CHAPTER 5

Security Verification Systems for Digital Media

Jianping Chen

The development of photocopy technology and manufacturing technology provides many possible ways for adversaries to fake and modify paper-based legal documents such as certificates, licenses, and invoices without being detected. It makes managing the paper-based legal documents a challenging task. Hence, managing and authenticating digital legal documents becomes a practical and requisite task in daily life. To relieve the efforts of document management and authentication, in this chapter, we propose two security verification systems for digital media: the public key encryption based system and the Chinese Remainder Theorem (CRT) based system. Both systems are able to produce and verify secure electronic documents while keeping the owners' legal privacies secret. Throughout the chapter, we present and analyze the background, structure, security performance, and implementation of the two schemes.

Jianping Chen
Institute for Infocomm Research
Fusionopolis, 138632 Singapore
e-mail: jchen@i2r.a-star.edu.sg

Editors: C.W. Ahn, M. Ali, M. Pant, *Embodying Intelligence in Multimedia Data Hiding*
DOI: 10.15579/gcsr.vol5.ch5, GCSR Vol. 5, pp. 83-99, 2016

©The authors; licensee Science Gate Publishing P.C. - CC BY-NC 4.0 International License

5.1 Introduction

Organizations have traditionally relied on paper filing systems for document storage and retrieval. However, paper records are extremely difficult to manage because they have to be stored in and retrieved from only one place. Electronic document management systems solve many of the storage and retrieval problems inherent in paper filing systems, while reducing business costs simultaneously.

The development of photocopy technology and manufacturing technology makes managing and authenticating the paper-based legal documents such as certificates, licenses, and invoices a challenging task. It also provides ways for adversaries to fake and modify paper-based legal documents without being detected.

To conquer illegal actions, attempts have been made by researchers and engineers. In China, lots of authentication sites have been set up for verifiers to authenticate legal documents such as certificates, professional licenses, invoices and etc. To authenticate a certificate, the verifier has to log onto the official web site, key in basic information such as identification (ID) number, name, date of birth, and etc. If the presented materials match those stored in the database, the authentication succeeds and more details of the certificate prompted to the verifier.

Obviously, the above and similar solutions are far from complete and perfect. The systems are in nature still paper-based and within the scope of paper documents: the authentication system works like a judge of the paper certificates. To authenticate certificates and licenses from different sources, the verifier has to visit different websites. Even worse, the kind of system provides no provision on privacy for the document owners at all. Since the authentication site is open to public, anyone is able to retrieve the private information from the so-called authentication site easily by feeding basic materials collected from other channels. From the point of privacy, the kind of system is a failure. It is really inappropriate and definitely not allowed to hook the sensitive materials such as transcripts and professional licenses on the public websites.

The use of watermarking, sometimes called data hiding, is almost as old as paper manufacturing [6, 7]. Paper watermarks have been in wide use since the late middle ages. The earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock. In more recent times, watermarks have been used to certify the composition of the paper. Today, most developed countries also watermark their paper currencies and postage stamps to make forgery more difficult.

The digitization of our world has expanded our concept of data hiding to include immaterial, digital impressions for use in authenticating ownership claims and protecting proprietary interests. A digital watermark is a digital signal or pattern inserted into a digital document, e.g., text, graphics, or multimedia presentations. It is a form of electronic watermark much like the corporate logos used by the cable television industry to identify the source of the program.

The art and science of data hiding are sometimes also called steganography. A great number of data hiding or watermarking algorithms have been proposed so far [2, 11], both in grayscale/colorful field and binary field, in space domain and transform domain. Cryptography techniques have also been utilized and exploited to achieve security and privacy purposes [1, 3, 5, 10].

In this chapter, we propose two Secure Electronic Document (SED) schemes for legal document issuing organizations. Both systems are able to issue verifiable electronic document while keeping the privacy secret. The first system is built up by utilizing public key encryption technology and data hiding technology, while the second one is created on the base of the Chinese Remainder Theorem (CRT). Both systems can be used to issue legal documents such as electronic certificate, electronic transcript, digital license, digital invoice, purchased audio clip, purchased video clip, so on and so forth. Throughout the chapter, we present and analyze the principle, system architecture, security performance, and implementation for both systems.

The rest of the chapter is organized as follows. In Section 5.2, we present the background of watermarking technology, where we describe the basic techniques in image watermarking, video watermarking, and audio watermarking. In Section 5.3, we present and analyse the principle and architecture of the public key encryption based secure document system. In Section 5.4, we describe the CRT based system. In Section 5.5, we do a simple comparison between the two schemes. Finally, conclusions are drawn in Section 5.6.

