DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4631

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

OBJECT ORIENTED MODELING FOR AUTHENTICATION OF CERTIFICATE IN E-LEARNING USING DIGITAL WATERMARKING

Soumendu Banerjee
Research Scholar, Department of Computer Science
The University of Burdwan
Burdwan, West Bengal, India

Sunil Karforma
Associate Professor, Department of Computer Science
The University of Burdwan
Burdwan, West Bengal, India

Abstract: As the popularity of e-learning system is increasing day by day, the question of security is also becoming a matter of concern. While the administrator sends certificate or any essential document in an e-learning system via internet or intranet, if the hacker can reach the document, can easily change or destroy it, which makes a bad impact on the corresponding e-learning institution. Through digital watermarking along with some cryptography techniques, the administrator can make this kind of transmission very secure. The advantage of object oriented modeling of any system is to reduce the maintenance cost, improve reliability and flexibility, code reusability etc. To achieve these advantages, we wrapped our proposed model in object oriented modeling utilizing the benefits of object oriented analysis and design.

Keywords: Digital watermarking, IDEA, RC4, UML diagrams

1. INTRODUCTION

E-learning is comparatively new kind of learning, which totally depends on Internet. It is information and communication based application in the field of learning. It helps to erase the distance between the learner and the institution; time saving is another reason for which e-learning is getting popularity in the present day learning scenario. E-learning is in particular very much helpful for the persons who are already engaged in job but also has desire to learn, since there is no barrier of place and time in case of e-learning[1]. Like all other kinds of learning, the components of e-learning system are administrator or developer, teachers and students or learners[2]. All the communications between these components of e-learning are done via Internet and it is publicly accessible, so security has a major role to play and the kind of selection of the type of security is provided by the administrator. Privacy, integrity, non-repudiation and authenticity are the four major security aspects of e-learning system. Digital watermarking helps in authenticating the sender. A digital signature is also a part of digital watermarking through which authentication can be achieved.

Watermarking is a technique through which a watermark can be impressed on a paper during production to provide copyright identification. In the digital world we work with binary numbers, so digital watermarking means a pattern of bits inserted into a digital image to authenticate the sender[3]. Digital watermarking, if implemented along with cryptography algorithms, serves a great number of purposes, two of them are copyright protection and data authentication. A watermarking system is shown in Fig.1 (in annexure)[4,5] which demonstrates the watermark incorporation and watermark extraction. In this diagram, we have shown a general architecture of the total watermarking system. The sender will select and send the original document after encoding it using the secret key. This process is known as watermark encoding. Then the watermarked document will send to the receiver through the communication channel. The receiver will decode the watermarked document by using the same secret key, used for the watermark encoding and extract the watermark. Watermark encoder is used to insert or embed the watermark into the original image and watermark decoder is used to decode or extract the watermark from the watermarked document.

In this paper we limited our discussion on the sending of certificate from the administrator to the learner. Section II covers the key generation algorithm and watermark embedding algorithm. Section III includes the retrieval of watermark from the transmitted document. Section IV covers the object oriented modeling of the proposed system and finally we conclude at section V.

2. KEY GENERATION ALGORITHM

Digital watermarking can be combined with secret key cryptographic approach and also public key cryptographic approach[6] to provide better security and authenticity. Secret key cryptography means when both the sender and receiver use the same key for encryption and decryption[7]. In this system, since the same key is used for both the cases, this key should be kept in secret; otherwise, if the hacker can reach the key, may change or destroy the document.

In this paper, we choose two symmetric key cryptography algorithms from the above, to generate the keys, one for encrypting document and the other as a watermark key. As the certificate is a very important document to a student, so it should be sent through a very secure way. In this paper, we choose RC4 for encryption of the certificate and IDEA for the watermark key. The common thing between these two algorithms is the number of keys they use for encryption and decryption and the number is 128. The advantages of using RC4 is[8]

1) It is very difficult to find out the location in the table where a particular value exits.
2) A particular encryption algorithm key can be used only once.
3) Encryption is about 10 times faster than DES.

