A SECRET KEY DIGITAL WATERMARKING BASED AUTHENTICATION OF MARK SHEET IN E-LEARNING

Soumendu Banerjee[1], Dr. Sunil Karforma[2]

[1]Research Scholar, [2]Associate Professor, Department of Computer Science,
The University of Burdwan

ABSTRACT

In any e-learning system, the institutes apply different kinds of Information and Communication Technology (ICT) tools and techniques to communicate between the three main parties- administrator, teachers and students of an e-learning system. All the necessary documents in any e-learning system, like study materials, admit cards, mark sheets etc. are always been sent via Internet or intranet. This kind of transmissions need to be much secured, otherwise, the hackers may destroy or damage the documents during transmission. For this reason, now-a-days, the e-learning organizations give so much importance on authentication. Digital watermark is mainly used in verification of authenticity and integrity of any image, audio or video and carry the identity of its owner. A secret key cryptography is also used for authenticity and secrecy by providing data encryption (at the sender end) and decryption (at the receiver end). In this paper, we propose a secret key digital watermarking for authentication of an important e-learning document, mark sheet, transmitting from administrator to the student. The application of digital watermarking makes this system more accurate, because if the hacker may be able to reach the document and make any changes, then the watermark will also be changed and the receiver (here student) will identify the change and would request to the administrator to resend it.

Keywords**: *E-learning, Digital watermarking, DES, Blowfish***

I. INTRODUCTION

As the computers and networking facilities are becoming less expensive and easily available, the use of Internet is also increasing. The applications of Information and Communication Technology (ICT) in various e-service fields like e-commerce, e-governance, e-banking as well as e-learning are also being widely spread. In case of e-learning, all communications between the three main participants - administrators, teachers and students, have been done either through Internet or Intranet[1]. Here, we will discuss on the authentication of the transmission of one of the important document in any kind of learning- mark sheet, transmitting from administrator of any e-learning institute to their students. With the increasing rate of using internet, the different kinds of attacks are also increasing and most of them are occurring during transmission of any documents. If the hacker can reach to the mark sheet while transmitting from the administrator to students, they can change or destroy it, which makes a bad impact about the institution. For this reason, now-a-days, the e-learning institutes give emphasis on authenticity and secrecy while sending their data.

Digital watermarking is a very important technique which is mainly used to authenticate the sender of the documents and if we can implement it using a secret key encryption, then it will become a more powerful system for data authentication[2]. In this paper, we will propose a secret key digital watermarking which can be imposed to mark sheet, during transmission, and after receiving the watermark can be decomposed for verification.

Here we apply two different symmetric key cryptography and two things are common to them: both of them use 64 bit block at a time and use the Feistel construction of network.

In this paper, Section-II provides information about the insertion and extraction of watermark in the mark sheet while transmitting from administrator to student. In section-III, we discuss about the proposed algorithm for authentication of mark sheet and finally we will end up in section-IV by giving some brief conclusion and discussing on some future scope.

II. METHOD OF INCORPORATION AND EXTRACTION

Digital watermarking is a technique through which we can insert a pattern of bits into a digital image, audio or video and can also be extracted to verify the authentication of the owner[3,4]. The current watermarking systems use the same key for encoding and decoding of the watermark[5]. In this process, the sender inserts the watermark into the image, which is known as the carrier image or original image. After the insertion, the image may be slightly modified from the original image and known as watermarked image. This watermarked image is sent via communication channel to the receiver. When the receiver extracts the watermark from the watermarked image, the original image remains as it was before insertion of watermark. This method is known as watermark extraction.

In our proposed system, the sender is the administrator, the original image is the scan copy of the mark sheet; watermark is the unique authentication identity of the e-learning institution, secret key will be calculated from the following proposed algorithm; and the receiver is the student.