5.2 Watermarking Technology

Digital watermarking utilizes embedding techniques to hide information, watermark, into media such as image, audio video, and etc. Two distinct watermarking technologies are available for distinct purposes: robust watermarking and fragile watermarking. In robust watermarking, detection can be accurate even under serious modification. In fragile watermarking, however, detection fails even though a minor modification to the media has happened. Robust watermarking has been widely used in copyright protection, pirate tracking, and copying protection. Fragile watermarking has been exploited for the purposes of authentication, cover-up communication, right control and etc.

In signal processing, embedding is a process of adding feeble signal to strong background signal. Three points and aspects are usually concerned and discussed in watermarking technology: capacity, security and robustness [7]. In reality, a balance must be achieved among the three aspects.

Capacity describes the carrier medium's room available for the watermark. For example, if the least significant bits (LSBs) of the pixels are used as the embedding position, the number of pixels determines the capacity.

Security indicates the watermarking system's ability to deter the eavesdropper's detection of the hidden information. In increasing order of performance's difficulty and efforts, three levels of detections exist: 1) Determining whether a watermark is embedded; 2) Estimating the length of the watermark; and 3) Extracting the exact watermark.

We call a watermarking robust if the watermark could be detected reliably from the watermarked medium. On the other hand, we call the watermarking fragile or imperceptible if the watermarked medium is perceptually identical to the original. Robustness refers to the amount of modification the watermarked medium can withstand before an adversary can destroy hidden watermark. Apparently, the terminology ro-

bustness is used to describe robust watermarking.

In addition to the above three aspects, transparency or fidelity is another important point that needs to be carefully considered when we design a watermarking method. Transparency or fidelity is defined as the perceptual similarity between the original medium and the watermarked version. Watermarking should not introduce sensible distortions to the carrier medium as the level of distortions will decrease the carrier medium's commercial value. The embedded watermark cannot be perceived by human only if the signal's intensity is not higher than the contrast restriction of human visible system and the apperceive restriction of human audio system.

5.2.1 Digital Image Watermarking

Digital image watermarking is to embed messages into digital images. According to working domain, digital image watermarking is classified to spatial domain and frequency domain. It is similar to time domain and frequency domain of timed signals.

In spatial domain, watermark is embedded in the source image by simple addition or bit replacement of selected pixel positions. As a digital image is an array or a matrix of square pixels arranged in columns and rows, spatial representation of an image is the function of space involving horizontal coordinate and vertical coordinate. Pixels of binary, gray scale or colour images are used almost directly as embedding positions without any transform.

A binary image has only two possible values for each pixel. Hence each pixel is represented by 1 bit. A gray scale image contains more than just black and white pixels and each pixel has more information. In a colour image, each pixel is represented by three separate colour channels and it usually requires 24 bits of storage.

We obtain the frequency domain by transforming image from one spatial domain to another spatial domain through Fourier Transform (FT), Discrete Fourier Transform (DFT) or Discrete Cosine Transform (DCT). The FT is a mathematical operation that decomposes periodic functions or signals into the sum of sine and cosine functions. According to Fourier's theory, any periodic function can be performed as a sum of simple sinusoids. The DFT is the discrete version of FT. The DCT is the main tool of transforming an image from spatial domain to frequency domain. It has been widely used in image compression and watermarking.

Generally lower frequencies are more dominant in an image than higher frequencies. If an image is transformed into its frequency components and some of the high frequency contents are discarded, the amount of data needed to describe the image will be reduced while the image quality is almost remained.

The main advantage of frequency domain watermarking is the easy applicability of special properties in frequency domain. Working in frequency domain enables us to apply more advanced properties of the human visual system to ensure better robustness and imperceptibility criteria.

5.2.2 Digital Video Watermarking

Digital video watermarking is implemented by embedding watermark to the positions in the still image of each film frame or the inherent features of the video sequence.

All the image watermarking techniques could be extended to video situation while the latter has additional technique requirements. The large volume of inherently redundant data between frames, unbalance between the motion and motionless regions and real-time requirements in video broadcasting bring up new technical challenges for video watermarking. Pirate attacks through averaging frames, swapping frames, statistical analysis, digital analogue conversion and lossy compressions also make the watermarked video susceptible. Similar to image situation, video watermarking techniques also deal with spatial domain and frequency domain.

5.2.3 Digital Audio Watermarking

Digital audio watermarking involves embedding messages in an audio file. Audio watermarking is very similar to video watermarking. An audio watermark could be embedded to all records prior to the release to signify the information such as the author of the work as well as the user who has purchased the legitimate copy. The auxiliary information for a particular song such as lyrics, album information, small web page and etc. can also be embedded to the audio. Link image and video, audio watermarking methods deal with time domain and frequency domain.

5.3 Public Key Based Electronic Document

There are two distinct encryption algorithms: symmetric encryption and asymmetric encryption. Usually, the symmetric encryption is also called secret key encryption and asymmetric encryption public key encryption.

