International Journal of Security and Its Applications
Vol. 1, No. 1, July, 2007

Database Design Scheme for Copyright Protection Using Multimedia Documents Authentication

Jae-Woo LEE
Department of Computer Science & Information, Kyungbok College
it21c@korea.ac.kr

Abstract

Many multimedia documents are produced and distributed widely for many applications. And those many multimedia documents are spread fast through the Internet. But there have been illegal behaviors that many unauthorized users transform multimedia and use illegally so, legal issues for copyrighted multimedia arise as a necessary consequence. In this paper, we propose a procedure for secure watermarking using authentication key when a multimedia document is used by authorized user in the Internet or distributed information systems. Before a client requests using a multimedia document from the application server, the user acquires authentication key from the authentication server. And then the application inserts a watermark into the multimedia document comparing the client's authentication key with that of authentication server. And the authentication key is inserted into the multimedia as a digital watermark. The proposed digital watermarking algorithm can be used for inserting authentication number like serial number of the multimedia. So, the owner of the multimedia document can get copyright based on authentication server. Using the digital watermark with authentication number of a multimedia document the owner of the document can assert copyright ownership.

1. Introduction

Nowadays, information systems including the Internet have been being used in information society. Especially there is many digital multimedia documents in our life by growing information technologies. Many multimedia documents are produced and distributed widely for many applications. And those many multimedia documents are spread fast through the Internet. In this information society, they can always gain various multimedia documents easily without restriction of location. Also there have been illegal behaviors that many unauthorized users transform multimedia and use illegally so, legal issues for copyrighted multimedia arise as a necessary consequence. It is natural for creators or workers of the multimedia documents to claim exclusive ownership. So the copyright legislation guards every document whose owner puts the copyright logo on it and can prove ownership at court. In case of a dispute, the party with earlier copyright is considered to be the rightful owner. But a simple execution of the copy operation generates a new copy of the document, indistinguishable from the original. Copyright protection has become of utmost importance to companies and individuals that are selling their own multimedia documents [1].

Copyright protection of a multimedia document uses steganography and cryptography. Steganography uses various techniques of information hiding so the information is invisible to an observer like invisible ink. When a user copies and modifies a multimedia document illegally, the owner of the multimedia can prove their ownership by information hiding that the owner only knows. Cryptography scrambles the information so although visible, is unintelligible. And then even though an illegal user gains much information about multimedia documents, the stolen information and multimedia are no longer useful to the user [1, 2, 4].

A multimedia document with small noise is almost the same as the original document because of the nature of human vision and hearing, so the watermark can be inserted into an image, audio and video documents without deterioration of the quality of sound or picture. A watermark noise is first generated normally at random including by using cryptography and later incorporated into the document. Watermarks can be visible or invisible. Visible watermarks are physically displayed on the multimedia documents. Invisible watermarks are inserted into documents to trace a possible illegal use. This small watermark noise is added to a piece of the multimedia documents like music or picture. Due to limitations of our senses, those changes will not be detected. Watermarks can be classified robust or fragile. Robust watermarks should be difficult to remove by illegal users. An intentional attempt to remove watermarks from a multimedia document should lead to considerable deterioration of the quality of the multimedia documents. Fragile watermarks are very sensitive to any change and are destroyed after any attempt to interfere with the document contents. They are used to prove that the document originated from a specific source. Fragile watermarks are useful for detecting tampering with the document [1, 2].

But, in the Internet or distributed client server systems, many clients access various multimedia documents and illegal users get a multimedia document and attempt to modify as their own documents. So, it is not always secure that we use digital watermarking on our multimedia documents. In this paper, we propose a procedure for secure watermarking using authentication key when a multimedia document is used by authorized user in the Internet or distributed information systems. Before a client requests using a multimedia document from the application server, the user acquires authentication key from the authentication server. And then the application inserts a watermark into the multimedia document comparing the client's authentication key with that of authentication server. And the authentication key is inserted into the multimedia as a digital watermark. The proposed digital watermarking algorithm can be used for inserting authentication number like serial number of the multimedia. So, the owner of the multimedia document can get copyright based on authentication server.

This paper is organized as follows. In Section 2, we introduce briefly the digital watermarking and authentication. In Section 3, we define authentication procedure and propose a new procedure of digital watermarking with authentication. Finally, in conclusion we establish more secure watermarking with authentication and plan to future works.