IDEA is also a symmetric key block cipher which operates on 64 bit block using a 128 bit key and its application is widely spread now-a-days like audio and video data for cable television, e-mail via public networks, smart cards etc[9,10].

Key generation algorithm:

As we discussed above, first we will apply the encryption technique on the certificate then make it watermarked. For the encryption process, we select RC4 symmetric key algorithm. These processes will be done at the administrator's end. RC4 algorithm is cryptographically very strong and easy to implement. The steps for implementing RC4 algorithm is given below[11]:

RC4 algorithm consists of two parts: a) key scheduling algorithm and b) pseudo-random generation algorithm

a) In the key scheduling algorithm it generates the state array

In this initialization state the 256 bit state table S is created using the key k, which is done in two steps, the pseudo-codes are shown below:

```
First step:
for i=0 to 255 do{
        S[i]=i // S is a set equal to the values from 0 to 255
        T[i]=k[i  mod(|k|)]} // T is a temporary vector and k
is array of bytes of secret key and |k| is key length of key k
Second step:
j=0;
for i=0 to 255 do
        j=(j+S[i]+T[i])(mod 256);
swap(S[i],S[j]);
```

Here T is used to produce the initial permutation of S. The single operation on S is swap and S contains the values from 0 to 255. After the initialization phase the input key and the temporary vector T will be of no longer used.

b) In pseudo-random generation algorithm[12,13], it generates the key stream and XOR key stream with the data to generate encrypted system. It generates the key stream k one by one and XOR S[k] with next byte of message to make the data encryption. The pseudo-code of this stage is given below:

```
i=j=0;
while(more byte to encrypt){
        i=(i+1)(mod 256);
        j=(j+S[i])(mod 256);
        swap(S[i],S[j]);
        k=(S[i]+S[j])(mod 256);
        Ci=Mi XOR S[k];
}
```

The above algorithm, shown in the above section, generates a stream of pseudo-random values and the input stream is XORed with these values bit by bit.

Watermark embedding algorithm:

After making the encryption, the next job of the administrator is to embed the watermark into the encrypted document. To fulfill this purpose, here we use IDEA symmetric key algorithm[14]. The encryption algorithm of IDEA regarding the watermark embedding on the digital certificate is discussed briefly[15,16] in the following section:

The 64 bit plaintext will be divided into four 16 bit sub-blocks namely S1, S2, S3 and S4 and each complete round requires six sub keys. The required key size is 128 bit, which is split into eight 16 bit blocks. The first six sub keys are used in round one and remaining two are used in round two. Below the 14 steps of a complete round of IDEA algorithm are shown below:

1. Multiply S1 and the first sub key Z1.
2. Add S2 and the second sub key Z2.
3. Add S3 and the third sub key Z3.
4. Multiply S4 and the fourth sub key Z4.
5. Bitwise XOR the results of steps 1 and 3.
6. Bitwise XOR the results of steps 2 and 4.
7. Multiply the result of step 5 and the sub key Z5.
8. Add the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth sub key Z6.
10. Add the results of steps 7 and 9.
11. Bitwise XOR the result of step 1 and 9.
12. Bitwise XOR the result of step 3 and 9.
13. Bitwise XOR the result of step 2 and 10.
14. Bitwise XOR the result of step 4 and 10.

After round 8, a ninth half round final transformation occurs:

1. Multiply S1 and the first sub key.
2. Add S2 and the second sub key.
3. Add S3 and the third sub key.
4. Multiply S4 and the fourth sub key.

The concatenation of the blocks gives the final result.

3. RETRIEVAL OF THE ORIGINAL CERTIFICATE

All the above processes will be done at the sender (here administrator's) end. Administrator will make the certificate encrypted using the RC4 algorithm and then embed the watermark using the watermark key by using the IDEA algorithm. After the completion of all above processes, administrator will send the same to the learner along with both the secret keys. Learner will first extract the watermark from the watermarked image using the watermark key and then decrypt the certificate using the decryption algorithm using the private key used for encrypting the document.

