Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique

Sheng Cao Zheng Chen Xuandong Sun

Chengdu Institute of Computer Application, Chinese Academy of Science, Chengdu 610041, P. R. China

Abstract

To protect printed information from being forged, tampered with or misappropriated, a logic signing technique was developed, which was applied to anti-counterfeit authentication system so as to intelligently make printed information verified quickly, conveniently, precisely and feasibly. The technique is independent of what physical equipment used, the system based on the technique is characteristically open and secure cryptographically due to the logical association between synthetic information and encrypted verification information, which essentially changes the mode of the existing anti-counterfeit techniques for printed information. PMI is bestowed to resolve the issue of management of crpto-keys as a convincing complementarity for the authentication system based on the logic signing technique.

Keywords: Anti-Counterfeit, Logic Signing, Printed Information, PMI

1. Introduction

Nowadays, printed information is used most widely in the world. A certificate (license) is an official written or printed statement that may be used as proof or evidence of certain facts. So far all kinds of soft certificates can be very easily forged, juggled, and embezzled, which greatly weakens their authority and credit system. Obviously this fact poses a growing threat to the social order and has become a critical problem. After "911Affair" in America, the anti-counterfeit technique of certificates is thought much of in most countries. The American government has been investing a great deal on the research on the security system of anti-counterfeit. And in China, feigned soft certificates are omnipresent and disturb the social order as well as endangering the national credit system seriously. Therefore, looking for the new anti-counterfeit techniques used to protect the information in soft certificates are in increasingly intensive need [1].

The current anti-counterfeit methods of soft certificates are multiplex in original carrier and anti-counterfeit mechanism. Diversified subjects such as physics, chemistry, biology, electronics and optics are imported into anti-counterfeit study, which not only show the idiographic fascination of anti-counterfeit fields but also lay out the superiority of each subjects. Concretely speaking, the means of anti-counterfeit includes:

1) Traditional physical means, by which mimeograph prints or steel seals are stamped onto certificates [2];
2) Traditional physiological means, by which photos or fingerprints are stuck on certificates [3];
3) Complicated physical means, by which the presswork with shading or laser anti-counterfeiting tags serve as the media of certificates [4];
4) Electronic means, by which registered serial numbers or bar codes are printed in certificates for retrieval [5].

However, there exist several disadvantages in those mentioned anti-counterfeiting techniques of soft certificates in varying degree. For the physical and physiological means, the feigners can make use of modern high-techs to forge public prints, replace photos and imitate the materials of certificates. As a result, the certificates can be feigned quite easily. And for the latter two means, the limitation lie in the high cost of establishing and supporting an enormous network database system and high reliance on infrastructures and environment; meanwhile the research into the security techniques of database and remote access has been a long-term topic that is imperative to be intensified.

Besides printed information, the portable electronic storage devices like IC cards [3] are being employed in a growing domain of applications. But as a matter of fact, IC cards can't completely take the place of some important certificates like diplomas due to their characteristics and IC card-based system doesn't automatically allow users mobility [6]. In addition, the security mechanisms inside IC cards must be improved, which inevitably increases the cost of using IC cards. Obviously the costs and inconveniences outweigh the potential benefits of using IC cards in some canaries [6].Therefore, it still

imperative to research and develop anti-counterfeit technologies for certificates under the situation in certain fields.

In the face of the current critical problem of certificate counterfeit, we developed a logic signing technique for printed information against counterfeit and applied it to the authentication system of some certificates, which makes their verification feasible, quick, convenient, and precise. In the proposed technique, the text of a certificate is transformed into graphic codes (namely digital stamps) so that its content can be protected by so-called 'digital fingerprints'. Furthermore, we have designed and implemented the prototype of the authentication system based on this technique. Unlike other anti-counterfeit techniques of automatic identification, in this system, the private information of holders are embedded in the master-secondary prints in their certificates, and the logical restriction relation between the digital seals was in a position to put an end to be counterfeit. The character of the certificate that it is incapable of counterfeiting is ruled by the logical configuration of the possessor's character information. It is independent of the device so that the technique criterion can be an open system. What's more, this method replaces low-cost complicated logical operation instead of the techniques complexity of the physical device. It also replaces the technique which was concerned with sense organs of human being by the electronic information process. The verification is regardless of database and internet so that this method is low-cost.

