Software Encryption and Software Authorization Management Based on Sentinel

Jinzu Wang¹, Zi Wang² and Tao Li³

¹ Shaanxi Xueqian Normal University, Xi’an, Shaanxi, China
² Zhongxing Telecommunication Equipment Corporation, Xi’an, Shaanxi, China
³ Xi’an University of Posts and Telecommunications, Xi’an, Shaanxi, China

wang@xajsc.com

Abstract. In this paper, based on Sentinel encryption tool, according to the important functions and publishing methods that Smart-Color medical image acquisition system needs to protect, combined with software authorization mode, the S-Color Medical Image Acquisition System is encrypted. The steps and methods of encryption are introduced in detail.

1. Introduction

Smart Color Medical Image Processing System (Short for S-Color) is a product that I developed for a company and is included in the horizontal project of our University. This scientific research project has been completed and pushed to the market, which has produced better social benefits. I'm going to talk about some of the work we’ve done on the protection of software's intellectual property, and I'm looking to help other Software developers and software companies.

1.1. Main Functions and Requirements of S-Color

S-color is software for the medical imaging department. The basic function is to convert black and white B-super images into color images, which can better improve medical staff's inspection and confirmation of tumor diseases. The main functions are:

(1) Registration of Medical Record
(2) Image Acquisition
(3) Diagnostic Processing
(4) Processing of Reports
(5) Print Reports

When we developed software, we creatively proposed the idea of distinguishing the back area from the lesion, and this technology achieved the effect of separating the suspected area from the entire background. It has a powerful combination of background modulation and pathological area search. The search of the lesion area is carried out by gray step, the color of the lesion can be adjusted and the chromability can be adjusted. It can be found that the tissue variation is difficult to detect because the gray scale is close, and the distribution of suspected regions and the outline of edges can be effectively observed.

Curve mapping function, this function to achieve the stratification of the gray order. Curves can be adjusted in real time, and the effects can be feedback in real time on the video. There are standard templates in the curvilinear template library, and medical personnel can apply them directly to the current video. This method is relatively fast and can be fine-tuned on the basis of the corresponding template. Curve templates can be added by themselves and can be named and saved, and will be used...
This software is aimed at small and medium-sized hospitals and rural hospitals, including some individual clinics. Intellectual property protection awareness is relatively weak. In various ways, they will use it in an unauthorized environment, which will cause greater losses to copyrighted developers. How not only can the product be encrypted and protected, but also enable the vendor to easily arrange the software, and also allow the customer to obtain a good experience of use. There will be no habit changes and simple and convenient software upgrades during the use process. We selected a number of products for trial. Tests were conducted in various environments, and various assessments were conducted. Finally, the Gemalto (Beijing) Information Technology Co., Ltd.’s sentinel series of products were selected.

1.2. Introduction to Sentinel Series Software Encryption Tools
Software protection is the process of protecting applications or intellectual property rights by combining automated and customized security policies. Protection is achieved by implementing specific security policies, such as wrapping applications in security envelopes or incorporating security measures into application code during development. The more security measures involved, the more complex they are, and the more secure the application is. For more than 30 years, Sentinel Hard Lock series has won the trust of global software suppliers for its high quality and reliability. With the continuous development of software technology and applications, and the evolution of user usage habits and methods, Sentinel also introduced license-based (soft lock), cloud-based and authorization management solutions. From the aspects of design and development, promotion and distribution, order management and usage tracking, it meets the needs of software products.

2. Using Sentinel to Encrypt Smart Color Medical Imaging System (The main program file name is S-Color.exe)
S-Color is for all kinds of customers, and their needs are different. First of all, there are different types of customers and different needs. Then make different authorization plans for different customers. We collate the types of customers as follows:

![Figure 1. Hospital Client Types Using Software](image)

Sentinel LDK is a role-based system, and the tasks you can perform depend on the Sentinel LDK administrator for you. There are four roles:

1. **Product manager role**: This role is usually the product manager responsible for deciding which product components to protect (referred to as work in Sentinel LDK). Can use these components to define the method of the product and the authorization structure of the product.

