Watermarking Algorithm for Software Privacy Protection

Kamini Solanki [1], Abhishek Mehta[2]
[1]Associate Professor (Parul Institute of Computer Application, Parul University, India)
[2]Assistant Professor (Parul Institute of Computer Application, Parul University, India)

***Abstract*—Digital Watermarking describes techniques that hide information, for example a number or text in digital media, such as images, video or audio. Software piracy is one such risk, which proves unsafe in protecting the intellectual property rights. There have been a variety of techniques developed to address the issue like software watermarking and code protection. This paper presents a new watermarking technique that create a string using personal information from software and merged it with hardware parameters of the client machine then combine with dealer's license key. Our proposed algorithm embed a watermark based on this string contents and send to the server for registration. The proposed technique will be beneficial in combating software piracy and securing the software code from redeployment.**

Index Terms*—Digital watermarking; copyright protection; authentication; software piracy; redeployment

INTRODUCTION

Digital watermarking is the means for providing authentication and copyright protection for digital contents. Currently, software piracy is a major problem for software developers. Techniques are being developed and employed to control software piracy [2], [3], [7], [8], [9], [10], [11], [12]. Various schemes have been proposed and put in operation to minimize the impact of software piracy by limiting unauthorized modification.

Also, the problem of protecting software from illegal copying and redeployment has been the focus of considerable research.Sometime unfortunately software is illegally redistributed or an important algorithmic secret is stolen, an owner would like to be able to take action against the theft. This requires demonstration of ownership and/or identification of the source of the illegal redeployment. A technique which enables such action is software watermarking which has been the core aspect of this paper.

In this paper, we proposed a new technique for securing the software from being pirated. It has been divided in three phases. First phase involves the extraction of personal information from software, hardware parameters of the client machine and dealer's license key.And Second phase encrypt extracted contents and third phase includes embedding a watermark in the software using extracted and encrypted contents from first and second phase.

What is Digital Watermarking?

A digital watermark is a signal permanently embedded into digital data (audio, images, video, and text) that can be detected or extracted later by means of computing operations in order to make assertions about the data [13] [14]. The watermark is hidden in the host data in such a way that it is inseparable from the data and so that it is resistant to many operations not degrading the host document. Thus by means of watermarking, the work is still accessible but permanently marked. Digital watermarking techniques derive from steganography, which means covered writing (from the Greek words stegano or "covered" and graphos or "to write"). Steganography is the science of communicating information while hiding the existence of the communication.

Why Digital Watermarking?

Digital watermarking is an enabling technology for e-commerce strategies: conditional and user specific access toservices and resources. Digital watermarking offers several advantages. The details of a good digital watermarking algorithm can be made public knowledge. Digital watermarking provides the owner of a piece of digital data the means to mark the data invisibly. The mark could be used to serialize a piece of data as it is sold or used as a method to mark a valuable image. For example, this marking allows an owner to safely post an image for viewing but legally provides an embedded copyright to prohibit others from posting the same image.

Types of Digital Watermark: Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

i. Text Watermarking ii. Image Watermarking iii. Audio Watermarking iv. Video Watermarking

In other way, the digital watermarks can be divided into three different types as follows:

i. Visible watermark
ii. Invisible-Robust watermark
iii. Invisible-Fragile watermark

previous work

Many approaches are proposed and implemented to prevent software piracy. Some people gave the concept of robust watermarking technique to prevent software piracy [2]. The SMS based gateway

technique was used in this paper where an automation process is required as a manual response for each software. S.Mumtaz et. al [3] in her paper has relied on the extraction of hardware characteristics of client machine while registering for software which is not well enough for illegally distributing the software invariably. The paper [6] was based on static software watermarking techniques which are highly susceptible to semantics preserving transformation attacks and are therefore easily removed by an adversary. This paper had future inclinations towards the use of dynamic software watermarking algorithms. Z.Jian-qi et. al. [7] presented a novel robust dynamic watermarking scheme based on STBDW that first utilizes the Shamir Threshold Scheme to split the watermark number into pieces, which help to retrieve the original watermark with partial information and increase resilience, then the encryption is done and self-isomorphic mapping are embedded into dynamic branch structure of the program, which can resist most semantics-preserving attacks. However, these techniques are susceptible to statistical attacks. J. ZHU, J. Xiao, and Y. Wang [8] introduced Fragile Watermarking Algorithm which was implemented on Software Content Management. This paper solves the defects and problems of Software Version Control and Software tamper-proofing, still there is more need of perfection while embedding the watermark with compiler program.

software watermarking

Software watermarking is used to embed additional information in a piece of software in order to encode identifying information. However, for software watermarking to be useful it must be resilient against a variety of attacks, e.g. semantics-preserving code transformations and program analysis tools. Software watermarking takes the approach of discouraging piracy through a program transformation which embeds a message (the "watermark") into the program. Each watermarking algorithm is categorized based on a set of characteristics. Software watermarking algorithms [6] and [7] are classified in different classes depending upon their goals, extraction, execution and implementation. These watermarking algorithms are further classified into [2] robust and [8] fragile techniques. Of these, Fragile Watermarking technique has been used in this paper for embedding the watermark in the software.

proposed techniques

The current research proposes the design, development and implementation of a model for controlling the software piracy (Fig. 2). The design and development of this technique is discussed in three phases. Our technique for securing the software from being pirated. It has been divided in two phases. First phase involves the extraction of personal information from software, hardware parameters of the client machine and dealer's license key. And Second phase generates watermark and third phase includes embedding a watermark in the software using extracted contents from first phase and encrypted by second phase.

Phase 1:

When the process of installation starts on client machine the unique personal information + hardware parameters + dealer's license key are extracted.