2. Digital watermarking and authentication

2.1. Digital watermarking

Many multimedia documents are produced and distributed widely for many applications. And those many multimedia documents are spread fast through the Internet. And there have been illegal behavior that many unauthorized users transform a multimedia and use illegally so, legal issues for copyrighted multimedia arise as a necessary consequence. Copyrighted multimedia documents include a certain sign in the document. It is natural for creators or workers of the multimedia documents to claim exclusive ownership. Digital watermark is inserted into a multimedia document for copyright protection of owner.

Digital watermarking is classified various aspects. Watermarks can be visible or invisible. Visible watermarks are physically displayed on the multimedia documents. At the same time it is important for watermarks not to deteriorate the overall quality of the document. Invisible watermarks are inserted into documents to trace a possible illegal use. For example, a small

watermark noise is added to a piece of the multimedia documents like music or picture. Due to limitations of our senses, those changes will not be detected [1, 2].

Watermarks can be classified robust or fragile. Robust watermarks should be difficult to remove by illegal users. An intentional attempt to remove watermarks from a multimedia document should lead to considerable deterioration of the quality of the multimedia documents. Robust watermarks are used to assert the ownership of multimedia documents. Fragile watermarks are very sensitive to any change and are destroyed after any attempt to interfere with the document contents. They are used to prove that the document originated from a specific source. This sort of watermarks may apply cryptography and the watermark is a digital signature whose form depends on the document and the secret key of the copyright holder. Fragile watermarks are useful for detecting tampering with the document. A multimedia document with small noise is almost same as original document because of the nature of human vision and hearing, so a watermark can be inserted into an image, audio and video documents without deterioration of the quality of sound or picture. A watermark noise is first generated normally at random including by using cryptography and later incorporated into the document [1, 2, 6, 7].

2.2. Authentication and encryption

To protect our multimedia documents from using illegally many security services are needed in a network and server system. Many authorized clients wish to access on server's multimedia database system through the network in distributed database systems or Internet. And then the server systems should be able to restrict access of unauthorized users and admit authorized user's request for multimedia database services. Security service is an information technology that enhances the security of resources of computer systems. Several security services are needed to protect our network or computers for preventing these various security attacks, such as authentication, access control, confidentiality, integrity and non-repudiation. Always an authorized user may be able to gain access to services and database that they are not authorized to access. Among them we think that authentication is one of the most important security services because we protect many multimedia resources of systems using authorized client authentication in the Internet or distributed client server systems [3, 4].

Authentication service is to assuring whether a client is authentic or not, by using user's ID, password or Internet address, etc. In the Internet including distributed client server systems, a server system requires a user's ID and password for preventing unauthorized users from using resources of the server. Authentication is focus on that a multimedia document is used legally. Before a multimedia document is used or spread widely to many users, if an authentication process is performed by authentication server, copyright protection of a multimedia can be assured by the authentication server besides digital watermarking and encryption [3, 4, 5].

As above mentioned, authentication services are needed for protecting our multimedia resources of computer systems. But it is not always secure that we use various security services, because of repeated and specialized attacks by unauthorized users or hackers. So, it is very important all of messages in a network should be encrypted by protocol of sender and receiver. And then even though hackers gain many multimedia documents about our network or server systems, the stolen information or message is no useful to them. There is conventional encryption procedure in figure 1. A client creates some messages for transmission in a network, and then the message should be encrypted by encryption algorithm using secret key. So, the result of encryption is that plaintext is changed to ciphertext. And the ciphertext is transmitted to destination in network, server system on the destination decrypt

the ciphertext by decryption algorithm using secret key. After all the ciphertext is changed to original plaintext, destination node computer can read the messages. Because the messages are encrypted, the contents of the message are secure in spite of risk of stealing in a network [4, 5, 8].

