VNU Journal of Science, Mathematics - Physics 27 (2011) 1-7

Secure delivery of multimedia data: a system model

Nguyen Tien Ban[1,*], Nguyen Linh Giang[2]

[1] *Post and Telecommunications Institute of Technology*

[2] *Hanoi University of Technology*

Received 9 December 2010

Abstract. In this paper, we propose a multimedia data delivery system model with secure solutions. This security is included both in data transmis‹ ‚on and in data protection. The approach for the former is the combination between encryption methods and content authentication. The latter is solved by using watermarking method for the characteristics of possessive person as well as data user. These characteristics are used to deal with contention in the case of copyright violation. The article also proposes the operation mechanism, the basic communication models and the experimental diagrams for the proposed system.

Keywords: multimedia data, copyright protection, secure delivery, watermarking.

1. Introduction

Due to the strong development of the Internet, the need for using multimedia data services is exponentially increasing. The applications such as online entertainment, e-learning require a delivery system of multimedia data efficiently and securely. Along with ensuring the quality of data in the delivery, the safety in delivering data and the data copyright after the delivery are also the essential issues. Therefore, the development of solutions for the secure delivery of multimedia data to ensure the requirements is necessary.

Thanks to the delivery system of multimedia data, users can utilize data in two ways: online viewing and data downloading to the computer [1]. In tl.e first one, the multimedia data are distributed to end users by real time streaming transmission method. Hence, it is not time consumption for users to wait for downloading data to the computer. However, data do not be saved on the workstations after viewing. In the remaining way, data are delivered in a conventional unit transmission method and stored in the user's workstation before the presentation.

The secure delivery system of multimedia data has to meet the following requirements:

- Guarantee for the quality of data requirements including the quality of video and audio, the synchronization as well as delay in transmission.
- Securely guarantee for the data exchange between service providers and users. This process relies on the encrypted coding infrastructure and the authentication methods.
- Guarantee for data protection against the copyright infringement as well as data usage control. This protection is based on the digital signing aıld information marking methods on data.

[*] Corresponding author. E-mail: bannt@ptit.edu.vn

In this paper, we focus on introducing the structure model and the operation of the major phases in the system. The algorithms for the protection of multimedia data ownership were discussed in [2-5]. The flows of this paper are as follows: Section 2 will present an overall system model. In section 3, we will discuss about the important transactions in system. The experimental diagram of this system will be introduced in section 4. This diagram allows the authentication capability and the basis for the settlement of contention.

2. The secure multimedia data distribution system model

In delivering multimedia data over the network, the following factors will affect the system:

- "Man in the middle attack" – data are stolen when transferring over the network.
- Data are distributed by the recipient without permission.
- The occurrence of disputes relating to the data ownership.

Therefore, the system needs to provide the following abilities to prevent the above attacks:

- The ability to provide a secure communication infrastructure.
- The ability to provide methods of marking distributed data for the ownership.
- The ability to provide methods of detecting violations customers when using distributed data.
- The ability to solve disputes arising in providing services.

The secure communication infrastructure is built based on the public key infrastructure which is capable of providing a secure communication channel and an authentication mechanism for the parties. It also enables to prevent the acts of fraud in the process of data exchange. In addition, this public key infrastructure is capable of providing digital signatures. This signature will be used as a signal that uniquely identifies a subject in the data exchange.

To mark the ownership on the distributed data, the system should provide the mechanisms for the data owners signing on data by the specific signatures. This signature may be one of the following types: the logo of the owner, the specific code string or the owner's private key. This characteristic have to be marked on the data firmly as well as not to be removed by any methods.

To detect the violations of customers in using the distributed data, the system has to provide the specific signs for customers. This sign will be used by customer for registering and by the system for marking on the distributed data. It is very useful for identifying the customer when the violations occur.

To deal with disputes when providing services, the system has the capability of fighting against the negation when disputes arise.

The secure delivery system model of multimedia data has the major parts as follows (Figure 1):

- The multimedia data providing part: management of the delivery process of multimedia data to users.
- The part of watermarking and controlling the right for data usage: implementation of watermark embedment and separation of the supplier and receiver to data.
- Multimedia data store: multimedia data management.
- The part of granting certificates and solving the violations: this part has responsible for granting certificates to the parties.
- The data receiver: user requests data.

In the model, the data providing part and multimedia data store are built in the service providing server. The part of granting certificates and solving the violations are considered as a third party that is not constructed in this system. Agents participating in the system include user, administrator and CA providing certificates and solving disputes.

