Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 63 (2013) 18676-18678

ISSN: 2229-712X

A Novel Approach for Resolving Watermark Disputes through Watermark Authentication Server

Himanshu Agarwal* and Rakesh Ahuja

Department of Computer Science & Information Technology, Moradabad Institute of Technology, Moradabad-244001, Uttar Pradesh, India.

ARTICLE INFO

Article history:

Received: 3 September 2013;

Received in revised form:

2 October 2013;

Accepted: 21 October 2013;

Keywords

Watermark authentication server,

Ownership-Life,

Shared secret key.

ABSTRACT

Due to the rapid development of internet, perfect copy and illegal use of digital data becomes easy, which enforces the newer mechanism to provide means of protecting all forms of digital data. The purpose of this paper is to propose a novel approach of protecting the ownership rights and resolving the dispute of unauthorized addition of second watermark on already watermarked data by the use of watermark authentication server (WAS). Watermark authentication server serves as a trusted third party and solves the problem of deadlock in watermarking.

Introduction

Ownership protection is one of the basic goals of digital watermarking. The strategy of ownership protection consisting of embedding of some special pattern called metadata or watermark, which identifying the owner in the digital data. If an illegal copy is found the owner prove its paternity and can sue in the court [1]. A number of watermarking strategies [2-6] has been found in literature for protecting the ownership. The main focuses of these schemes are generally the gain of robustness and perceptibility using the pioneer algorithms [7]. In some extent these algorithms seem to be successful but no one algorithm/strategy can completely claims to protect the ownership. For example, what happens when an attackers adds a second watermark in the digital data. Simple scenario becomes complicated here as both the owner and the attacker prove their paternity in the court which simply defeats the purpose of embedding the watermark. In order to ensure the ownership by the original owner a trusted third party called a watermark authentication server is proposed in this paper.

The rest of the paper is organized as follows: In section two we briefly introduce the concept of authentication server and public key encryption techniques for understanding our approach. In section three we presents the propose WAS watermarking approach. The conclusions and future work of our propose approach are stated in section four.

Preliminaries

Since the details of authentication server and public key encryption are found in Refs. [8] and [9], this paper gives only a brief overview as below.

Authentication Server

An authentication server is a specialized database that stores the credentials of the user and grouped this information in a rigid manner. The basic structure of AS is shown in figure. 1. Each user initially registers itself on the AS, so that whenever a user approaches to the server, it matches the user with the help of information already stored in the database. The main task of AS is to verify the identity of the user that whether the user is actually who that it declares itself to be.

Nomenclature	
WAS	Watermark Authentication Server
AS	Authentication Server
^{Sh}E	Shared secret key between WAS's
$^{WAS}E_U$	Public key of WAS
$^{WAS}E_R$	Private key of WAS
$^{Us}E_U$	User public key
ID_{WAS}	Identity of WAS
TS	Timestamp

AS plays a vital role in public and private computer networks by providing authentication with the help of stored knowledge generally in the form of passwords.

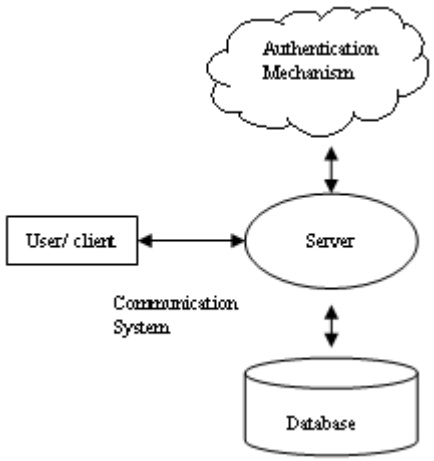

Figure. 1. Basic Structure of Authentication Server

Since credential based system have inherent weakness as they are forgotten or stolen, therefore digital certificates issued by some certificate authority in combination with credentials becomes a standard way to perform authentication

Public key encryption

A cryptographic system that require two separate but mathematically linked keys for encryption and decryption

Tele:

E-mail addresses: himanshu.agg2000@gmail.com

purpose is known as public key cryptography. Out of the two keys, one is secret (must not revealed to anyone) and only known to the owner itself is known as private key, another one which is available (published) to public is known as public keys. One key is used to encrypt the plain text into cipher text and another decrypt the cipher into plain text. Neither key can perform both functions by itself. The structure of public key encryption is shown in figure.2.

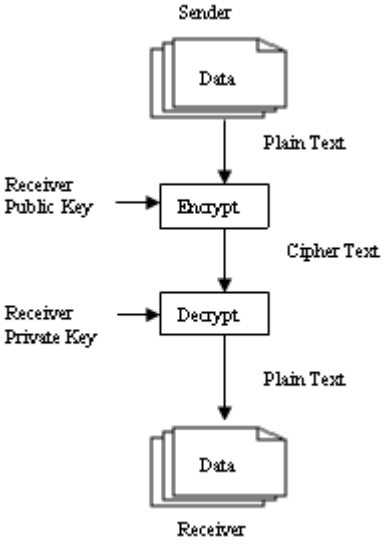

Figure. 2. Public Key Encryption Process

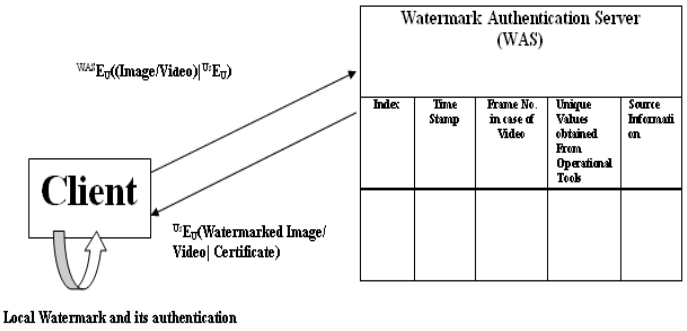

Figure. 3. Watermarking of Digital data through WAS

Watermarked data contains: $^{Sh}E(TS|\ ID_{WAS}|$ Ownership-Life)

