Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Security in E-Tendering using Secret Key Digital Watermarking

Sirsendu Sarbavidya[*]
Research Scholar, Computer Science
Burdwan University, India

Sunil Karforma
Associate Professor, Computer Science
Burdwan University, India

Abstract* — In today's world, different government as well as private organizations have taken initiative to successfully implement electronic version of services in transparent & accurate manner among the citizens and customers by using different ICT tools and techniques. Tendering process for procurement of different objects is one of the sensitive functions, which lacks transparency, accountability and security. In present days, this tendering process is implemented by electronic way to simplify complex manual activities for purchasing of goods and services using the Internet in a transparent manner, as it is a significant part of the procurement cycle. But, one of the major factors that are limiting the success of E-Tendering approach is that the security measure is not properly implemented. In this paper, we propose a Secret-Key Watermarking algorithm for verification of integrity of transmitted tender document via Internet from different organization to the supplier and vice versa in E-Tendering environment, so that the watermark is capable enough to detect any changes made to the online tender document by malicious users.

Keywords* — AES, Digital Watermarking, E-Tendering, G2B, ICT, Public-key, Secret-key, Symmetric-key Algorithm, Watermark-Extraction, Watermark-Insertion.

I. INTRODUCTION

The conventional tender processing system [1] uses personal human to human interactions and suffers from various drawbacks such as delay in tender processing, human interference at every level of processing, inadequate transparency, and most importantly lack of security. The process also involved a large vendor community; most of them took advantage of the dependencies involved, manipulated the prices and dictated terms. Obtaining a better price and provides transparency, accountability and security is a prime challenge for the organizations. In order to achieve simplification of process, greater transparency, reduced processing time, fair competition and enhanced security measurement, organizations implemented a web-based Government to business (G2B) solution for E-Tendering process.

In modern days, with the help of Internet, we can get end to end transmission between different communicating parties. As the communication is easy to establish and is of low cost, there is always a high chance of getting hacked [8] by malicious users who can not only destroy the online information but also hampers confidentiality of the system and society.

So, providing security is the most important aspects of success of any online service. To successfully execute E-Tendering process, we need to provide high level of security of online tender documents as Internet is the only medium via which confidential documents are exchanged between different stakeholders.

The primary objective of E-Tendering system is to provide high level of security but it also satisfy some other objectives as well, like –

1. Cost savings for supplier and organizations.
2. Speed up the process by shortening the tender cycle.
3. Anytime, anywhere access to information.
4. Transparency and accountability in the process.

In this paper, Section-II identifies basics of Secret-key Watermarking technique. Section-III provides information about methods of incorporating watermark into E-Tender document and its extraction. Section-IV identifies the proposed algorithm for authentication in E-Tendering system in detail, which may be used to support security strength of the system, and Section-V identifies some of the features of the proposed work and also indicates its future scopes.

II. BASICS OF SECRET KEY WATERMARKING TECHNIQUE

Digital watermarking [3] is a technique to insert a digital signature into the message so that the signature can be extracted for the purposes of ownership verification and/or authentication. It inserts the hidden information into the message, also called the cover-media [11]. This hidden information is called the watermark. After inserting the watermark [5] via specific algorithms, the original media will be slightly modified and is referred as watermarked media. There might be no or little perceptible differences between the original media and the watermarked one.

After embedding the watermark, the watermarked media are sent over the transmission channel to the receiver, where they are checked for authenticity of the owner. A technique called watermark extraction [5] is performed here for verification of the ownership.

There are two types of cryptographic approaches that we can use in watermark applications – Secret-key approach and Public-key approach [6].

In Secret-key watermarking [10], we have an embedding function that takes a message, an original work and outputs a watermarked work. Similarly, we have a detection function, which takes a watermarked work and outputs a message. The mapping between watermarked works and the messages is controlled by a watermark key. Watermarking algorithms based on a Secret-key present a security that they do not allow a public recovery of the watermark. To implement Secret-key watermarking, the watermark embedder use one watermark key and the watermark detector use the same watermark key for extraction.

III. METHODS OF INCORPORATION AND EXTRACTION

In watermark embedding process [10], [12], the input to the scheme is the watermark (unique supplier id), the cover-media (tender document) and a Secret-key (generated using our proposed algorithm). The Secret-key is used to enforce security, which is the prevention of unauthorized parties from recovering and manipulating the watermark. The output of the watermarking scheme is the watermarked tender document.

In Watermark detection process [7], [9], inputs to the scheme are the watermarked tender document and Secret-key (that are used in the watermark insertion). The output of the scheme gives us confidence measure regarding privacy and confidentiality of the online tender document by checking integrity and authenticity of the test data.

IV. PROPOSED ALGORITHM FOR E-TENDERING AUTHENTICATION

We used a Secret-key in our proposed algorithm for embedding and extraction process of watermark as secrecy is the primary concern in successful E-Tendering application. The key-space [15] that we have chosen for our proposed algorithm is large enough to make exhaustive search attacks impossible.

We add an extra level of security [13] in the watermarking method and the message is encrypted before it is embedded and decrypted after it is detected. Such a system requires two types of keys – the watermark key, which controls watermarking process for security reasons and the encryption key, which controls encryption and decryption process and provides extra level of security.

A. Key Generation Algorithm

In this algorithm, server side machine (organization) generates two types of keys, the watermark key and the encryption key, that are used in the watermarking application. The encryption key along with tender paper is supplied to the contractors via secure channel and the contractors can use the supplied tender paper to create their tender proposal at client side (contractor site) with the help of shared secret key.