The symmetric encryption algorithm uses same cryptographic key for encryption and decryption. The cryptographic key is deemed as the piece of private information shared by the entities. The requirement that both encryption and decryption need to access to the same cryptographic key is one of the main disadvantages of the symmetric encryption algorithm. The receivers have to use the same or lightly transformed cryptographic key to decrypt the cipher text. Distributing cryptographic keys among the entities poses extra burden to the system. The symmetric encryption can be implemented by using either stream ciphers or block ciphers. Typical symmetric encryption algorithms include Data Encryption Standard (DES), Triple-DES, Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and etc [4].

In contrast, the public key encryption makes use of key pair - a widely available public key and a securely owned private key. The two keys are mathematically related and one-to-one mapped. The ciphertext encrypted with a public key must be decrypted by the corresponding private key and vice versa. Since the public key is not a secret, it can be transmitted in plaintext over public channels. However, the private key must be kept in secret. In comparison with the symmetric encryption, the public key encryption significantly simplifies key distribution. Popular public key encryption algorithms include Rivest-Shamir-Adleman cryptosystem (RSA), Digital Signature Algorithm (DSA), Elliptic Curve Cryptography (ECC), Diffie-Hellman Key Exchange (DHKE), and etc [8].

5.3.1 Principle of RSA Algorithm

RSA is a typical public key encryption algorithm that has been widely used in research, business and industry. The RSA based Public Key Infrastructure (PKI) has seen more and more applications in security world. As RSA is one of the public key algorithms suggested for our SED system, we give a brief introduction to it in the following. Readers are referred to [8] for more details.

Euler's Phi Function$\phi(n)$

If n is a positive integer, then Euler's Phi Function is defined as the number of integers k in the range $1 \leq k \leq n$ for which $gcd(n,k) = 1$, where $gcd(n,k)$ is the greatest common divisor of n and k.

Euler's Theorem

Assume that n is a positive integer. If n and α are relatively prime integers, then $\alpha^{\phi(n)} = 1 (mod\, n)$.

Key Pairs $\phi(n)$

The sender chooses two large prime numbers p and q, and let $n = pq$. He then chooses an e such that $gcd(e, \phi(n)) = 1$ and solves for d where $ed = 1 (mod\, \phi(n))$. The numbers $(n, e)$is the public key and d is the private key.

Encryption

Suppose m is the plaintext, then the cipher text is $c = m^e (mod\, n)$.

Decryption

To get the plaintext, it has been proved that the receiver can compute from the ciphertext by $m = c^d (mod\, n)$.

5.3.2 Creating Electronic Certificate

The public key based SED system uses the private key to encrypt the hash value of a document's media contents, embeds the encrypted results into the trivial positions of the document, and publishes the corresponding public key for authentication. The term trivial place has distinct meaning in different contexts. E.g., in binary images, the trivial places are the qualified pixels selected by embedding algorithms; in gray scale images, the places are the least significant bits (LSBs) of the pixels; in colourful images, they could be the least significant parts of the RGB colour space or YUV colour space; so on and so forth.

Suppose a university is going to issue certificates to a batch of students and colourful images are used as the carrier media. Figure 5.1 illustrates the process of creating electronic certificates. Prior to the issuing, the university designs and generates normal certificates, raw images, with the students' necessary information present. The issuing system then generates a pair of private key and public key for the batch of certificates. For each raw image, the system finds out the trivial places and sets them into initial values, e.g., flip all the LSBs of the pixels to 0's or 1's. At the stage, the system

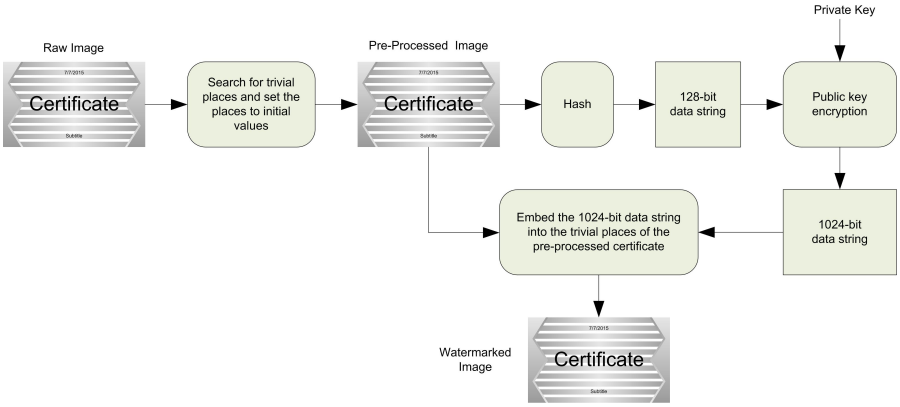


Figure 5.1: Creating electronic certificate.

obtains a pre-processed image. Subsequently, the hash value of the pre-processed image is encrypted with the private key, and the result is embedded into the trivial places reserved earlier. The resultant image is the electronic certificate that could be distributed to the student in any effective way.