With such model above, the user rights are as follows:

- Request for granting certificate.
- Signing in the system.
- Searching for data.
- Request for data: online viewing or downloading.

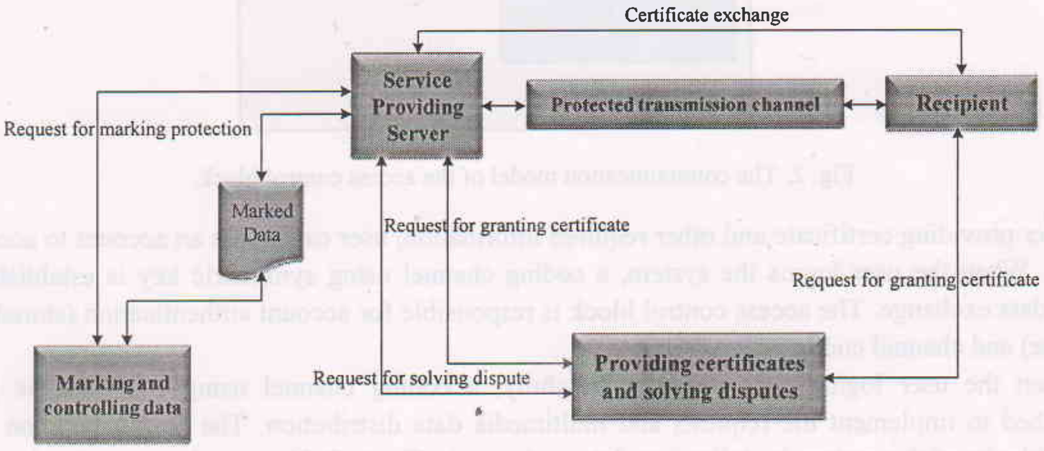
Certificate exchange
Service Providing Server
Protected transmission channel
Recipient
Request for marking protection
Marked Data
Request for granting certificate
Request for granting certificate
Marking and controlling data
Request for solving dispute
Providing certificates and solving disputes

Fig. 1. The secure delivery system model of multimedia data.

The administrator rights are as follows:

- Request for granting certificates.
- Managing multimedia data.
- Controlling the system access: the management of account information, delegation and user access.
- The management of generating, embedding and separating signs.
- The management of data transmission (in stream or block transmission).
- Sending request for the determination of data ownership to the CA in case of data violations.

CA is an external agent that is responsible for communication and data exchange with the system. CA will implement the system requirements such as:

- Issuing certificate;
- Settlement of disputes related to data ownership as required.

3. Communications among components in the system

The communication model between log-in block (belong to client) and access control block (belong to server) in the log-in phase is illustrated in Figure 2.

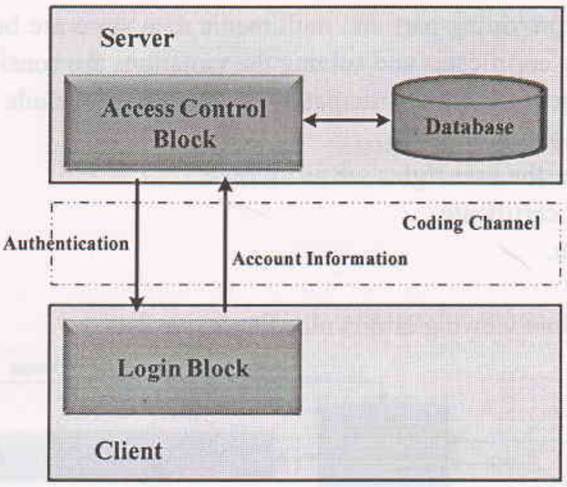

Fig. 2. The communication model of the access control block.

After providing certificate and other required information, user can create an account to access the system. When the user logins the system, a coding channel using symmetric key is established for secure data exchange. The access control block is responsible for account authentication (stored in the database) and channel coding.

When the user logins the system successfully, a coding channel using a symmetric key is established to implement the requests and multimedia data distribution. The communication model among blocks of the system in delivering data is shown in Figure 3. User send request for data to the data management block. This block will search in the database and reply to user's request. After that, the user's request will be forwarded to the marking block. This block then will embed the provider's mark and user's mark corresponding with database into the required data. The management block will deliver data to users and process the received data depending on user's request.