2. Intelligent Anti-Counterfeiting Mechanism

At present one of common anti-counterfeiting methods is to print feature information of licit holders in their certificates. However, it's not difficult to forge an ordinary soft certificate because there is merely sociological and physiological feature information in it. Thus in this proposed mechanism, the information of holders is added to make it hard to imitate but easy to validate the features of licit holders, which can effectively protect the licit certificates from being used by unlawful holders. It is inexpensive and cryptographically secure for printed information.

The authentication mechanism utilizes the logic signing technique to protect synthetic information on a certificate. The synthetic information is composed of public information and the legal holder's private feature information. The former consists of common information about the manufacture of the certificate and the legal holder's public feature information (say name, age, stature, blood type, photo, fingerprints and other physiological features). The latter are facts or knowledge sets only known to legal holders (say his or her hobbies, question answer, password, etc). Particularly the private information is transformed into machine-readable-only symbol strings after being encrypted for safeguard against falsification.

To make synthetic information maintain a strict logic association with verification information, we make use of the mathematical model, based on a combination of a hash function and encryption/decryption function of modern cryptographic techniques. That is, textual data is hashed using a cryptographically secure hashing algorithm. And the functions coupled with encryption/decryption key map synthetic information to verification information, which indicates that the association between two kinds of information is quite easy to be established with encryption key and couldn't be deciphered without decryption key. Verification information aims to protect and check the integrity and authenticity of synthetic information, thus reducing the verification cost. As a result, the content of the certificate is difficult to be imitated and easy to be validated. Moreover, any illegal modification of synthetic information will certainly make it disassociated with verification information and this disassociation can be checked quickly.

Anyhow, a certificate can be given an instant and precise identification whether it's forged or tampered utilizing the three digital stamps, whose uniqueness is totally dependent on encryption key as well as the logic association between synthetic information and verification information. It's such an open authentication system that all the utilized technologies and standards of technical equipment are kept public except the keys and the legal holder's private information. In spite of that, anybody couldn't forge, tamper with or abuse others' certificates without decryption key. And the key points of authentication mechanism mentioned above were patented [7].

3. Design of Authentication System

3.1. Process of Manufacture

The information on a certificate is classified into: 1) hidden information (namely encrypted private information), which couldn't be encrypted or decrypted without authorized keys; 2) synthetic information (including public information and hidden information), which is transformed into human-readable textual message; 3) verification information, which is generated from synthetic information.

Besides human-readable textual message, three

machine-readable digital stamps(master stamp, slave stamp and private stamp),which hold synthetic information, verification information and hidden information respectively, are encoded and printed as graphic codes onto the certificate. Consequently, different verification information is generated from different encryption keys and textual messages, which results in different slave digital stamps. That is, the logic association among information inside the digital stamps varies with encryption keys, thus forming a security mechanism in which textual message, digital stamps and holders' privacy are associated highly closely. Fig.1 depicts how to generate three digital stamps.

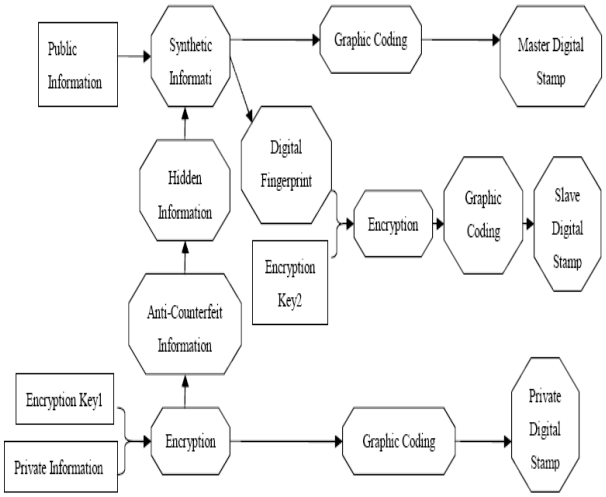

Fig. 1: Generating digital stamps.