Along with distributing the certificates, the university publishes the public key in the official web site accessible to all the verifiers. The private key for the batch of certificates can be kept in a confidential place or simply deleted immediately after the certificates are issued and distributed. The private key completes its task once the certificates have been issued. In verification stage, only public key is involved and the private key is no longer useful.

5.3.3 Verifying Electronic Certificate

If the certificate holder looks for a job or faces situations that require him to demonstrate his education background, he presents the electronic certificate to the examiner in any valid way, e.g., email, memory, or any other effective media. The examiner receives the certificate and stores in any media. Everything is fine if the examiner only wants to view the certificate and keep it as a record. In the situation, the certificate is nothing different from a normal image.

If the examiner wishes to check the authenticity of the certificate, he can download the public key from the official website and proceed as shown in Fig.(5.2). Firstly, the verification system searches for the trivial positions and do two things: 1) Retrieve the watermark, and 2) Set the trivial positions to initial values and obtain a preprocessed image. The watermark is decrypted by using the public key to get the hash value, a data string of 128 bits. On the other hand, the preprocessed image is digested again to get another hash value. The two hash values are compared. If they are equal, the certificate is authentic; or else, the certificate is not true or has been tampered.

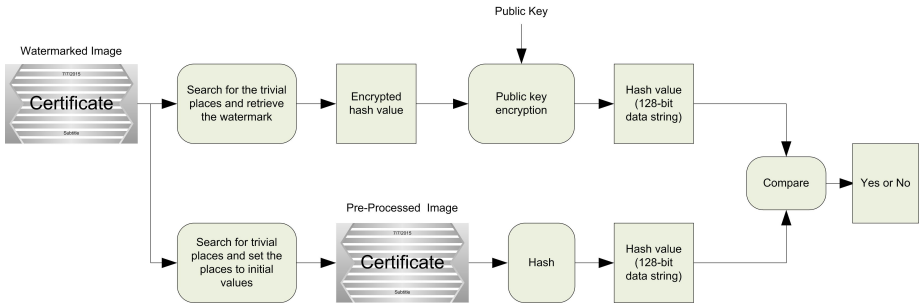


Figure 5.2: Verifying the electronic certificate.

5.3.4 Security Analysis

Security of public key based SED system depends on the security of the underlying infrastructure, namely, the public key encryption algorithm, and the private key. Apparently, the adversary with the private key can issue "true" certificates or modify the certificates at his willing, just like an authorized university officer. Though the possibility is low, the private key in the university office might be leaked incidentally or purposely. It is also possible that the private key is compromised from the public key or other channels. We call such key leaking issues as *key stolen issues*.

In conventional security system, key stolen issues can be resolved by periodically changing the key pairs. However, for the e-certificate system, the method may not work because it is useless to change the key pairs after the certificates are distributed to the students. Tradeoffs must be made between security and convenience. Here we propose two solutions to the issue.

The first solution is to refresh the e-certificates periodically, like what is done in the conventional security systems. In the solution, the university uses one key pair for a large batch of e-certificates with conditions that the certificates expire in a period of time, say, 2 years or 5 years. Once the certificates expire, the holders need to apply for new ones. With the method, the chance of security compromising is greatly reduced while the system sill has acceptable convenience and flexibility.

The second solution is to decrease the number of certificates for which a key pair is applied. If the single key pair is used for the whole batch of certificates, the system risks invaliding a large number of certificates when the system is compromised. To decrease the risk level, the number of certificates encrypted by the key pair should be tuned to the most suitable number. In extreme situation, every certificate uses a different key pair. Hence, compromising of certain key only affects the specific certificate. Refreshing certificates can still be performed in parallel mode to improve the system's security.

5.3.5 Implementation

The issuing system involves key generation and certificate production. Particularly, the following functionalities are included in the issuing system:

- Generating key pair, including private key and public key.
- Generating the e-certificates.
- Distributing the e-certificates.
- Keeping the private key secretly or delete it.
- Publishing the public key on official web site.

The verification system involves authentication and ownership verification. It contains the following functionalities:

- Downloading the public key and the verification tool kit from the official web site.
- Verifying the certificate.

Pictures in Fig.(5.3) illustrate the process of creating a batch of certificates with the public key scheme. Figure (5.3a) displays the certificate template, where common information of the certificates is present and the spaces for each student's particulars such as name, degree and issuing date are left blank; Figure (5.3b) demonstrates the process of tuning formats for the specific particulars; Figure (5.3c) illustrates uploading the required materials for the certificates such as private key, format settings, and database on the students' particulars, and etc.; and Fig.(5.3d) depicts the process of creating certificates; respectively. After the processes, secure certificates are produced.