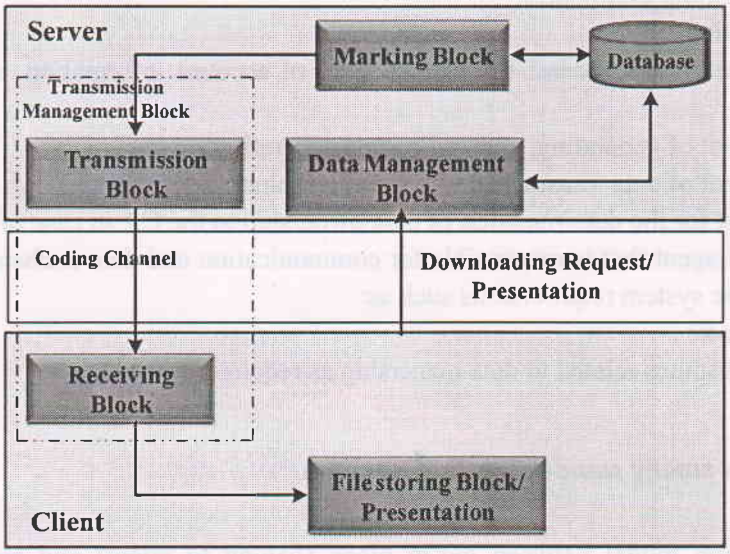

Fig. 3. The communication model among the blocks of the system during the data distribution.

The communication model of demarking block is depicted in Figure 4. Data suspected copyright infringement is transferred to the system. The demarking block then analyzes data to extract the owner's mark and violated user's mark, separately. During the analysis, the information is matched with the database as well as exchanged with CA to make a conclusion related to the violated user.

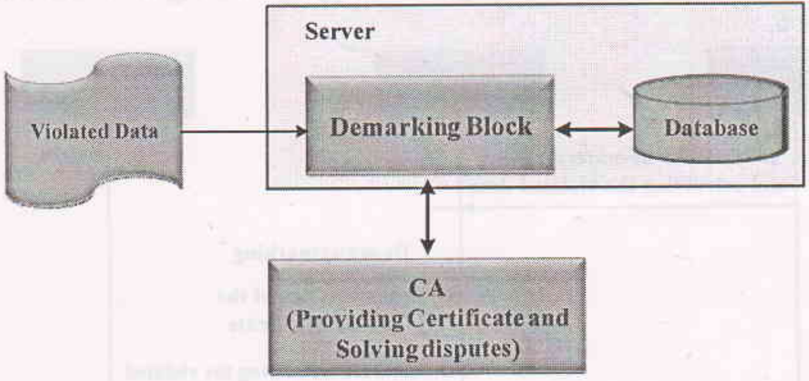

Fig. 4. The communication model of the demarking block.

4. The experimental system

The system is tested in two scenarios including the data requirement and the copyright infringement determination. The first scenario is described in Figure 5.

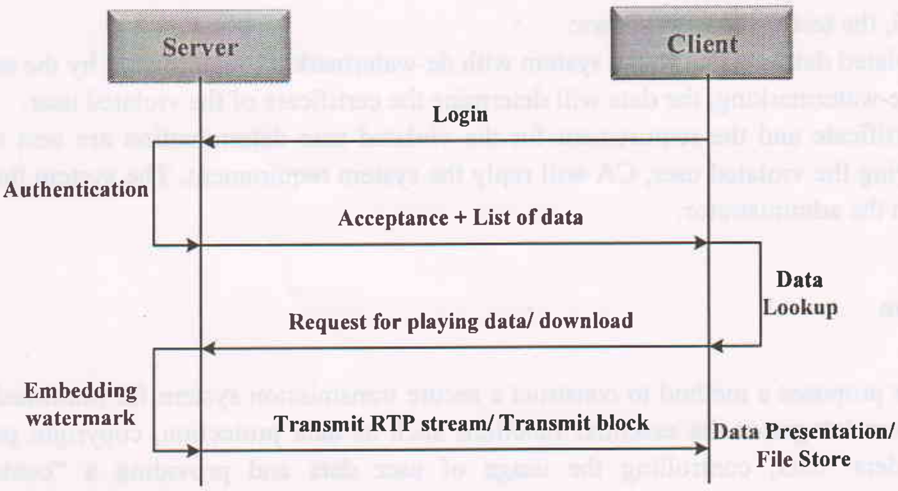
Server
Client
Login
Authentication
Acceptance + List of data
Data
Lookup
Request for playing data/ download
Embedding
watermark
Transmit RTP stream/ Transmit block
Data Presentation/
File Store

Fig 5. The experimental scenario of client's data request.