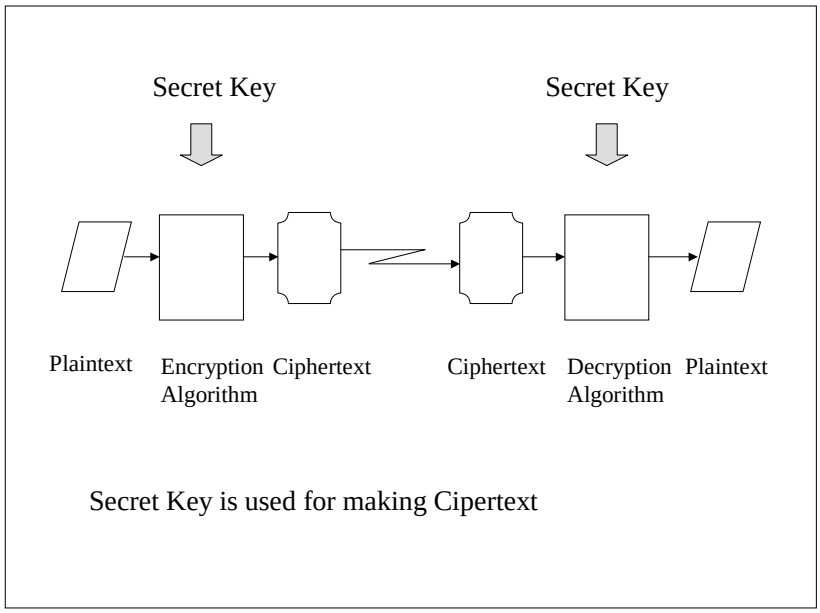

Figure 1. Conventional encryption and decryption procedure

3. A procedure for authentication and watermarking

3.1. Authorized user authentication

In section 2, we have described digital watermarking, user authentication and multimedia documents encryption. In this paper, we consider that authentication for multimedia documents is needed besides inserting digital watermark. So, we propose a procedure for secure watermarking scheme using authentication key when a multimedia document are used by authorized user in the Internet or distributed information systems.

A server system has authorized users' identifier and password in authentication database as the authentication server. So, when a request occurs for accessing the server system including multimedia database query, the server systems always examine whether the client is authorized or not to access systems before processing the transaction request. And then the server systems gain the authorized information from database for user's profile. Generally the user's profile database table has several fields, client's identifier, password and other information like IP address. The layout of user profile table is shown in table 1, ID={id_1, id_2, ..id_i, ..,id_n } is assumed as a set of client's identifier. And the client's passwords are defined set of password as PW={pw_1, pw_2, ..pw_i, .., pw_n }. When the server system selects a client's password using the client's identifier.

id_i : ith client's identifier
pw_i : ith client's password
in_i : ith client's information

Table 1. Client's profile database

Client's ID	Password	Client's Information
id_1	pw_1	in_1
id_2	pw_2	In_2
…	…	…
id_i	pw_i	in_i
…	…	…
id_n	pw_n	in_n

Before a client request for using a multimedia document, the user should acquire authentication key from authentication server. And then the authentication server create authorized serial number using a function, like randomize(). That is used for authentication key. And the client and authentication server store the authentication key in it's own authentication database. The client's requests for multimedia document are defined set of request as RQ={rq_1, rq_2, ..rq_j, .., rq_m }. And the authentication key for the client's requests are defined set of request as AU={au_1, au_2, ..au_j, .., au_m }.

rq_j : jth client's request
au_j : jth authentication key
tm_j : jth client's request time stamp

Table 2. Authentication database

Request ID	Request Time	Client's ID	Authentication Key
rq_1	tm_1	id_1	au_1
rq_2	tm_2	id_2	au_2
…	…	…	…
rq_j	tm_j	id_i	au_j
…	…	…	…
rq_m	tm_m	id_n	au_m

As shown in table 2, using the authentication database our proposed authentication procedure is as follows:

When a client request authentication key for getting a multimedia document to application server of the multimedia document,

Step 1 : Client send a message including user's identifier and password for authentication to authentication server before requests to application server.

Step 2 : Authentication server examine whether the client is authorized or not. And then authentication server create authentication key for client request using a function like a Randomize( ). Using authentication database authentication data are added to authentication database.

Step 3 : Authentication server returns authentication key to the client as the type of encrypted key.

Step 4 : Authentication server also send the authentication key to the application server for multimedia documents.

Finally the authentication key is notified to application server with multimedia documents. The proposed authentication procedure is shown in figure 2.