Figure 5.4 illustrates the process of verifying the electronic certificate. Figure 5.4a displays a secure certificate generated by the system, and Fig.(5.4b) illustrates the process of verifying the certificate, respectively. Prior to the verification, the public key of the batch of certificate is downloaded from the official website. Figure 5.4b shows that the verification is successful and the certificate is valid.

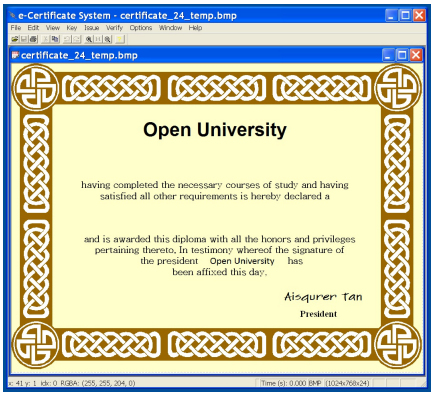
Figure 5.5 illustrates the process of verifying a tampered certificate. As shown in the dashed oval area in Fig.(5.5a), the certificate was tampered with a black dot. Figure 5.5b shows that the verification failed.

5.4 CRT Based Electronic Document

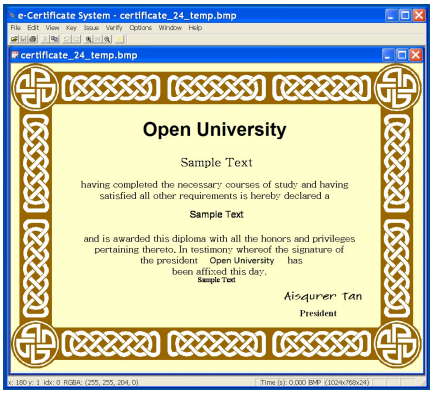
To resolve the key stolen issue in the public key based document system, we propose another scheme for electronic document - the Chinese Remainder Theorem (CRT) based system. As will be seen in the following section, neither private key nor public key is required in the solution.

5.4.1 Chinese Remainder Theorem (CRT)

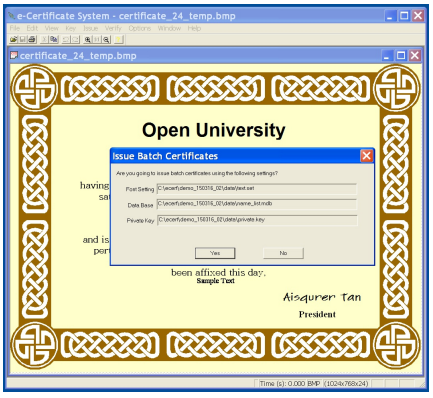
The CRT is a theorem on congruence over integers [9]. It is the oldest remainder problem in the world discovered in a third century Chinese mathematical treatise entitled *Sun Zi Suanjing*. According to CRT, an integer can be completely described and determined by the sequence of its remainders provided that the number of remainders



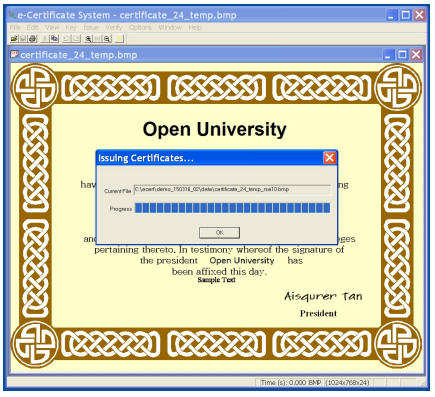
(a) Template of the certificates.



(b) Tuning formats for the specific particulars.

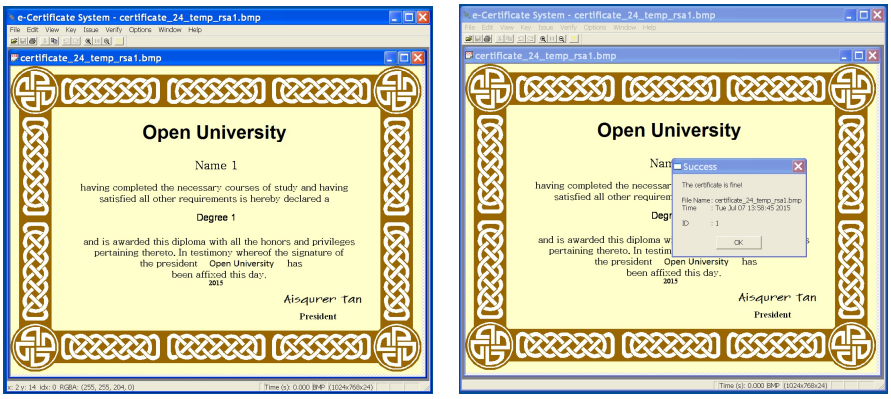


(c) Uploading materials for the certificates.