In the figure, the testing process shows:

- The system authenticates user through the client certificate and the login information.
- The workstation connects to the server, view the list of available data on the server, perform data lookup based on demand and download data.

- The server has made ownership watermarking and workstation watermarking on required data before transferring data blocks to the workstation.
- On the client side, data can be presented or received and stored the files on the hard drive.

The second experimental scenario relating to the copyright infringement determination of user is depicted in Figure 6.

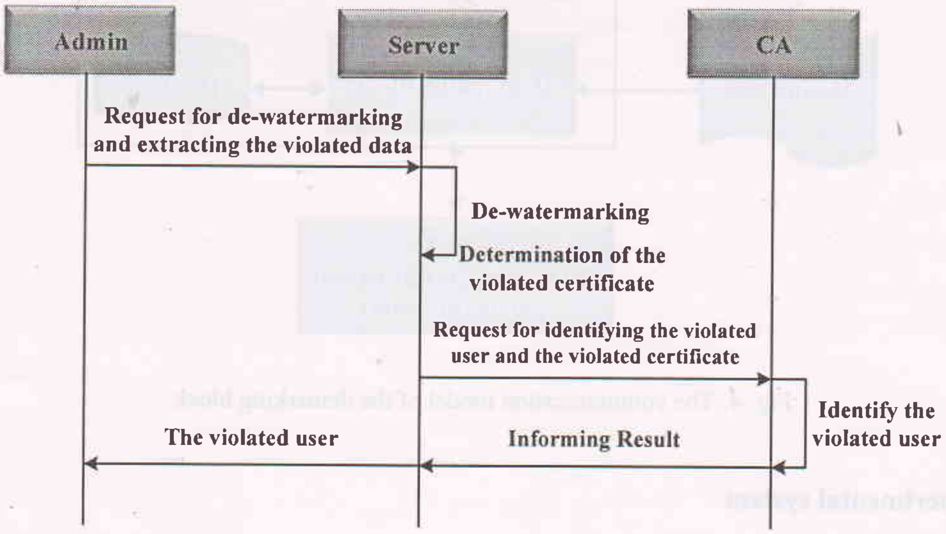
Admin
Server
CA
Request for de-watermarking and extracting the violated data
De-watermarking
Determination of the violated certificate
Request for identifying the violated user and the violated certificate
Identify the violated user
The violated user
Informing Result

Fig. 6. The experimental scenario for the determination of copyright violation of user.

In figure 6, the testing process shows:

- The violated data are sent to the system with de-watermarking requirement by the manager.
- After de-watermarking, the data will determine the certificate of the violated user.
- The certificate and the requirement for the violated user determination are sent to CA. After identifying the violated user, CA will reply the system requirement. The system then sends this result to the administrator.

5. Conclusion

This paper proposes a method to construct a secure transmission system for multimedia data. The proposed system integrates the essential functions such as data protection, copyright protection for service providers' data, controlling the usage of user data and providing a "contention free" mechanism. Besides, the system model and the functions of components are also discussed in this paper. The analyzing and making the basic communications among the blocks of the system are taken into account to ensure the data delivery securely. This system has the open structure. Therefore, the components of the system can be implemented under the specific requirements. This paper also introduces some experimental scenarios for the system. According to the received results, the proposed model can meet the requirements of the secure multimedia data transmission system through basic transactions.

References

[1] Nguyen Linh Giang, Multimedia Communications Services and E-learning Systems, *Proceedings of National Conference ICT'rda*, 2003 (in Vietnamese).

[2] Chun-Ying Huang, Yun-Peng Chiu, Kuan-Ta Chen, Hann-Huei Chiou, Chin-Laung Lei, Secure content delivery using key composition, *The IEEE Conference on Local Computer Networks, 30th Anniversary*, 2005.

[3] M.A. Qadir, I. Ahmad, Digital text watermarking: secure content delivery and data hiding in digital documents, *39th Annual International Carnahan Conference on Security Technology* (2005) 101.

[4] Qibin Sun, J. Apostolopoulos, Chang Wen Chen, Shih-Fu Chang, Quality-Optimized and Secure End-to-End Authentication for Media Delivery, *Proceedings of the IEEE*, Vol. 96 (1) (2008) 97.

[5] K. Mokhtarian, M. Hefeeda, Authentication of Scalable Video Streams With Low Communication Overhead, *IEEE Transactions on Multimedia*, Vol. 12 (7) (2010) 730.