Server side machine use a random number generator [2], [14], [15] to produce the watermark key and the encryption key. Here, server side machine used cryptographically strong pseudorandom number generator. The generator uses three 3DES [2], [4] standard algorithm with two keys (encryption – decryption – encryption). The first pseudorandom number uses a 112 bit seed as the initial vector (IV), the rest of the pseudorandom numbers use the seed that are generated by the previous phase.

B. Watermark Embedding Algorithm:

This algorithm is developed to insert generated watermark in the original message (tender document) to provide security and authenticity. This process is also executed in the server side (organization) of the application.

1. Initially, server side application program pad some information (if needed) within the message so that they can evenly break the message into blocks of 128 bits.
2. The server side machine then chooses the generated encryption key to encrypt the block using encryption function E (.). The encryption function uses AES technique with 12 rounds and key size of 192 bits.
3. After encrypting the block, the server side machine applies another encryption function E1 (.) using watermark key to incorporate the watermark information on the message block. The encryption function here uses AES technique with 14 rounds and key size of 256 bits.

C. Watermark Detection Algorithm:

This algorithm is developed to extract generated watermark [13] from the watermarked message to identify authenticity of the message. The decryption functions are complementary of the encryption functions that are used in the embedding algorithm. This process is executed in the server side (organization) of the application.

1. The server side machine split the watermarked message into several blocks.
2. Then, the server side machine applies a decryption function D1 (.) on individual blocks using the same watermark key to produce the corresponding block of watermarked message. The decryption function here uses AES technique with 14 rounds and key size of 256 bits.
3. Finally, the server side machine applies another decryption function D (.), using the same encryption key, which is used to decrypt the block to identify actual information. The decryption function uses AES technique with 12 rounds and key size of 192 bits.

In 3DES, we used only two keys. The first and the third stages in each block use one key and the second stage uses another key. The keys that are used here are generated by cryptographically strong pseudorandom number generator. The encryption of message includes encryption-decryption-encryption blocks. On the other hand, decryption of message includes decryption-encryption-decryption blocks.

V. CONCLUSIONS

We have applied AES block cipher algorithm for encryption and decryption of messages as well as for watermarking. It is an open algorithm and can be implemented in software, hardware, and firmware at ease. The algorithm is so simple that they can be easily implemented using cheap processors and a minimum amount of memory is needed. Practically the space in digital contents where watermarking can be applied is very limited. So, we need a simple algorithm rather than a complex method, which takes less amount of space and requires smaller execution time. The proposed algorithm is designed in such a way that we can easily implement the algorithm into any Government-to-Business (G2B) model.

We can enhance the security of e-Tendering system or any other G2B model, if we are able to construct an algorithm that will follow the approaches of Public-key Watermarking, and key distribution problem will no longer exists there. Nowadays, it is common to use a Secret-key algorithm for large amounts of data transmission and a Public-key algorithm to transmit its key. If we can apply compression prior to encryption of the message, the computational demand of the subsequent encryption stage will be decreased.

The main drawback of the proposed algorithm is that, if the distribution of key among the supplier and the public sector organization is not controlled in secure way, then the hacker can hamper the security of the system in large.

As we know, the main requirements on watermarking schemes is security and robustness against intentional or un-intentional attacks attempting to remove or destroy the water-marks, this Secret-key authentication watermark can detect any changes made to the document & thus satisfies our purpose.

REFERENCES

[1] Agarwal A., *E-governance: Case study*, Hyderabad: University Press, 2007.

[2] B. A. Forouzan, *Cryptography and Network Security (Special Indian Edition)*, New Delhi: Tata McGraw Hill, 2007.

[3] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, *Digital Watermarking and Steganography (2nd edition)* , USA: Morgan Kaufmann Publishers, 2008.

[4] *NIST, Data Encryption Standard (DES), National Institute of Standards and Technology,* Gaithersburg, MD, May 1994.

[5] *IEEE, IEEE STD 1363-2000: Standard Specifications for Public key Cryptography*, January 2000.

[6] Schneier, B., *Applied Cryptography*, New York, USA: John Wiley & Sons., 2nd ed., 1996.

[7] Hartung, F., and B. Girod, "Fast Public-Key Watermarking of Compressed Video," in *International Conference on Image Processing*, Santa Barbara, California, Oct. 1997.

[8] Stevenson, F.A., *"Cryptanalysis of Contents Scrambling System,"* Usenet Posting, November 1999.

[9] Fabien A. P. Petitcolas and Ross J. Anderson, "*Evaluation of copyright marking systems*," Proceedings of IEEE Multimedia Systems'99, vol. 1, pp. 574-579, 7-11 June 1999, Florence, Italy.

[10] Wong, P.W., "A Public Key Watermark for Image Verification and Authentication," in *Proceedings of the International Conference on Image Processing*, vol. 1, Chicago, Illinois, Oct. 1998.

[11] Tirkel, A., et al., "Electronic Water Mark," in *Proceedings DICTA 1993*, Dec. 1993, pp. 666-672.

[12] Stefan Katzenbeisser, and Fabian A.P.Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, London: Artech House, 2000.

[13] Jeng Shyang Pan, Hsiang Cheh Huang, and Lakhmi C. Jain, *Intelligent Watermarking Techniques (Series on Innovative Intelligence – Vol. 7),* Singapore: World Scientific, 2004.

[14] Bender, W., et al., *"Techniques for Data Hiding,"* IBM Systems Journal, vol. 35, Nos. 3&4, 1996, pp. 313-333.

[15] Kahn, D., *The Code Breakers – The story of Secret Writing* – New York, USA: Scribner, 1996.