

Authentication of Certificate in E-Learning Using Secret Key Digital Watermarking

Soumendu Banerjee¹ and Sunil Karforma²

¹Research Scholar, Department of Computer Science, The University of Burdwan, India

²Associate Professor, Department of Computer Science, The University of Burdwan, India

Corresponding author: bansoumendu@gmail.com

Abstract

In an e-learning system, while the documents are transmitting between the communicating parties, authentication is too much necessary. Digital watermarking along with the encryption technique may be used to provide authenticity. International Data Encryption Algorithm (IDEA) is one of the very useful symmetric key cryptographic algorithms, which is also free to all for any users, can be used for the key selection for encryption and 3DES can be used for watermark key selection. Digital watermarking is one of the very popular authentication techniques. So, while transmitting any document like registration certificate in any e-learning system, which should be transmitted from the developer to learner, the developer can use this technique to make a secure transaction. As we know that certificate is very essential document for any kind of learning, if the hacker can reach the document while transmitting from developer to learner, he can modify or destroy the documents. If the developer uses our proposed technique while transmitting, and if the hacker makes any changes, then it affects the watermark, and easily identified. In this situation, student can also ask for retransmitting the certificate.

Keywords: Digital watermark, Cryptography, IDEA, 3DES

Objectives:

The main objective of this paper is authentication of e-learning resources such as certificate, would be done by developer utilizing the benefit of IDEA as most useful encryption algorithm along with the benefits of triple DES algorithm for watermarking key selection.

In case of transmitting e-learning documents, authentication plays a vital role. Registration certificate contains the unique registration id of a student. If any kind of problem occurs regarding this identification

number, then it becomes difficult for the developer or administrator in future and also it makes a hazard for that student. So, during transmission of certificate, the developer should protect this for the sake to maintain a good impact of the e-learning institute.

Digital watermarking helps the receiver to identify the source, creator, owner, distributor or authorized consumer^[1] of the document he/she receives. In case of watermarking, the process includes the two main steps: watermark embedding and watermark extraction. When the watermark is attached with the watermark, the image is known as embedded watermark and one of the characteristics of this embedded watermark is private versus public. Private watermark means only the authorized users can extract the watermark by using the private pseudo-random key and public watermark means the place of the watermark is known to everyone and the detection software can easily detect the watermark by scanning the image. Comparing the above two cases, we can easily conclude that the private watermarking is robust than the public watermark. In this paper we will use the International Data Encryption Standard (IDEA) algorithm for choosing the secret key for private watermarking. IDEA is a symmetric key block cipher and an improved version of Proposed Encryption Standard (PES), which was designed in the year of 1991 by James Messy of ETH, Zurich and Xuejia Lai with the intention of replacing the Data Encryption Standard (DES)^[2]. Triple Data Encryption Standard (3DES) is an improved version of DES.

In this paper, we have proposed a model to implement the encryption algorithm with the digital watermarking concept, which makes any transmission process more secure. Here we will concern only the transmission of certificate from the developer to learner through our proposed model. Digital watermarking is a technique which can be combined the encryption algorithm through which sender can provide authenticity to the receiver.

Section II includes the watermark insertion and extraction process along with diagrams regarding the transmission of certificate from developer to learner. Section III covers the proposed algorithm to provide authenticity to the learners. It includes the key generation algorithm, watermark embedding algorithm and also the algorithm to retrieve the original. Finally, we conclude in section IV by showing some future scopes.

Review of Literature

Digital watermarking using secret key cryptography

Digital watermarking is a technique through which authentication of any document can be achieved. The factors, which are the main concerns of this paper, are authenticity and robustness by selecting the secret key, which is essential for the encryption. Prior works had been done on the basis of selecting the appropriate secret key by taking the suitable secret key cryptography algorithms. Chen Ling et al. discussed in their book about the importance of choosing the key for authentication in image watermarking^[3]. S.Sarbavidya et al. used AES algorithm to achieve security in E-commerce system. In my prior work, I had chosen DES and Blowfish as secret key encryption algorithms. The robustness of the model is based on the choosing of the secret key using the appropriate encryption algorithm.