In this system, the digital stamps can be printed using a high-density graphic code zymology capable of storing kilobytes of information in a single symbol and unlimited data in multiple symbols [8]. We may explain why we use graphic codes for the information carrier. With the development of modern technology, which presses for the technique of graphic code to express more information in finite geometry room so that it can satisfy the kinds of information demand .To achieve this aim, we should get rid of the redundancy in vertical direction of 1-D graphic code and think out multidimensional information distributing graphic code. Multidimensional graphic code is an important advance in digital front port technique and automatic identify field. It can embody the whole information of President Lincoln's photo and the Declaration of Independence in multidimensional lattice graphic that is as small as a thumb, making it a micro moving database.

The multidimensional graphic code has several advantages: big information quantity, wide coding range, strong error-correcting ability, and high decryption reliability. And it can encrypt information repeatedly; the internal information of multidimensional graphic code cannot be counterfeited without a key. Through the cryptograph information, it can be only read in the condition of gaining the key, which increases the difficulty of forgery and enhance the anti-counterfeit performance. In addition, multidimensional graphic code can be managed without database, which is very flexible and convenient. Using graphic codes is that possibly a large amount of easily-and accurately-read data can "ride" with the certificate. And it's very hard to counterfeit the encrypted message held by graphic codes without encryption keys because it can be deciphered only with decryption keys. But it's not an effective anti-counterfeit approach to merely print graphic codes directly in a certificate unless they are coupled with a good security mechanism.

Multidimensional graphic codes mainly include two-dimensional [9] and three-dimensional bar codes [10] that are technologies of automated data collection, storage and transmission. The former, composed of PDF417 [9], Data Matrix [11] and Maxi code [12], has been accepted as a standard by ISO and IEC and used widely in an increasing number of countries. The latter has a much bigger capacity, in which even audio and video information can be stored. Although three-dimensional bar codes are not standardized at present, digital stamps are printed with three-dimensional bar code symbiosis in this authentication system.

3.2. Process of Verification

Digital stamps are used for verification as the method mentioned above, with the criteria of perfect security that a certificate is valid if there is an established logic association among synthetic information, private information and verification information. That is, the security of a certificate stems from the fact that changing a single bit of the textual message or altering the photo causes a global change in the bar-code that appears to be random without the knowledge of the issuer's keys.

During the verification process, a verifier first scans the digital stamps in the certificate with a hand-held bar code reader, then decodes the information inside them and computes it. If computed results are matched and the information inside the master digital stamp is identical with the text of the certificate, it is judged to be accurate and valid, otherwise it's not.

To prevent illegal possession by an impostor, the verifier may decode the private information stored inside the private stamp utilizing authorized decryption key, and check whether the information

provided by the practical holder is identical with it by questioning him or her about private information. It's pretty easy to determine if the certificate is misappropriated or not according to the offered answers due to the fact that the legal holder surely knows his or her own private information very well. As a result, an impostor is incapable of possessing a certificate illegally even though he forges the photo or impersonates the legal holder by any high-tech means for the reason that he couldn't obtain private information without authorized keys. Fig.2 illustrates the verification of a certificate.

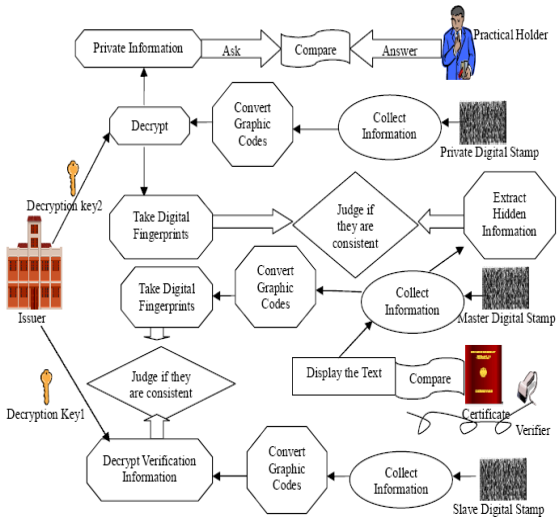

Fig. 2: Verifying a certificate

Especially, even though the certificate was lost or stolen, it is difficult to imitate and easy to identify a legal holder's feature information through the legal holder's private information.

4. An Example of Application

Let's give an example to set out the advantages of logic signing technique for printed certificates.