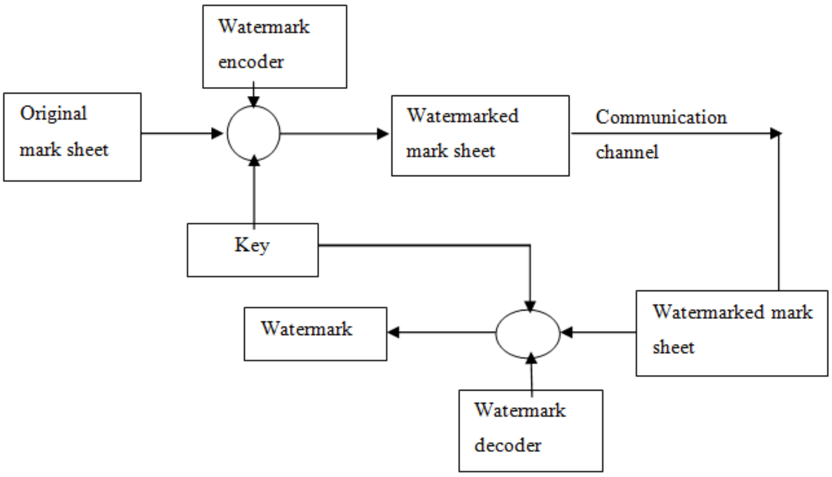

Fig.1: A digital watermarking system

In the above figure (Fig.1), we have shown a general digital watermarking system[1,5] regarding the transmission of the mark sheet from the administrator to the student. After the transmission of the watermarked mark sheet, student will be able to perform the watermark detection process. This process requires the watermarked mark sheet, and the secret key, that was used in the watermark insertion. Here the secret key will be selected by the administrator and have to send secretly to the student. The output of this process carries the authenticity of the e-learning institution.

III. PROPOSED ALGORITHM FOR MARK SHEET AUTHENTICATION

In digital watermarking, we can apply two types of cryptographic approaches – secret key approaches and public key approaches[6frm paper]. In secret key cryptography, the sender and receiver both use the same key for the encryption and decryption. In this process the secret key[6], used by the both parties should be kept secret from the outsiders; otherwise, if the hacker can get key, then they can decrypt the message and may damage it. In public key approach, two keys are used, one for encryption and the other for decryption. The message can be encrypted by the public key of the sender, but decryption is only possible by using the receiver's private key[7].

Key generation algorithm:

In our proposed system, to make the authentication process better, first we will use the encryption technique by using secret key and then use watermark on that encrypted message. For these, we need two keys, one for encryption and the other for watermark. Encryption and the watermark insertion are done at the administrator end and watermark extraction and decryption is done at the student end.

In our proposed system, we use DES algorithm to encrypt the mark sheet. The steps of the DES algorithm are shown below in brief:

Step 1: Administrator will take a 64 bit plaintext of which 8 bits are parity.

Step 2: Discard the parity bits and make the permutation on the data and break them into two halves to calculate 16 sub keys.

Step3: Encode each 64 bit block of data and finally a permutation has been done with the left and right block.

Watermark embedding algorithm:

After encrypting the mark sheet, the next thing done by the administrator is to embed the watermark with it, to provide better security and authenticity. Here, we use the Blowfish algorithm[8] to generate keys. The steps of this process are given below:

Step 1: First the administrator has to choose the 64 bit block of data at a time. This algorithm is divided into two parts: key expansion and data encryption.

Step 2: In the key expansion method, the algorithm converts a key of almost 448 bits into several sub keys.

Step 3: The data encryption step include 16 rounds of iterations. The 64 bit plaintext is divided into two halves of 32 bits each and the XORs and the additions are done on these halves. Each round of iterations includes key dependent permutation and key and data dependent substitution.

Algorithm to retrieve the original mark sheet:

This process is used to get the original message back from the watermarked image. This process is done at the student's side. Student has to first extract the watermark and then decrypt the encrypted message to get the original image back. These steps are discussed below:

Step 1: The student has to choose 64 bit block at a time and divide them into exactly two halves. Then the total decryption technique is the reverse of the encryption technique.

Step 2: In case of the decryption process of DES algorithm, the steps are identical with the steps applied in the encryption technique; only the student has to apply the sub keys in the reverse order[9].

IV. CONCLUSION

In our present paper emphasis is given on authentication of mark sheet. However, the same model may be used for authentication of study material, admit card, registration certificate etc. which are must important documents in e-learning. The digital watermark technique use DES for key selection and Blowfish for message encryption. The main problem of present system is secure distribution of key from sender to receiver. This problem can be overcome by using public key cryptography which is beyond the scope of present work.

REFERENCES

[1] "Security in E-Learning", Weippl, R.E (2005), Springer

[2] "Digital watermarking and Steganography: Fundamentals and techniques", Frank Y. Shih, CRC Press, New Delhi, 2008

[3] http://www.webopedia.com/TERM/D/digital_watermark.html

[4] 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

[5] "Techniques and applications of digital watermarking and content protecton", M.Arnold, M.Sschmucker and S.D.Wolthusen, Artech House, Boston, London. 2003

[6] http://www.dcs.ed.ac.uk/home/adamd/essays/crypto.html

[7] https://en.wikipedia.org/wiki/Public-key_cryptography

[8] http://iitd.vlab.co.in/?sub=66&brch=184&sim=1147&cnt=1

[9] http://www.herongyang.com/Cryptography/DES-Algorithm-Decryption-Algorithm.html