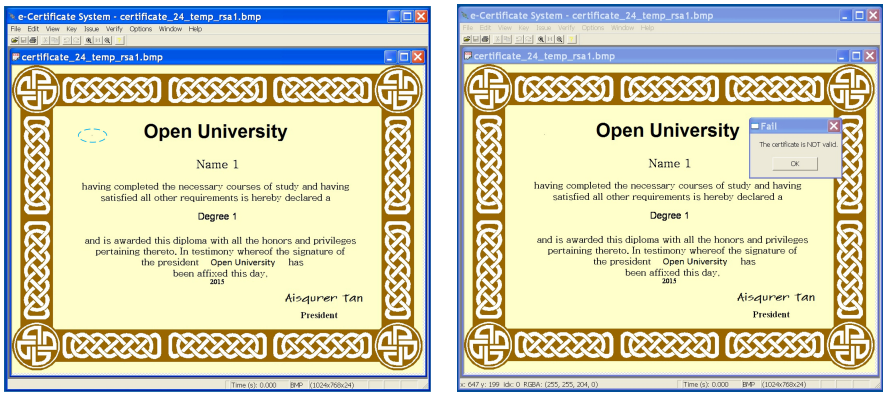
(d) Issuing the certificates.

Figure 5.3: Process of issuing certificate.



(a) Template of the certificates. (b) Tuning formats for the specific particulars.

Figure 5.4: Process of verifying the certificate.



(a) Template of the certificates. (b) Tuning formats for the specific particulars.

Figure 5.5: Verifying a tampered certificate.

is big enough. Since antiquity there were many extensive researches which had been done on the CRT and the theorem has evolved into a systematic theorem that can easily be found in many elementary mathematical texts.

Particularly, the CRT can be stated as follows. Let $m_1, m_2, ..., m_n$ be positive integers that are pairwise relatively prime and $a_1, a_2, ..., a_n$ be any n integers. Then the simultaneous congruence,

$$x \equiv a_i \,(mod\, m)\,,\ i = 1, 2, ..., n \tag{5.1}$$

has unique congruent solution $0 \leq x < M$ of the form,

$$x \equiv \sum_{i=1}^{n} a_i y_i M_i \,(mod\, m)\,, \tag{5.2}$$

where $M = m_1 m_2 ... m_n$, $M_i = M/m_i$, and $y_i M_i = 1 \,(mod\, m_i)$, $i = 1, 2, ..., n$.

For more information on CRT, readers are referred to [9]. The CRT provides a practical and efficient framework for building up the SED system.

5.4.2 Creating Electronic Certificate

Again, suppose a university is going to issue n electronic certificates. Figure 5.6 depicts the process of creating electronic certificates with the CRT scheme. Particularly, the certificates could be created and distributed in the following steps:

1. Select n positive pairwise relatively prime integers: $p_1, p_2, ..., p_n$.
2. For each certificate identified by i, hash the content by using message digest algorithm and get hash value h_i. Repeat the step and obtain n hash values: $h_1, h_2, ..., h_n$.
3. From CRT, it is ready to know that there is a unique number H satisfying

   $$0 \leq H < p_1 p_2 ... p_n \tag{5.3}$$

   and

   $$H \equiv h_i \,(mod\, p_i)\,,\ i = 1, 2, ..., n. \tag{5.4}$$

4. Publish H on the public official web site.

5.4.3 Verifying Electronic Certificate

Figure 5.7 illustrates the process of verifying the certificates. Particularly, the system proceeds with the following steps to verify the certificate:

1. Download the total hash value H from the official web site.
2. Hash the certificate by using message digest algorithm and obtain a hash value $h_i^{'}$, $i \in \{1, 2, ..., n\}$.

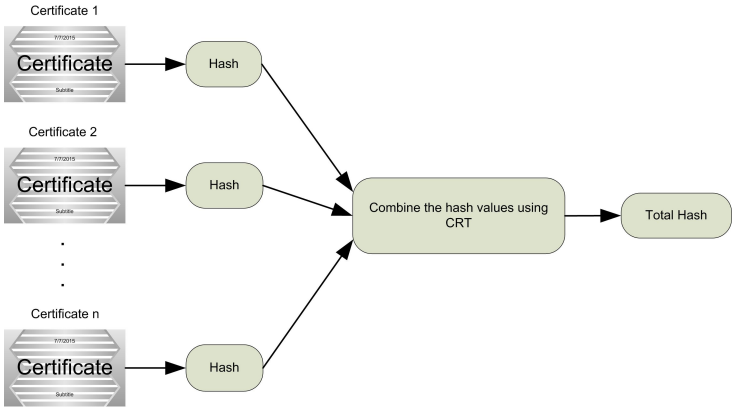


Figure 5.6: Creating electronic certificates.