In case of decryption using IDEA decryption algorithm, the process is quite similar discussed above.

In case of decryption using the RC4, learner has to use the same key used by the administrator during the encryption phase. Learner has to generate key stream by running the key scheduling algorithm and pseudo-random generation algorithm as discussed above and XOR key stream with the encrypted text to get the plain text.

4. OBJECT ORIENTED MODELING OF THE PROPOSED SYSTEM

Now, we will analyze our proposed model by showing some of the object oriented modeling diagrams. This analysis helps to make the understanding better and easy to implement.

A. Class diagram:

Class diagram is a part of Unified Modeling Language, which is used to describe the structure of a system by using the system's classes[17]. To represent our proposed model using class diagram (shown in Fig.2, annexure), we have used three classes BASE, ADMIN and LEARNER. BASE class is used as the base class and the other two classes are publicly derived from the base class[18]. A brief discussion on the classes is given below:

BASE: This class is used as a base class. In the time of encryption, it will convert the plain text into cipher text and vice-versa during decryption. Since same key is used for both the encryption and decryption, we use base class for the key.

ADMIN: This class is designed for the administrator. The functions of the administrators in our model are received all the necessary documents from the learner, generate the certificate and the key and after making it encrypted and embedding with watermark, he/she will send it to the learner.

LEARNER: This class is publicly derived from the base class. Learner will send the required information to the administrator for generating certificate and after receiving the encrypted and watermarked certificate from the administrator and decrypt it using the key provided by the admin and then extracts the watermark.

B. Use case diagram:

Use case diagram is a part of Unified Modeling Language (UML) to show the requirements of a system including internal and external influences. These requirements are generally related with the design requirements. So when a system is analyzed to gather its functionalities use cases are prepared and actors are identified[19]. In our proposed model we have used two types of objects: Administrator and Learner. Here administrator is generating the digital certificate and after encryption and watermarking it, sends to the learner along with the keys. Learners are extracting the watermark using the watermark key by watermark decoder and decrypt the certificate using the same key used by the administrator used at the time of encryption. So, to design the use case diagram, we have used two use case diagrams, one for the administrator and the other for the learner.

In our first use case diagram, shown in fig.3(in annexure), we discuss about the tasks related to the administrator. Administrator has to generate the certificate, make it encrypted using symmetric key encryption algorithm, then watermarked it using the watermarked encoder and for the key also use another symmetric key algorithm. At the end, administrator will send this certificate to the learner along with the private keys.

In the second use case diagram, which is shown in fig.4(in annexure), discuss about the learner's activities. After receiving all the documents from the administrator, learner will first extract the watermark from the certificate using watermark decoder and the decrypt the certificate using administrator's private key.

C. Activity diagram:

Activity Diagram is also a part of UML diagrams, which is used to represent a system graphically like a flowchart, to show the workflows of stepwise activities and actions with support for choice, iteration and concurrency[20].

Fig.5(in annexure) shows the activity diagram of our proposed system. Here administrator choose the RC4 and IDEA algorithm for key generation which will be used in the system for encryption and watermark insertion and the same keys will be used by the learner for decryption and watermark extraction respectively.

D. Sequence Diagram:

Sequence diagram is another example of behavioral UML diagram. It is used to represent the interaction among objects as a two dimensional chart, which is read from top to bottom. The sequence diagram of our proposed model is shown in fig.6(in annexure) which shows the objects interaction arranged in time sequence[21].

5. CONCLUSION

In this paper, we have consider only the transmission of certificate which can be extended to the other essential documents like mark sheet, registration, admit card, study materials etc. This model can also be applicable for other online transaction systems, like e-Commerce, e-Governance and e-Banking. We can also use public key cryptography instead of private key for better security, which is out of scope of this paper.