Watermark embedding and extraction

The main benefits of the digital multimedia files are distortion free transmission, compact storage and easy editing. Watermark is a way to design impressed on a piece of paper during production like a logo. Digital watermarking is a process to embed a marker to hide the digital information from the outside world and sometimes for checking the authenticity and integrity or to show the identity of the owner^[4]. The sender while transmitting the document, embed the watermark and after receiving the document the receiver can extract the watermark and can check for the originality^[5].

In our proposed system the developer of the e-learning institute is the sender and the learner is the receiver and the transmitted document is the certificate of the e-learning institute.

In the digital watermark technique, the steps include insertion of the watermark, extraction of the watermark and watermark detection. Here, we use the following diagram regarding the transmission of certificate from developer to the learner in an e-learning system referred to a digital watermarking system.

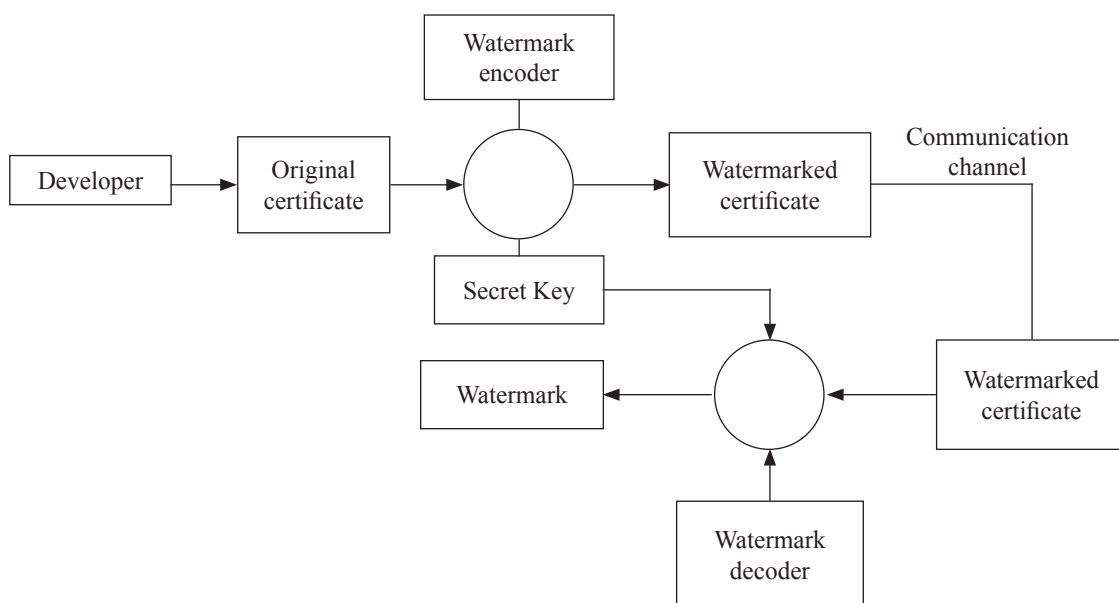


Fig. 1: A digital watermarking system

The above diagram shows the digital watermarking system regarding the transmission of certificate from developer to learner. This process includes the original certificate to which watermark will be embedded, a secret key which is used in both the watermark insertion and extraction and watermark encoder to encode the watermark and watermark detector to detect the watermark.

Proposed algorithm of certificate authentication

Digital watermarking includes secret key cryptographic approach and also public key cryptographic approach^[6]. When we use the secret key cryptography in digital watermarking, the developer and the

learner both use the same secret key for the both the insertion and extraction processes. Since, both the developer and learner use the same key, that key should be kept secret; otherwise, if the hacker can reach the key, they may change or destroy the certificate. In case of public key cryptography in digital watermarking system, the developer and the learner use different keys, one for insertion 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

To make our proposed system more authenticate, first we will use the encryption technique and then apply digital watermarking. The same process will be applied in reverse order at the learner's end. To achieve this we required two secret keys: one for the encryption process and another for the watermark process. The encryption and the watermark insertion are done at the developer's send and the decryption and the watermark extraction are done at the learner's end.