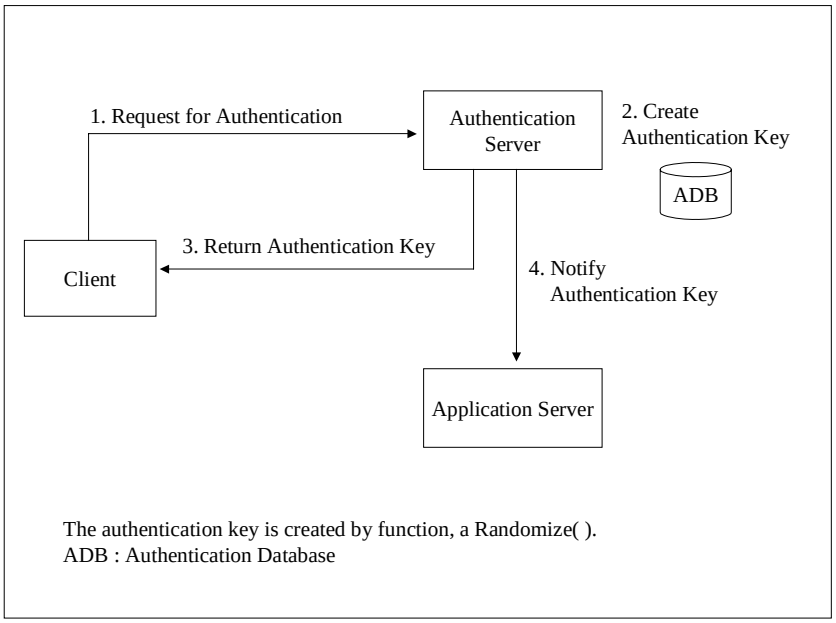

Figure 2. Client authentication procedures

3.2. Digital watermarking using the authentication key

After the client acquire authentication key from authentication server, a client requests multimedia documents that he needs using authentication key. The application server of multimedia documents compare client's authentication key with that of authentication server. And then the application server inserts a watermark into the multimedia documents that is requested by the client. The application server systems have many multimedia documents. The multimedia documents are defined set of multimedia document as MD={md_1, md_2, ..md_k, .., md_l }.

md_k : kth multimedia document requested by the client
on_k : kth multimedia document owner
ds_k : the description of the kth multimedia document

The multimedia documents list is managed by the application server systems for copyright. The layout of multimedia database can be constructed as shown in table 3.

Table 3. Multimedia documents database

Multimedia ID	Document Owner	Multimedia Description
md_1	on_1	ds_1
md_2	on_2	ds_2
…	…	…
md_k	on_k	ds_k
…	…	…
md_l	on_l	ds_1

The authentication key is inserted into the multimedia as a digital watermark. The unique digital watermark is embedded into requested multimedia document and the authentication key is used for inserting authentication number like serial number of the multimedia. So, the owner of the multimedia document can get copyright based on authentication server. As shown in figure 3, the procedure of digital watermarking uses the authentication key for copyright protection. The proposed digital watermarking procedure is summarized as follows:

During the former authentication procedure, the authentication server send the authentication key to client that request the multimedia document and also notify the authentication key to application server. And the client requests the multimedia document using the authentication key. The application server checks the request of the client.

When the client request multimedia document that he or she wants, the client send a message to application server that has the multimedia document,

Step 5 : Client send a message including user's identifier and password with the authentication key that is acquired from authentication server.

Step 6 : Application server of the multimedia document checks whether the client is authorized or not to get the multimedia document with the authentication key. And the authentication key are used for creating digital watermark.

Step 7 : The digital watermark using the authentication key is embedded into the multimedia document.

Step 8 : The multimedia document with digital watermark is sent to the client that requests the multimedia.

That is, the server send the multimedia document to client after inserts digital watermark into the multimedia document. The multimedia document with digital watermark will be copyrighted document for authorized users. The authentication key means copyrighted authentication number like serial number of the document.