Firstly, in accordance with asymmetric cryptosystem ,we should assign two keys say K_p （encryption key）and K_v (decryption key)for the manufacturer and verifier respectively. Besides, the technological schemes as well as standards of technical equipment used during manufacture and verification ought to be issued. The approach of manufacturing and verifying the certificate are shown as follows: After select a template of manufacturing a certificate, input message M(including public information and private information),and then extract the message digest with HF(M) from hidden information that is encrypted with EF（S，K_p）, and combine it with public information to manufacture synthetic information X. Afterward, extract message digest S with HF(X) from synthetic information X, and encrypt it with K_p and EF（S，K_p）again to manufacture verification information which serves as validating the certificate afterward. The digital stamps (slave, master and private) are generated from verification information, public information and hidden information respectively using GCP. And three kinds of information mentioned above are typeset and printed. Thus, a certificate is produced.

During verification, a verifier first chalks up synthetic information, private information and verification information by scanning the digital stamps in the certificate with a graphic code reader. Then comparing the human-readable text with synthetic information A displayed on the screen. If any unconformity is found, the certificate is judged to be invalid. If not, the verifier chalks up checking code V_1 and information B by decrypting the information inside the slave and private digital stamps respectively. Simultaneously, checking code V_2 is chalked up by extracting message digest from information AB (a combination of A and B) with HF. If V_1 is equal to V_2, the certificate is judged to be valid, otherwise it's not. It's significant to point out that the verifier ought to inquire practical holder according to information B (that is kept secret from the holder) displayed on the screen and identify whether the holder is an impostor or not if necessary.

Fig.3 illustrates the result of verification.

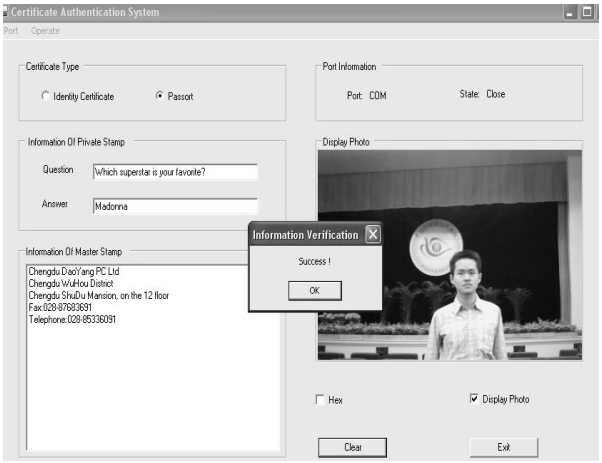

Fig. 3:The result of verification.

5. Management of Keys

Our discussion above has not make out how to manage the keys efficiently. And then we adopt the PMI technique to solve the issue. PMI (Privilege Management Infrastructure) [13] is a criterion put forward by IETF, which separate the management right of users from the symbol of individual. PMI is a

helpful tool that it can carry out the key management unitary based on the attribute certificate of X.509v4 which was proposed in the year 2000.PMI could replace traditional accessing control policies, such as MAC,DAC and so on. The very merits of PMI consist in the independency of concretely application. In other words, it can provide high potent and unitive authorization management mechanism for kinds of applications, which is capable of exerting the variability, adaptability and low cost in accessing control application. In modern application environment, for example, distributing electronic system, work stream and otherwise, we can abstract a suit of accessing control rules without exception so as to realize the security exchange visits and currency.

Attribute certificate (AC) is the key technique of PMI, we make use of it to manage authorization information of holders, and the PMI model is set up based on the attribute certificate. We bring forward the RLBAC (role level based accessing control) for attribute certificate to bring into play. The course of RLBAC to support attribute certificate is as follows: firstly, award some attribute certificates which used to define the roles each other; secondly, award one attribute certificate for the ultimate user and appoint one or several roles for him. A holder can hold a number of attribute certificates, which can be awarded by different issues, but each attribute certificate corresponds to the only identification certificate. The RLBAC designates distinct roles and the relationship among them. The relationship chart can be a tree or loop. A simple general RLBAC is shown in Fig.4.