2. **Development Engineer role**: This role is usually a software engineer responsible for using Sentinel LDK Envelope or Sentinel EMS. Licensing API protects software and performs other development-related tasks, such as generating Sentinel runs.

3. **Customer service staff role**: This role is responsible for manually activating the product.

4. **Authorized manager role**: This role is responsible for defining and managing customer authorization (orders).
2.1. Defining Features (Product Manager)
A Feature is an identifiable functionality of a software application that can be independently protected or licensed. In Sentinel LDK EMS, a Feature may be an entire application, a module, or specific functions, such as Image acquisition, Diagnostic Processing, and Print reports in S-Color.

Features are typically defined by the Product Manager based on business decisions, and are then implemented by the software engineers.

To launch Sentinel EMS:
1. From the Start menu, select Sentinel LDK EMS is launched in a Web browser. In the User ID and Password fields, type password, click Login.
2. To define the two features:
   1) S-Color All, In the Feature ID field, type 10. (This feature contains all functions)
   2) S-Color 2, In the Feature ID field, type 20. (This feature does not contain Diagnostic Processing function).

2.2. Defining Product (Product Manager)
A Product is a licensing entity that represents one of the vendor’s marketable software products. The Product is coded into the memory of a Sentinel key and contains one or more Features.

License terms are defined for each Feature in a Product. Like Features, Products are defined using Sentinel LDK EMS. Typically, this function is performed by the Product Manager, and implemented by the software engineer. Defining four Products With an Execution-based License Launch, then Click Save.

1) S-color Frequency
2) S-color Full
3) S-color Time
4) S-color Trial.

2.3. Protecting the S-Color Program (Development Engineer)
To prepare for protection:
1. In the Sentinel LDK Envelope Project pane, select Programs.
2. Click Add Programs in the top right of the Programs pane. The Add Programs window is displayed, showing the contents of the \Vendor Suite\samples folder.
3. Select S-Colore.exe and click Open. S-Colore.exe is now listed in the Programs pane.
4. In the Project pane, under Programs, select S-Colore.exe. The Display pane lists the Protection Details.
5. In the Project pane, under Programs, select S-Colore.exe, then in the Display pane, click Protect Selected. A message informs you that the protection process is running.
6. Click Close when Sentinel LDK Envelope notifies you that the protection process has completed.
2.4. Creating and Distributing an Entitlement for Sentinel HL-Protected Software (Customer service staff or Entitlement Manager)

To produce a Sentinel HL key-based entitlement for a customer:

1. From the function bar in the Sentinel LDK EMS screen, select Customers. The Customers screen is displayed.
2. Click New Customer. The Create Customer screen is displayed.
3. Add customer lists and customer information.
4. Ensure that the type Company is selected.
5. In the Company Name field, type Trial Customer.
6. In the Contact Information pane, enter your own (or any other) name and e-mail information.
7. Click Save. The new customer is listed in the Customer screen.
8. From the function bar in the Sentinel LDK EMS screen, select Entitlements. The Entitlements screen is displayed.
9. Click New Entitlement. The Create New Entitlement screen is displayed.
10. Select the companies from the list of customers that appears. The full name of the customer is displayed.
11. In the Product Details pane, click Add Product.
12. In the Product Selection screen, select the check box for S-Color-Trial and click Add Product to Entitlement. The S-Color-Trial Product is added to the Product list.
13. Select the check box for S-Color-Trial. Select the corresponding Feature ID (2.1 Defining Features) according to the type of customer.
14. Repeat (13), (14) steps, Select the check box for S-Color-Full, for S-Color-Year, for S-Color-Lite.
15. Complete the authorization of four types of customers.

