International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Multimedia License Models in a Work of Art When Handling Multimedia Material

Apostolos C. Klonis*

Informatics Secondary School Teacher, M.Sc., PhD., Lefkonas Serron, Serres 62100, Greece
Email: apoklonis@gmail.com
Email: atklonis@itl.auth.gr

Abstract

In this research, the artist-audience relationship will be studied through the comparison of access control models. These models will be evaluated based on the type of work to be protected, which is artistic creation. A system for creating and interacting with multimedia environments that allow collaboration between artists and the audience is also proposed. This system approaches safety issues in multimedia environments that perform authenticity and watermark mechanisms. The authentication mechanism controls the processes of artists and audiences in multimedia files based on a set of actions required in real-world scenarios. The digital watermarking mechanism handles the protection of copyright and authenticity issues that occur in multimedia systems by applying a secure watermark.

Keywords: Distribution; material; art; watermark; multimedia.

1. Introduction

Today, the World Wide Web offers a platform for creating collaborative digital art programs, which include the use and sharing of a diverse multimedia content. Such technological platforms favor the formation of collaborative communities that focus on developing multimedia art programs.The gradual use of multimedia data on the Internet and Intranets has highlighted their potential and increased the complexity of these networks. New issues have emerged that relate to the complex structure of the data being shared. One of these problems is multimedia data permissions and access control.

---

* Corresponding author.

Unlike plain text format information, multimedia objects have various properties, such as low-level features (texture, color, shape, etc.), metadata (author name, keywords, etc.), as well as the relationships between the individual objects (temporal, semantic, spatial, etc.), which make the process of protecting the multimedia objects really difficult. In this research, the approach addressed to the field of multimedia licenses will be presented.

2. Multimedia license models

Access control and the rules by which the public decides to access a shared work of art become more complex when trying to protect non-textual multimedia objects. For example, hiding the face of a secret agent next to the president of the USA without a relevant text description remains a difficult task if current licensing models are used [8,9].

2.1 User model

The various methods and techniques used in research in various fields and by various scientific communities in order to represent user information are called User Model or User Profile. In our approach, the user model describes both the information related to the users and the application services used by the user. It is officially defined as the whole [1,3]:

$$\mathbf{UM: (id_{UM}, Cred^{*1}, Int^{*}, S_M^{*}, id_D), where:} \quad (1)$$

- IdUM: is the user ID.
- Cred: is the evidence that contains a feature of the user that is related to the application field (eg. age, occupation, studies, etc.).
- Int: describes the user's interest. It can be written as: (α1: (v1, w1) *, α2: (v2, w2) *, ...) where ai is a feature and (v1, w1) * represent all values such as ((Football, 0.5), (NBA, 0.4), etc.).
- SM: includes both a feature of the device, such as the name of the device, its operating system, its manufacturer, IP address.
- idD: is the identifier of the duration component, during which the user model has been created.

2.2 Role model

In the present research, roles are broadly defined as a work [1] function that the user can understand. So, when it comes to highly confidential multimedia applications, such a definition may not be effective enough to meet the requirements, as many other constraints should be involved and considered to maintain relative protection. We are officially writing a role, like [1,8]:

R: (Id_{ro}, name, f *, (relation, cond) *), where: (2)

• Idro: is the identifier of the role.

• name: represents the name of the role to be determined.

• *f*: is a filter function based on user model elements (eg. age> 18, occupation = agent, etc.).

• (relation, cond): represents a couple in a relationship and a situation where for any relationship a role is defined.

2.3 Rule model

One rule is the basic element of our license and the access control model. One rule is considered to be fivefold of the following form [8,9]:

(Id_{RU}, F_i*, action*, Condition*, Effect), (3)

where:

• IdRU: is the identifier of the role.

• Fi: is a characteristic object [2].

• Action: is the command given by the objects. For example, it displays an image, a video forward, a pause, and so on.

• Condition: is a condition that must be met (eg. time> 8 pm).

• Effect: is the status of the rule. It is usually described as acceptance or denial.

2.4 Policy Model

Policies are considered one of the most important issues in handling licensing standards. Several researchers have worked in this area to cover issues related to politics, their evolution, and how they should be manipulated. In our approach, a policy is seen as a set of rules assigned to a specific role. It is officially written as Policy [3,4]:

(IdP, IdRule *, status, desc), (4)

where:

• Idp: is the policy identifier.

• IdRule: is the rule identifier represented by the policy.

• status: determines the status of the policy, such as open policy or closed.

• desc: is the text description of that policy.

2.5 Connection model

In our approach, typed connections can be defined between Idu, IdR, or Idp where idu is the ID of the user model, idr is the ID of the role, and idp is the ID of the policy [5]. The values of the link can be calculated automatically based on the other node components, or given manually by the license administrator. It can be officially written as [5,8]:

$$\textbf{Link = (IdL, Type, Desc, Weight, Stnode *, EndNode *),} \quad (5)$$

where:

• IdL: is the link ID.

