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.

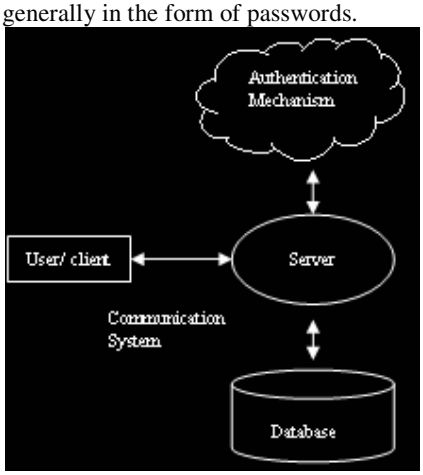


**Figure. 1. Basic Structure of Authentication Server**

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