In our proposed system, we use IDEA algorithm to for the encryption of the certificate:

The steps of the IDEA algorithm are shown below in brief^[8,9,10]:

First we have to split the 64 bit plaintext into four 16 bit sub-blocks X_1 , X_2 , X_3 and X_4 . Each complete round requires six sub keys. The 128 bit key 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. Here the 14 steps of a complete round are shown below:

1. Multiply X_1 and the first sub key Z_1 .
2. Add X_2 and the second sub key Z_2 .
3. Add X_3 and the third sub key Z_3 .
4. Multiply X_4 and the fourth sub key Z_4 .
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 Z_5 .
8. Add the results of steps 6 and 7.
9. Multiply the result of step 8 and the sixth sub key Z_6 .
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 X_1 and the first sub key.

2. Add X_2 and the second sub key.
3. Add X_3 and the third sub key.
4. Multiply X_4 and the fourth sub key.

The concatenation of the blocks gives the final encrypted certificate.

Watermark embedding algorithm

The next job of the developer after doing the encryption is to embed the watermark into the encrypted certificate. To implement this one, we have required one secret key. To select that secret key, in our proposed model, we use triple DES or 3DES algorithm.

Triple DES or 3DES is an up gradate version of the Data Encryption Standard algorithm. In 3DES, the steps of DES algorithm are same but they are applied for 3 times to each block of data. In 3DES, in general, 3 keys are used for encryption. At first developer will encrypt the certificate using the key k_1 , then decrypt it using key k_2 and again encrypt the material using key k_3 ^[11,12]. We can explain it simply as: Cipher text= $E_{k_3}(D_{k_2}(E_{k_1}(\text{plaintext})))$.

Algorithm to retrieve the original certificate

Here we use this process to get the original certificate back from the watermarked image. This process is done at the learner's end. Learner will first extract the watermark from the watermarked certificate and then decrypt the encrypted certificate to get the original one back. During this process the original may be quite distorted, which can overcome by using some watermark techniques. These steps are discussed below:

1. In case of decryption using IDEA follows the same rules as in the time of encryption discussed above but new keys must be generated for decryption.
2. Student has to decrypt the encrypted certificate after receiving it from the developer. First, student will decrypt the study material using k_3 , and then encrypt the material using k_2 and again decrypt using the key k_1 . We can explain it simply as: Plain text= $D_{k_1}(E_{k_2}(D_{k_3}(\text{cipher text})))$

Conclusion

Authenticity is one of the main issues in not only for e-learning but also for the other electronic systems like e-commerce, e-banking, e-governance etc. All of these include transmission of documents via internet. So, this proposed model may also be useful for the administrators for these kind electronic transactions. Public key encryption techniques can also be used in case of encrypting the documents, which is time consuming and more cost effective, but will make the system more secure. Public key encryption is also slower and more complicated in compare to the secret key encryption. We can also use digital right management for better security, which is beyond the scope of this paper.

References

1. Frank Y. Shih, "Digital watermarking and steganography: Fundamentals and techniques", CRC Press, London, New York

2. https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm
3. C. Ling and O. Ur-Rehman, "Watermarking for image authentication(Chapter 2)", "Robust image authentication in the presence of noise", Springer international publishing, Switzerland, 2015. N.Zivic(ed).
4. https://en.wikipedia.org/wiki/Digital_watermarking
5. 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
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. https://en.wikipedia.org/wiki/Public-key_cryptography
8. B.Schneier, "Applied cryptography", Second edition, Wiley publication
9. A.Menezes et al., "Handbook of applied cryptography", CRC press, 1996
10. <http://www.nku.edu/~christensen/simplified%20IDEA%20algorithm.pdf>
11. <http://www.cryptographyworld.com/des.htm>
12. https://en.wikipedia.org/wiki/Triple_DES