3. Check whether the following congruence satisfies,

$$H \equiv h_i^{'} \left(mod\, p_i\right),\ i \in \{1, 2, ..., n\}\,. \tag{5.5}$$

If the congruence satisfies, the authentication succeeds. Otherwise, the authentication fails.

5.4.4 Security Analysis

Security of the system lies in the security of the hash function $h\left(\cdot\right)$ and the lengths of the $p_i^{'}s$. There are kinds of attacks on the hash values of the certificates.

The first attack is to generate a certificate from scratch whose hash value satisfies congruence Eq.(5.4). By this way, to gain a successful search with a probability of 1, the attacker must try $\min\left(2^{l_h}, 2^{l_{p_i}}\right)$ times, where l_h is binary length of hash value and l_{p_i} is the binary length of p_i, respectively. The second attack is no better than the first one. In the attack, given a certificate, the attacker tries to falsify the certificate and make the result have the same hash value as the original one. The attacker also has to try $\min\left(2^{l_h}, 2^{l_{p_i}}\right)$ times before he has a successful result with a probability of 1. Hence the minimum length of the hash value and the prime number determines the security strength of the system.

In real implementation, we select a group of $p_i^{'}s$ in advance. Without deteriorating the system's security and for convenience, these $p_i^{'}s$ could be constants. E.g., we use the least prime number greater than 2^{128} as p_1, the second least prime number as p_2, so on and so forth. The issuing and verification system can use the same set of $p_i^{'}s$.

The total hash value H is mainly determined by $\sum_{i=1}^{n} l_{p_i}$ and it becomes cumbersome when n turns big. Hence, the number of certificates should be limited to certain level in each batch. Compared with the public key based scheme, this is one disadvantage of the CRT-based system. In the public key based system, the public key's size always keeps constant, no matter how many certificates are issued.

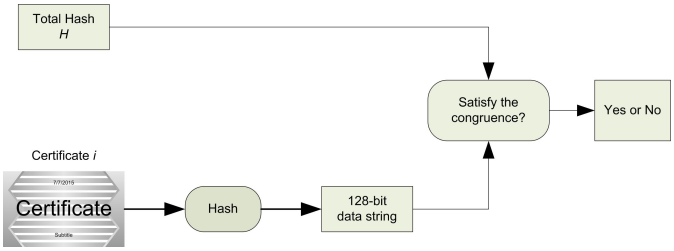
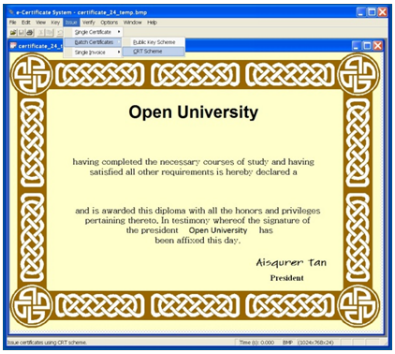
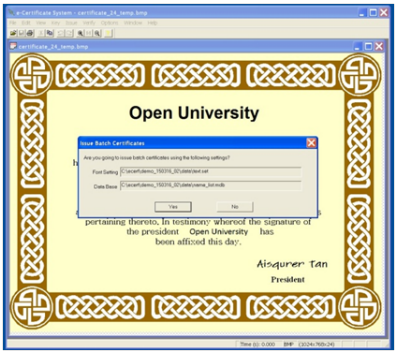


Figure 5.7: Verifying the electronic certificate.



(a) Template of the certificates.



(b) Tuning formats for the specific particulars.

Figure 5.8: Creating electronic certificates with CRT scheme.

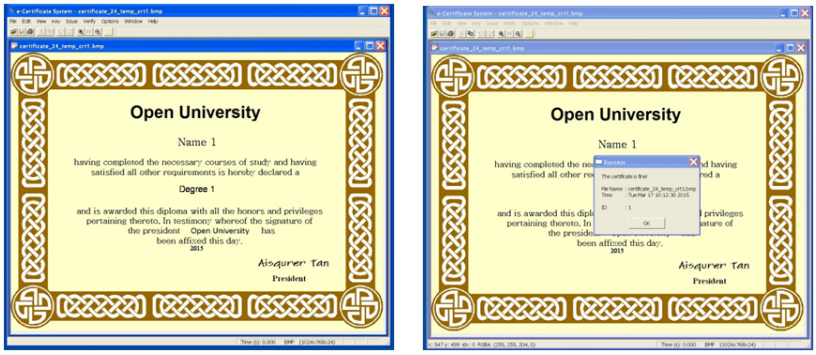
5.4.5 Implementation

The main function of the issuing subsystem is to generate the total hash value of the certificates. Specifically, the subsystem includes the following functions:

- Generating hash values for all the certificates.
- Generating the total hash value by combining the single hash values with CRT.
- Publishing the total hash value on the official website.
- Distributing the e-certificates to students.