Certificate contains: $^{WAS}E_U($ Index number $|$ TS$|$ Ownership-Life$|$ Source Info)

Proposed WAS Approach

WAS is a strong solution for resolving the disputes due to the addition of second watermark with no complexity of distributing hardware security tokens. The approach for resolving the disputes by the use of a WAS is shown in figure.3. Each client who wants to protect their ownership will send its digital data to WAS to embed watermark and ensuring its ownership in case of dispute. The WAS calculate the unique value obtained from any other popular watermark scheme of the data (in case of video a certain frames would be selected for calculation of values). The WAS then insert a Timestamp (TS), its identity (ID) and Ownership-Life by encrypt through its shared secret key between WAS's. It maintains an indexed table which stores the TS, unique value, source information and a frame number in case of video. The WAS than generate a certificate to the user containing the index number (the location address where all values about the watermarked data has been stored), TS and Ownership-Life by encrypt through its public key. The WAS than send both watermark data and certificate to the client. Any person or other WAS's can not modify the certificate, only WAS who issued the certificate can modify it, which makes the system highly secure. The client keep the certificate for the purpose of resolving the disputes if any conflict occurs.

Local watermark can be applied by the client itself for the purpose of showing its identity (visible watermark) over the data, but local watermark should restrict to apply before the certification from WAS.

TS indicating the date and time at which data is watermarked by the WAS. Ownership-Life indicating the length of time for which the watermark ownership is valid. In normal situation it includes the date and time after ten years of issuing the Timestamp.

To remove the limitation of storage at WAS's , either the maximum time of any watermarked data stores at WAS is upto 10 years because after such a long time the information contents are supposed to be obsolete in the rapidly changing world or it maximum time may set in Ownership-Life field on request. The data contents related to the national security will remain in the database of WAS for the longer time if it comes through some national security agency by modifying the Ownership-Life field.

There may be many WAS's exist around the glove and share the information between them. To minimize the communication among the servers and for the propose of limitation of the total number of WAS's, the total number of WAS may equals to the number of either the permanent members of united nations or the numbers of nations that have it marked GDP more than $ 9,00,000 millions.

Conclusions and Future work

The proposed scheme gives a fabulous way of protecting the ownership on the digital data by watermark it through watermark authentication server. This scheme takes an advantage that nobody can claim a forge watermarked data as its own because of certificate issued by WAS. Due to the shared WAS identity in watermarked data nobody can get a second watermark by any other WAS. The problem of ownership occurring due to addition of second watermark by the attacker is simply removed. A minimum amount of data has been embedded in the original digital data which improves the perceptibility of the digital contents. The only problem associated with this scheme that one more trusted third party (WAS) is involved in the process of authentication of original digital contents and the management of watermark authentication server. In summary the WAS approach provides an authentication technology which is easy to use, manage, secure and provides a cost effective solution of problem occurs due to the unauthorized addition of second watermark by some attacker.

Acknowledgements

The author would like to thank Dr. S. S Bedi, MJPR University, Bareilly (U.P) India for the careful reading of the paper and for constructive, focused comments and suggestions.

References

[1] Gwenael Doerr, Jean-Luc Dugelay, "A guide tour of video watermarking", Signal Processing Image, Communication 18(2003) 263-282.

[2] Gaurav Bhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman, "Robust gray-scale logo watermarking in wavelet domain", Computers and Electrical Engineering 3 (2012).

[3] Lama Rajab, Tahani Al-Khatib, Ali Al-Haj "Video Watermarking Algorithms Using the SVD Transform",

European Journal of Scientific Research, ISSN 1450-216X Vol.30 No.3 (2009), pp.389-401.
[4] C. Hsu, "DCT-Based Watermarking for Video," *IEEE Trans. Consumer Electronics*, vol. 44, no. 1, pp. 206-216, Jan. 1998.
[5] Dai Yuan Jun, Zhang Li He, Yang Yi Xian, "A new method of MPEG video watermarking Technology", in: Proceedings of the IEEE ICCT, Beijing, 2003, pp. 1845-1847.
[6] Himanshu Agarwal, Rakesh Ahuja, S. S. Bedi, " Highly roust and imperceptible luminance based hybrid digital video watermarking scheme for ownership protection", Int. Jour. Image , Graphics and Signal processing, 2012, 11, 47-52.
[7] S. Katzenbeisser, F. Petitcoals, "Information Hiding: Techniques for steganography and Digital Watermarking", Artech House, Norwood, MA, 1999 ISBN 1-58053-035-4.
[8] William Stallings, "Cryptography and network security", fourth edition, Pearson Prentice Hall, 2011. ISBN: 978-81-7758-774-6.
[9] G. Coulouris, J. Dollimore, T. Kindberg, "Distributed Systems: concept and design", fourth edition, Pearson Prentice Hall, 2009. ISBN: 978-81-317-1840-7.