Multicast Copyright Protection System Based on a Trusted Soft-Engine

Josep Pegueroles, Technical University of Catalonia, Spain
Marcel Fernández, Technical University of Catalonia, Spain
Francisco Rico-Novella, Technical University of Catalonia, Spain
Miguel Soriano, Technical University of Catalonia, Spain

ABSTRACT

One of the main problems that remains to be solved in pay-per-view Internet services is copyright protection. In Internet services such as near video on-demand, where multicast is used, watermarking can be directly applied. On the other hand, multicast fingerprinting has been seldom studied because delivering different marked content for different receivers seems a contradiction with multicast basics. In this paper we present a solution to prevent unauthorized redistribution of content in multicast scenarios. The system is based on a trusted soft-engine embedded in the receiver and co-managed by the content distributor. The trusted soft-engine is responsible for the client-side multicast key management functions. It only will allow the decryption and displaying of the actual data if it has previously inserted a fingerprinting mark with the identity of the decoder.

Keywords: copyright protection; multicast; multimedia distribution services

INTRODUCTION

The use of multicast is an important handicap when adding fingerprinting mechanisms to commercial content delivery over the network. In multicast communications, all the receivers get the same stream of bits. If any one of the end users illegally redistributes the content, there is no way to distinguish the pirate copy delivered by the malicious user from the original one held by honest users. So, unauthorized redistributors would be masked by the rest of the multicast group. In this sense, copyright protection for multicast arises as a challenging problem in commercial network applications.
Not many solutions that address this problem have been presented previously. Moreover, all of them present many disadvantages: incompatibility with multicast encryption schemes or reliance on the existence of trusted and programmable intermediate network nodes. These disadvantages make the current proposals infeasible to be implemented efficiently in real scenarios. In this article, we present a practical, ready-to-implement solution to the multicast fingerprinting problem.

Our scheme is based on what we call the trusted soft-engine, which is either a software or hardware tamper-proof entity embedded in the receiver at the client side. This engine has the following, particularity with respect to the actions it performs: some actions require the management of the content distributor alone; other kinds of actions will require the management of the end user alone; finally, there are some actions that require the activity of a trusted third party (TTP).

The trusted soft-engine will be responsible, on one hand, for receiving the stream of bits and decrypting it using the secure multicast group key. At the same time, it will embed a single mark to the actual data that are passed to the media player.

REQUIRED BACKGROUND

Fingerprinting Schemes

Multicast networks allow the delivery of digital goods that are not even contained in a physical support. Once the buyer has received the content, he or she is free to store it in the physical support of his or her choice. Of course, the buyer is also free to make as many (inexpensive) copies of the content as he or she wishes. This copying and storing easiness constitutes a severe threat to authorship and distribution rights.

Many experts share the opinion that e-commerce will not be a total reality until this threat to intellectual property rights can be counteracted efficiently.

Among the mechanisms used in protecting intellectual property are two groups: copy prevention mechanisms and copy detection mechanisms. The failure of copy prevention schemes, such as the DVD copy prevention system, has shifted many research efforts toward the search of feasible copy detection mechanisms.

These efforts have brought the development of new proposals of copy detection systems for many different types of digital content.

A large number of these new proposals can be grouped under the name watermarking. The watermarking technique consists of embedding a set of marks in each copy of the digital content. Since the embedded set of marks is the same for all copies, watermarking schemes ensure intellectual property protection but fail to protect distribution rights. If protection against distribution rights also is required, then the concept of watermarking needs to be extended further off.

The functionality of watermarking can be extended by allowing the embedded set of marks to be different in each copy of the object. This true original idea was introduced by Wagner (1983) and is called fingerprinting (Barg, Blakley, & Kabatiansky, 2003; Fernandez & Soriano,