Trans. Signal Process., 10 pp. 212-220, (2014).

[10] P. Zeng., Z. Cao., K.R Choo.: An ID-based digital watermarking protocol for copyright protection. Computers and Electrical Engineering 37 pp. 526–531, (2011).

[11] Kumar, A., Ghrera, S. P., & Tyagi, V. (2015). Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis. Indian Journal of Science and Technology, 8(35), 1-9.

[12] Kumar, Ashwani, Ghrera, S.P., Vipin Tyagi, 2015. A new and efficient buyer-seller digital Watermarking protocol using identity based technique for copyright protection, Third International Conference on Image Information Processing (ICIIP), IEEE.

[13] Kumar A, Ghrera S, Tyagi V. A comparison of buyer-seller watermarking protocol (BSWP) based on discrete cosine transform (DCT) and discrete wavelet transform (DWT). Emerging ICT For Bridging The Future-Proceedings of The 49th Annual Convention Of The Computer Society Of India (CSI) Volume 1: Springer. 2015; 401–408.

[14] Ashwani Kumar, S.P Ghrera, and Vipin Tyagi, An ID-based Secure and Flexible Buyer-seller Watermarking Protocol for Copyright Protection, Science & Technology, Pertanika J. Sci. & Technol. Vol. 25, no. 1, pp. 57 – 76, January 2017.