• Type: represents the type of connection, such as hierarchical, parental, friendly, family, similarity, etc.

• Desc: is a form of text representing the link.

• Weight: is a value in [0, 1] that describes the importance of connecting to security breaches. For example, a parent link should be more than a friendly link.

• StNode: represents the starting node that belongs to either Idu, IdR, or IdP

• EndNode: represents the end node which also belongs to either Idu, IdR, IdP.

This model allows it to represent many types of links and therefore to detect many security breaches.

3. Application Example

In the following example, consider the following scenario: Two users, u and s, are initially assigned roles officer 1 and 2. Users who have the role of officer1 must be disconnected from the Internet, while the role of officer 2 is only possible after 6:00. In addition, the officer2 role has a higher level of access and is hierarchically linked to the officer1. This hierarchical link does not involve any security breach in Figure 1. In addition, the user s assigned to officer1 has a marital relationship with the user u to whom the role 2 was assigned. The marital relationship between s and u can lead to a security breach which can be defined as follows in Figure 3. Suppose now that the licensee wishes to protect a particular agent x (Figure 2) from being seen by users assigned to role 1. So these images have no commentary and the agents being protected are not described. For this reason, the operator must specify a rule in which he specifies an image sample of the agent x he is protecting (Figure 2).

```
- <Link id="002" relation="role-role">
    <type>Hierarchical</type>
    <desc>hierachical inheritance</desc>
    <weight>0</weight>
  - <stNode>
      <roleId>1</roleId>
    </stNode>
  - <endNode>
      <roleId>2</roleId>
    </endNode>
  </Link>
```

Figure 1: Case of hierarchical link

```
<?xml version="1.0" encoding="UTF-8" ?>
- <LinkDB>
  - <Link id="001" relation="user-user">
      <type>marital</type>
      <desc>his wife</desc>
      <weight>0.5</weight>
    - <stNode>
        <userId>1</userId>
      </stNode>
    - <endNode>
        <userId>2</userId>
      </endNode>
    </Link>
```

Figure 2: Case of a linear link

Figure 3: Sample image of employee X.

4. Conclusions

Designing and developing a software system that works on the World Wide Web and is able to host and share artistic content protected and safe from malicious use is a very important issue. Its implications are many, as are the people involved in this process. Art is one of the most important achievements of mankind and every day we are surrounded by works of art. At the same time, the artistic creation is a marketable genre, which is the professional object of artists and many other professionals and companies. If we take into account how widespread the technologies of the internet have become, we will find that it is necessary to develop a technological platform accessible from the World Wide Web, open, flexible, economical in terms of consumption of computer resources but also secure and computational "Smart." So, seeing art as a digital object, its special features and its possible forms are studied and a method as well as a policy of safe sharing were developed, which were also implemented.

Acknowledgments

The authors thank teachers who give knowledge about how to read papers and write papers.

References

[1]. Béchara Al Bouna, Richard Chbeir. "Multimedia-based authorization and access control policy specification",Proceedings of the 3rd ACM workshop on Secure web services - SWS '06, 2006

[2]. Chalhoub Georges, Samir Saad, Richard Chbeir, Kokou Yétongnon, Towards Fully Functional Distributed MultiMedia DBMS, Journal Of Digital Information Management (JDIM), 2(3), September 2004:116-121.

[3]. Chbeir Richard. "Multimedia-based authorization and access control policy specification", Proceedings of the 3rd ACM workshop on Secure web services - SWS 06 SWS 06, 2006

[4]. E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. A fine-grained access control system for XML documents. ACM Transactions on Information and System Security (TISSEC), 5(2), 2002: 169 - 202.

[5]. Ferraiolo, D. F., Barkley, J. F., Kuhn, D. R., A role-based access control model and reference implementation within a corporate intranet, ACM Transactions on Information and System Security, 2(1), February 1999: 34-64.

[6]. F. Hartung, M. Kutter, “Multimedia watermarking techniques,” in Proc. IEEE Special Issue on Identification and Protection of Multimedia Information, vol. 87, no.7, pp. 1069-1107, July 1999.

[7]. C. I. Podilchuk, E. J. Delp, “Digital watermarking: algorithms and applications,”IEEE Sig. Proc. Mag., vol. 18, no. 4, pp. 33-46, July 2001.

[8]. Koukopoulos Dimitrios, Georgios D. Styliaras. "Security in collaborative multimedia art communities", Proceedings of the 2009 Euro American Conference on Telematics and Information Systems New Opportunities to increase Digital Citizenship - EATIS '09, 2009

[9]. Koukopoulos, Dimitrios K., and Georgios D. Styliaras. "Security in Collaborative Multimedia Web-based Art Projects", Journal of Multimedia, 2010.