REFERENCES

1. http://www.virtual-college.co.uk/elearning/elearning.aspx
2. Weippl, R.E (2005), Security in E-Learning, Springer
3. Frank Y.Shih, "Digital watermarking and steganography: Fundamentals and techniques", CRC Press, London, New York
4. S.Banerjee and S.Karforma, "A secret key digital watermarking based authentication of mark sheet in e-learning", IJATES, ISSN: 2348-7550, vol-4(8), Aug-16, pp: 104-107
5. M.Arnold, M.Sschmucker and S.D.Wolthusen, "Techniques and applications of digital watermarking and content protecton", Artech House, Boston, London. 2003
6. S. Sarbavidya and S. Karforma, "Implementation of security in E-tendering using secret key digital watermarking", International journal of advanced research in computer science and software engineering, ISSN: 2277 128X, vol-4, issue-10, October 2014, pp: 112-114
7. B.Schneier, "Applied cryptography", Second edition, Wiley publication
8. https://www.vocal.com/cryptography/rc4-encryption-algoritm/
9. https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm
10. https://www.slideshare.net/Saurabhprajapati759/idea-34236642
11. https://cpe.ku.ac.th/~nguan/class/204427-54/slides/01204427-RC4.ppt
12. William Stallings, "Cryptography and Network security: Principles and practice", Prentice Hall, Upper Saddle River, New Jersey, 2003
13. A.Mousa and A. Hamad, "Evaluation of RC4 algorithm for data encryption", International Journal of Computer Science and Applications, Vol:3(2), June-2006
14. S.Banerjee and S.Karforma, "Authentication of certificate in e-learning using secret key digital watermarking", International Journal of Information Science and Computing, vol:3(2), Dec-2016, pp: 53-58
15. A.Menezes et al., "Handbook of applied cryptography", CRC press, 1996
16. http://www.nku.edu/~christensen/simplified%20IDEA%20algorithm.pdf
17. https://en.wikipedia.org/wiki/Class_diagram
18. A.Ghosh and S.Karforma, "Object oriented modeling of IDEA for e-learning security", proceedings of the international conference on ICA, 22-24 December, 2014, Springer, ISBN: 978-81-322-2267-5 pp:105-113
19. https://www.tutorialspoint.com/uml/uml_use_case_diagram.htm