The verification subsystem is a bit simpler than the issuing subsystem. Its main functions include:

- Downloading the total hash value from the official public web site.
- Generating hash value of the certificate.
- Checking whether congruence Eq.(5.4) satisfies.



(a) Template of the certificates.

(b) Tuning formats for the specific particulars.

Figure 5.9: Verifying the certificate produced with CRT scheme.

Figure 5.8 depicts the process of creating electronic certificates with CRT scheme. Figure 5.8a displays the certificate template; and Fig.(5.8b) depicts generating secure certificates with format settings and database of the students' details. After the processes, certificates and a file containing the total hash value of all the certificates are generated.

Figure 5.9 illustrates the process of verifying the electronic certificate produced by CRT scheme. Figure 5.9a displays a secure certificate generated by the system, and Fig.(5.9b) illustrates the process of verifying the certificate, respectively. Prior to the verification, the total hash value of the certificates is downloaded from the official website. Figure 5.9b shows the successful verification.

Figure 5.10 illustrates the process of verifying a tampered certificate. As shown in the dashed oval area in Fig.(5.10a), the certificate was damaged with a thin curve. Figure 5.10b shows that the verification failed.

5.5 Comparison of the Two Systems

The public key based SED utilizes the security feature of public key encryption algorithm and therefore it has strong security. The scheme itself does not depend on any public key encryption algorithm and this makes it very flexible in selecting appropriate encryption algorithms to use. In addition, a single pair of public key and private key can be used for a large number of certificates or licenses. This simplifies significantly both creation and verification without compromising security. The main disadvantage of the public key based system is that a large number of certificates could be affected if the public key system is compromised. The kind of problem can be resolved by introducing valid time for the certificates or decreasing the number of certificates encrypted by the key pair. The public key based SED is particularly suitable for short-term digital invoices and licenses.

On the other hand, the CRT scheme does not have the key stolen issues. The

(a) Template of the certificates.

(b) Tuning formats for the specific particulars.

Figure 5.10: Verifying a tampered certificate.

security lies in the hash algorithms, which is deemed tough to compromise. The main disadvantage of the CRT scheme is that the size of total hash value grows along with the number of certificates, although the size of hash value is very small. The CRT scheme is particularly suitable for long-term certificates and licenses.

5.6 Conclusions

In this chapter, we have proposed two SED schemes for legal document issuing organizations. Both SED systems are able to issue verifiable electronic document while keeping the privacy secret. The first SED system is built up by utilizing public key encryption technology and data hiding technology, while the second one is created on the base of the Chinese Remainder Theorem (CRT). Both systems can be used to issue legal documents such as electronic certificate, electronic transcript, digital license, digital invoice, purchased audio clip, purchased video clip, so on and so forth. Throughout the chapter, we have presented and analyzed the principles, system architectures, security performances, and implementations for both systems.

References

[1] T. Bianchi and A. Piva. Secure watermarking for multimedia content protection: a review of its benefits and open issues. *IEEE Signal Processing Magazine*, 30(2):87–96, 2013.

[2] C.K. Chan and L.M. Cheng. Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3):469–474, 2004.

[3] J. Chen. Anti PoV-steganalysis data hiding algorithm. In *9th International Conference on Information, Communications and Signal Processing (ICICS)*, pages 1–5, 2013.

[4] D.S.A. Elminaam, H.M.A. Kader, and M.M. Hadhoud. Performance evaluation of symmetric encryption algorithms. *International Journal of Computer Science and Network Security*, 8(12):78–85, 2008.

[5] T. Furon and P. Duhamel. An asymmetric watermarking method. *IEEE Transactions on Signal Processing*, 51(4):981–995, 2003.

[6] V.M. Potdar, S. Han, and E. Chang. A survey of digital image watermarking techniques. In *3rd IEEE International Conference on Industrial Informatics (INDIN)*, pages 709–716, 2005.

[7] N. Provos and P. Honeyman. Hide and seek: an introduction to steganography. *IEEE Security /& Privacy*, 1(3):32–44, 2003.

[8] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[9] C. Schwarzweller. The Chinese remainder theorem, its proofs and its generalizations in mathematical repositories. *Studies in Logic, Grammar and Rhetoric*, 18(31):103–119, 2009.

[10] P.W. Wong and N. Memon. Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, 10(10):1593–1601, 2001.

[11] M. Wu and B. Liu. Data hiding in binary image for authentication and annotation. *IEEE Transactions on Multimedia*, 6(4):528–538, 2004.