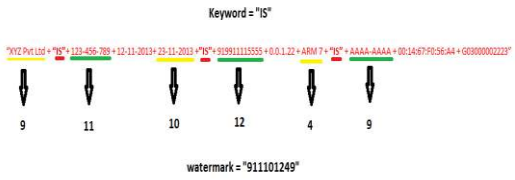
These parameters includes Name of company(NC), Social Security No. (SSN), Software manufacture Date (SMD), Software Installation Date(SID), Serial Number (SN), Version Detail (VD), client machine Processor ID (PID), Hard Disk ID (HDSN), Media Access Control Address (MAC). Introduce the License No. (LK) of software and merged with registration code.

RGC = NC + "IS"+ SSN + SMD + SID + "IS"+ SN + VD + PID +"IS"+ HDSN+ MAC + LK.

For example: RGC= "XYZ Pvt Ltd + "IS"+ 123-456-789 + 12-11-2013+ 23-11-2013 +"IS"+ 919911115555 + 0.0.1.22 + ARM 7 + "IS" + AAAA-AAAA + 00:14:67:F0:56:A4 + G03000002223"

Phase 2:

A keyword "IS" from the RGC code is selected and a watermark is generated based on the length of proceeding and next word length, to and from the keyword occurrences in RGC code text. This process is illustrated in fig. 1, where 'is' is the keyword and based on REG code text contents, a watermark is generated.



Phase 3:

Embedding a software watermark (SW) we are inserted registration code as watermark into the software. The algorithm which embeds the watermark in the text is called embedding algorithm. The watermark embedding algorithm requires original string and keyword as input by the copyright owner/dealer. A watermark is generated as output by this algorithm. Once this process is complete, the watermarked software (SW) is delivered to the client.

The algorithm proceeds as follows:

1. Fetch the parameters like personal information + hardware parameters + dealer's license key of the client machine.

2. Merge the string with "IS" keyword by multiple occurrences.

3. Create a string RGC = NC + "IS"+ SSN + SMD + SID + "IS"+ SN + VD + PID +"IS"+ HDSN+ MAC + LK for registration at the server end.

4. Submit RGC to the server.

5. Read RGC.

6. Count occurrence of each word in RGC.

7. Select KW based on occurrence frequency.

8. KWCOUNT = Total occurrence count of KW in string RGC.

CONCLUSION

The technique proposed in this paper was tested, verified and implemented with C# framework for number of systems. The software purchased cannot be installed on client system without the verification and validation of the watermarked information. If anybody wants to pirate the copy of software of the client on its system, the proposed technique does not allow him/her to do so, if implemented. This has given an opportunity to client to purchase the software and use it without the risk of redeployment of software to others. By doing so, intellectual property of the developer and value for money of the client, both are protected. This technique can be implemented over different mobile platforms.

RREFERENCES

[1] Robert, L., and T. Shanmugapriya, "A Study on Digital Watermarking Techniques ", International Journal of Recent Trends in Engineering, vol. 1, no. 2, pp. 223-225, 2009.

[2] A. Nehra, R. Meena, D. Sohu, and O.P. Rishi, "A Robust Approach to Prevent Software Piracy, in Proc. Students Conference on Engineering and Systems, pp.1-3, IEEE, March 2012.

[3] S. Mumtaz, S. Iqbal, and I. Hameed, "Development of a Methodology for Piracy Protection of Software Installations, in Proc. 9th International Multitopic Conference, pp.1-7, IEEE, Dec. 2005.

[4] Asifullah Khan, Anwar M. Mirza and Abdul Majid, "Optimizing Perceptual Shaping of a Digital Watermark Using Genetic Programming", Iranian Journal of Electrical and Computer Engineering, vol. 3, pp. 144-150, 2004.

[5] J. ZHU, J. Xiao, and Y. Wang, "A Fragile Software Watermarking Algorithm for Software Configuration Management", in Proc. International Conference on Multimedia Information Networking and Security, vol. 2, pp. 75-78, IEEE, Nov. 2009.

[6] C. Shengbing, J. Shuai, and L. Guowei, "Software Watermark Research Based on Portable Execute File", in Proc. 5th International Conference on Computer Science and Education, pp. 1367-1372, IEEE, Aug. 2010.

[7] F. Donglai, C. Gouxi, and Y. Qiuxiang, "A Robust Software Watermarking for jMonkey Engine Programs", in Proc. International Forum on Information Technology and Applications, vol. 1, pp. 421-424, IEEE July 2010.

[8] Z. Shao-Bo, Z. Geng-Ming, and W. Ying, "A Strategy of Software Protection Based on Multi-Watermarking Embedding", in Proc. 2nd International Conference on Control, Instrumentation and Automation, pp. 444-447, IEEE, 2011.

[9] Y. Zhang, L. Jin, X. Ye, and D. Chen," Software Piracy Prevention: Splitting on Client", in Proc. International Conference on Security Technology, pp. 62-65, IEEE, 2008.

[10] N. F. Maxemchuk, "Electronic Document Distribution," AT&T Technical Journal, September 1994, pp. 73-80. 6.

[11] N. F. Maxemchuk and S. Low, "Marking Text Documents," Proceedings of the IEEE International Conference on Image Processing, Washington, DC, Oct. 26-29, 1997, pp. 13-16.

[12] S. H. Low, N. F. Maxemchuk, and A. M. Lapone, "Document Identification for Copyright Protection Using Centroid Detection," IEEE Transactions on Communications, Mar. 1998, vol. 46, no.3, pp 372-381.

[13] S. H. Low and N. F. Maxemchuk, "Capacity of Text Marking Channel," IEEE Signal Processing Letters, vol. 7, no. 12 , Dec. 2000, pp. 345 -347.