20. http://www.tutorialspoint.com/uml/uml_activity_diagram.htm

21. https://en.wikipedia.org/wiki/Sequence_diagram

Annexure

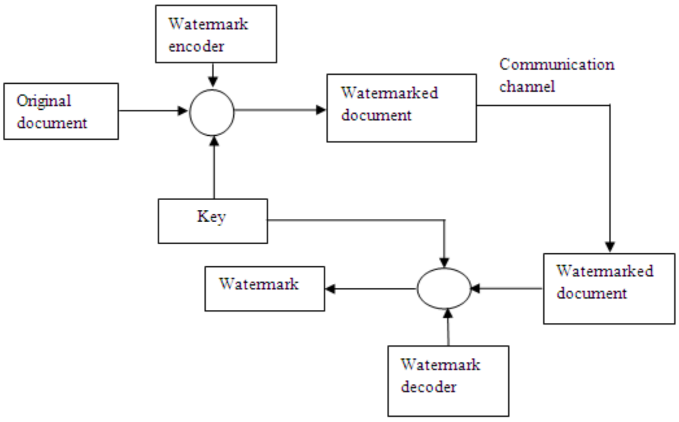

Fig.1: A digital watermarking system

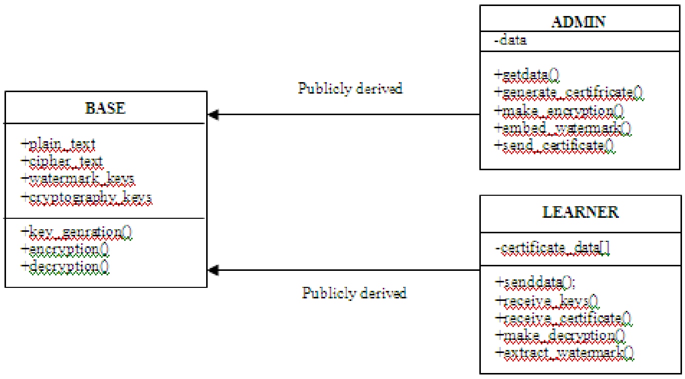

Fig.2: Class diagram of proposed model

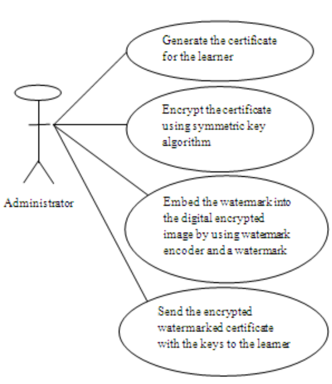
Administrator
Generate the certificate for the learner
Encrypt the certificate using symmetric key algorithm
Embed the watermark into the digital encrypted image by using watermark encoder and a watermark
Send the encrypted watermarked certificate with the keys to the learner

Fig.3: Use case diagram for administrator

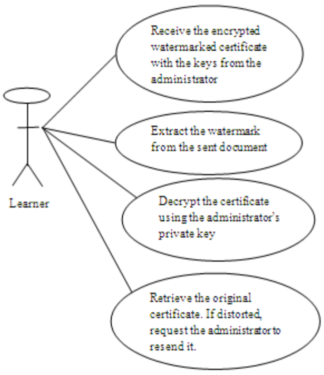
Learner
Receive the encrypted watermarked certificate with the keys from the administrator
Extract the watermark from the sent document
Decrypt the certificate using the administrator's private key
Retrieve the original certificate. If distorted, request the administrator to resend it.

Fig.4: Use case diagram for learner

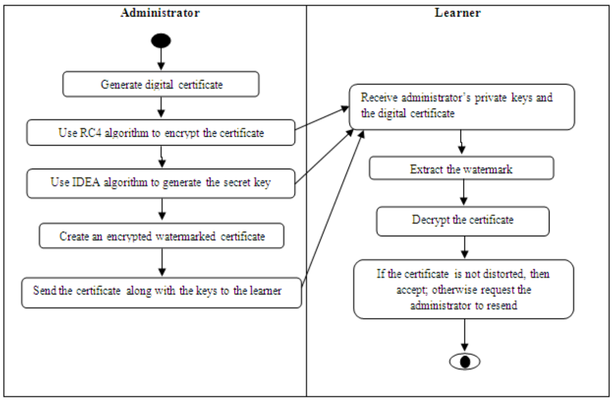
Administrator
Learner
Generate digital certificate
Use RC4 algorithm to encrypt the certificate
Use IDEA algorithm to generate the secret key
Create an encrypted watermarked certificate
Send the certificate along with the keys to the learner
Receive administrator's private keys and the digital certificate
Extract the watermark
Decrypt the certificate
If the certificate is not distorted, then accept; otherwise request the administrator to resend

Fig.5: Activity diagram of the proposed model

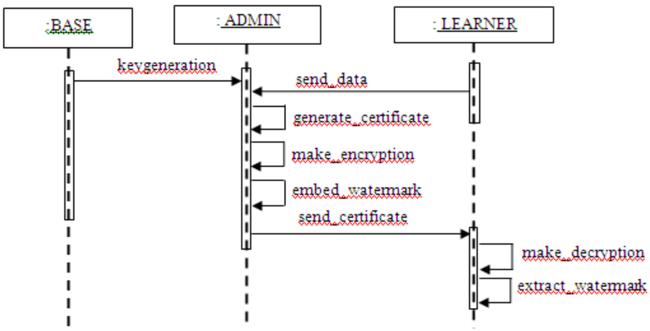

Fig.6: Sequence diagram of our proposed model