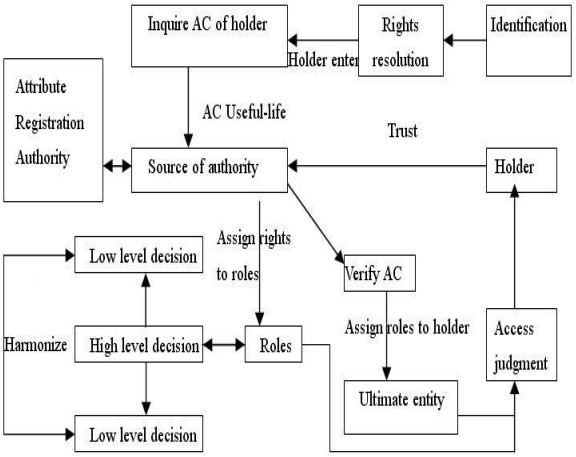

Fig.4: configuration of RLBAC.

The holder who needs identification is supposed to get across the entrance of rights resolution first, and then the useful-life of AC held by the holder may be checked carefully. Once the source of authority has verified it correctly, it will be delivered to attribute registration authority for keeping in archives; and the next process is to verify the AC to assign roles to holder. If this is all right, the ultimate entity could be judged whether the holder can be granted to the crypto-keys or not. In succession, the source of authority will assign rights to roles, and the different level decision can be harmonized by their different roles.

6. Conclusions

The reason why we introduce the novel, low-cost and efficient authentication system based on a logic signing technique for printed information is found on the judgment that, the counterfeit certificates do a lot of harm to social life and it is an urgent task for most countries to solve this critical problem effectively. So in the authentication system above, coupled with three digital stamps, it can give an instant and precise identification whether a certificate is forged, misappropriated or tampered with so as to assure its security. It's noted that the verification cost of this system mainly counts on the complexity of logic computation in its security mechanism. Whereas, the amount of data inside a certificate is usually so small that the computation cost is low enough to make the application of this technique to certificate anti-counterfeit feasible.

This instructive new approach commands a fine view of the safeguard of printed information. Besides, it can be applied in other anti-counterfeit schemes. It's a paradigm to develop intelligent anti-counterfeit mechanism of both printed and non-printed information. For instance, it can be utilized to improve the security mechanisms inside variety of portable electronic storage devices and the like.

References

[1] H.B. Shen, M. Zhang, A dialogue with those persons who forged soft certificates. *Reporter Observation*, 7:28－30, 2000.

[2] S.M. Tony, Bar Codes Sweep the World .*Invention and Technology*,pp.56-63,Spring 1993.

[3] N. Matsuo, K. Shimonhara, H. Matsui, etc., Personal Telephone Services Using IC-Cards. *Communications Magazine IEEE*, July 27(7):41-48, 1989.

[4] M.C. Chu , L.L. Cheng and L.M. Cheng, Magnetic Cards, *British Patent Application*, 1994.

[5] V.V. pitsyuga , M. Y. Kolesnikov , and I.V. Kosyak, Protection method for an optical information carrier, *International Conference on Optical Storage, Imaging, and Transmission of*

Information, Proceedings of SPIE, pp. 212-216, February 1997.

[6] D. Chadwick, Smart Cards Aren't Always the Smart Choice. *IEEE Computer*, 32(12):142-143, December 1999.

[7] X.J. Wang, Authentication mechanism of printed information based on a logic signing techqiue. *China Patent:* 1,570,962, January 26, 2005

[8] R.B. Johnston, Alvin Khin Choy Yap. Two-Dimensional bar code as a medium for electronic data interchanges.*Proceedings of 31st Annual Hawaii International Conference on System Sciences*. Kohala Coast, Hawaii, pp.83-91, 1998.

[9] T. Pavlidis. A New Paper/Computer Interface : Two-Dimensional Symbologies. *Proceedings of 15th International Conference on Pattern Recognition.* Bracelona, Spain, 145-151, 2000.

[10] H. Zhu, J. Zhou, H. Li, 3D barcode preprocessing scheme based on image recognition. *Proceedings of SPIE, Second International Conference on Image and Graphics.*Wei Sui, 651-655, July 2002.

[11] D.G. Priddy, R.S. Cymbalski. Dynamically Variable Machine-Readable Binary Code and Method for Reading and Producing. *U.S. Patent: 4,939,354*, July 3, 1990.

[12] D.G Chandler, E.P. Batterman, G.Shah. Polygonal, Information Encoding Article, Process and System. *U.S. Patent*: 4,896,029, January 23, 1990.

[13] Chadwick, An X.509 role-based privilege management infrastructure.*Business Briefing: Global Infosecurity* , 2002.