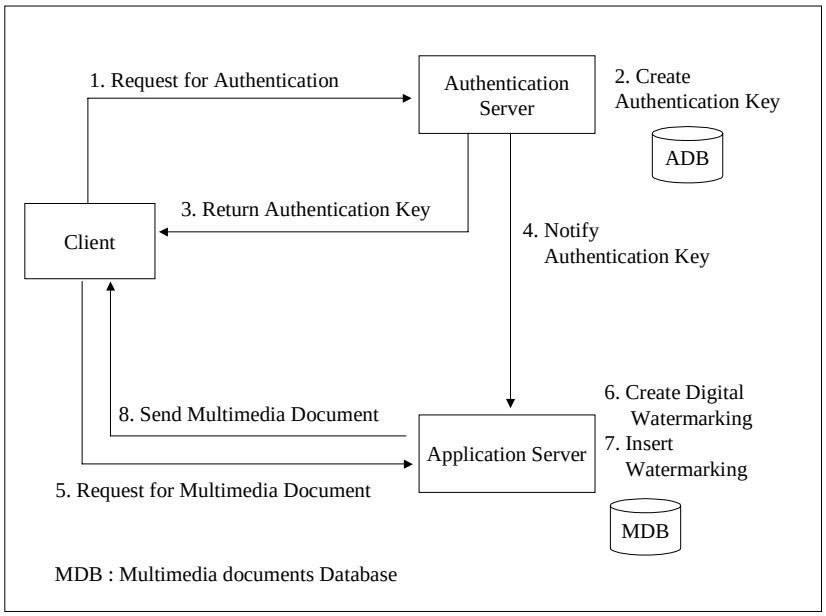

Figure 3. Authentication and digital watermarking procedure

The requested multimedia document list by the client is inserted into multimedia database for copyright. The layout of multimedia database for copyright can be constructed as shown in table 4. In this table, the requests of client for multimedia documents are managed adding authentication key from authentication server system.

Table 4. Multimedia documents database for copyright

Request ID	Client's ID	Authentication Key	Requested Multimedia
rq_1	id_1	au_1	md_1
rq_2	id_2	au_2	md_2
…	…	…	…
rq_j	id_i	au_j	md_k
…	…	…	…
rq_m	id_n	au_m	md_l

After the multimedia document with digital watermark is sent to the client that requests the multimedia documents, the application server systems add the requested list using request ID, client's ID, authentication key from authentication server systems and requested multimedia document as shown in table 4. That information of the requested multimedia document can be used for copyright protection against unauthorized users because there are digital watermark in requested multimedia documents using the authentication key from authentication server systems.

4. Conclusion

Multimedia documents can be replicated easily by a simple execution of the copy operation. In this information society, they can always gain various multimedia documents easily without restriction of location. Also there have been illegal behaviors that many unauthorized users transform a multimedia and use illegally so, legal issues for copyrighted multimedia arise as a necessary consequence. Copyright protection has become of utmost importance to companies and individuals that are selling their own multimedia documents.

We describe various digital watermarking and security services. In this paper, we propose a procedure for secure watermarking using authentication key when a multimedia document are used by authorized user in the Internet or distributed information systems. Before a client request for using a multimedia documents to an application server, the user acquire authentication key from authentication server. And then the application with the multimedia insert a watermark into the multimedia comparing the client's authentication key with that of authentication server. And the authentication key is inserted into the multimedia as a digital watermark. For this secure procedure, we design several databases such as client's profile, authentication, and multimedia documents database for copyright.

The proposed digital watermarking algorithm can be used for inserting authentication number like serial number of the multimedia. So, the owner of the multimedia document can get copyright based on authentication server. Using the digital watermark with authentication number of a multimedia document the owner of the document can assert copyright ownership.

In the future, we will further research to prevent various illegal behaviors about multimedia documents for protecting ownership of the documents. It will be very important that we define various modifying attack in detail and more secure client authentication and digital watermarking model.

5. References

[1] Syed Mahbubur Rahman, Design and Management of Multimedia Information Systems : Opportunities and Challenges, Hershey, Pa. Idea Group Publishing, 2001
[2] Syed Mahbubur Rahman, Interactive Multimedia Systems, Hershey, PA IRM Press, 2002.
[3] William Stallings, Network Security Essentials : Application and Standards, Prentice Hall, 1999.
[4] William Stallings, Cryptography and Network Security : Principles and Practice, Prentice Hall, 1999
[5] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, 1976, pp. 644-654
[6] Sung-Cheal Byun, Sang-Kwang Lee, Ahmed H. Tewfik, and Byung-Ha Ahn, "A SVD-Based Fragile Watermarking Scheme for Image Authentication," Lecture Notes in Computer Science, Vol. 2613, 2002, pp. 170-178
[7] Xiangui Kang, Jiwu Huang, and Yun Q. Shi, "An Image Watermarking Algorithm Robust to Geometric Distortion," Lecture Notes in Computer Science, Vol. 2613, 2002, pp. 212-223
[8] Ravi Sandhu and Pierangela Samarati, "Authentication, Access Control, and Audit," *ACM Computing Surveys*, Vol. 28, no. 1, pp.241-243, March 1996

Author

Jae-Woo LEE

Received a B.S. degree in statistics from Dongguk University, Korea, 1987, and M.S. degree in computer science from Seoul National University of Technology, Korea, 1997 and Ph D. degree in computer science and engineering from Korea University, Korea, 2004. In 1999 he joined the faculty of Kyungbok College, Korea where he is currently a professor in Department of Computer Science and Information. His research interests include Software Engineering, Distributed Database Systems, and Data Engineering.