2.5. Using an Application with a Sentinel HL Key (Customer service staff or Entitlement Manager)

Using an Application with a Sentinel HL Key. When customer service staff need to provide corresponding products to customers of a certain demand, Customer service staff or Entitlement Manager lock the license to a Sentinel HL key:

1. Connect the User Sentinel HL key to which you want to burn the Entitlement to your computer.
2. Click Produce. The Produce Sentinel HL Key screen is displayed.
3. In the list of keys, select the check box for your Sentinel HL key.
4. Click Burn. A graphical display indicates that the burn is taking place. Upon completion,
success message is displayed.
(5) Close the Update Physical Key screen.

3. Conclusion
This paper combines software encryption with authorization management. According to the types of software customers and the high security, high strength and convenience of sentinel products, it achieves a convenient, flexible, reliable, stable and easy to upgrade online encryption scheme, which is mainly embodied in the following aspects:

(1) S-Color software can be used only by inserting Sentinel hardware encryption lock, which effectively prevents users from using it under unauthorized conditions and protects the intellectual property rights of developers.

(2) According to different customer situations, the software is set up in different ways of use, and according to the type of customer, it is set up as follows: Trial edition, permanent edition, limited time edition (time period), limited number of times (rental customers), subscription customers;

(3) Encryption process only needs technical engineer to encrypt once, and the later distribution mode is authorized by sales department according to customers.

(4) The upgrading of software is automatically collected and reminding customers by the system.

(5) Customer software use authorized updates can be easily set by the login authority of the after-sales department. Online updates do not require development technicians to make changes.

4. References
[1] Yang wei, Xu quansheng, Wang hong: Design and implementation of software encryption lock based on DSP: Journal of Shenyang University of Technology: Vol.29 No.3(2007)
[2] Wei guangcun, Sun zhonglin, Xu yanni: Research on software encryption technology: Fujian Computer: Vol. 9(2006)
[3] Jiang Bing: Selection and design of a software encryption scheme: Information Technology: Vol. 12(2010)
[4] Tong xiaoyun, Wang zhu, Du yu, Yue yinliang: Research on hybrid encryption technology based on software security: Computer Engineering: Vol.30, No.23 (2004)
[5] Fang dingyi, Zhang hengtang, Zhanyong,Chenxiaohong: A virtualization software protection method against semantic attacks: Advanced Engineering Sciences: Vol.49.No.1 (2017)
[6] Huang dong, Li yewang, Zheng chi: Software protection method based on Trusted Computing and SGX: Communications Technology: Vol.50, No.10 (2017)
[7] Li shiqun, Wang kunsheng etc.: Effectiveness evaluation of software protection based on Fuzzy Analytic Hierarchy Process, http: // kns.cnki. net/kcms/detail/ 61. 1450. TP. 20171205. 0904. 028. html
[8] Mi qi, Zong junjuh etc.: Software protection technology: Ordnance Industry Automation: (2018.07)
[9] Cheng guisun, Li qian: Research on the impact of software protection on the bilateral pricing strategy of software platform providers: Chinese Journal of Management Science: Vol.24. No.9
[10] Cao weizheng: Computer software security analysis and defense strategy research: Internet Security: New China Communications (2016.12)
[11] Fan yuhong: Computer software security analysis and defense strategy research: Internet Security: New China Communications (2016.12)
[12] Sun wei, Xue linfeng, etc.: Review of software legality protection technology and Application: Information security research: Vol.3, No.5
[13] Shang kaiquan: Application of a hybrid encryption scheme in software authorization Electronic Technology & Software Engineering (2017)
[14] Li long.: Discussion on protection method of computer software: Computer programming skills and maintenance (2017.03)
[15] Liu sicheng: Analysis of computer software protection methods: Communication design and Application: No.24 (2017.12)
[16] Wang caimei, Liu wenjie: Software protection based on elastic protection mechanism Journal of Hefei University: Vol.34. No.5