
PERGAMON

Computerized Medical Imaging and Graphics 27 (2003) 185–196

Computerized Medical Imaging and Graphics

www.elsevier.com/locate/compmedimag

Medical image security in a HIPAA mandated PACS environment

F. Cao[a,*], H.K. Huang[a], X.Q. Zhou[b]

[a]*Department of Radiology, Childrens Hospital of Los Angeles, University of Southern California, 4650 Sunset Boulevard Mailstop 81, Los Angeles, CA 90027, USA*

[b]*Security Research Division, Network Associates Inc, Santa Clara, USA*

Received 27 August 2002; revised 24 September 2002; accepted 7 October 2002

Abstract

Medical image security is an important issue when digital images and their pertinent patient information are transmitted across public networks. Mandates for ensuring health data security have been issued by the federal government such as Health Insurance Portability and Accountability Act (HIPAA), where healthcare institutions are obliged to take appropriate measures to ensure that patient information is only provided to people who have a professional need. Guidelines, such as digital imaging and communication in medicine (DICOM) standards that deal with security issues, continue to be published by organizing bodies in healthcare. However, there are many differences in implementation especially for an integrated system like picture archiving and communication system (PACS), and the infrastructure to deploy these security standards is often lacking. Over the past 6 years, members in the Image Processing and Informatics Laboratory, Childrens Hospital, Los Angeles/University of Southern California, have actively researched image security issues related to PACS and teleradiology. The paper summarizes our previous work and presents an approach to further research on the digital envelope (DE) concept that provides image integrity and security assurance in addition to conventional network security protection. The DE, including the digital signature (DS) of the image as well as encrypted patient information from the DICOM image header, can be embedded in the background area of the image as an invisible permanent watermark. The paper outlines the systematic development, evaluation and deployment of the DE method in a PACS environment. We have also proposed a dedicated PACS security server that will act as an image authority to check and certify the image origin and integrity upon request by a user, and meanwhile act also as a secure DICOM gateway to the outside connections and a PACS operation monitor for HIPAA supporting information.

Keywords: Data encryption; Picture archiving and communication system security; Image integrity; Digital imaging and communication in medicine compliance; Health insurance portability and accountability act

1. Introduction

Picture archiving and communications system (PACS) is an integrated management system for archiving and distributing medical image data [1–3]. Communication of medical images in a PACS environment is usually over the internal hospital network that is protected by a firewall from outside intruders. As the communication extends over public networks outside the hospital to the physician's and patient's home or to anywhere needed for teleradiology and other telehealth applications, it may bring thousands of opportunities for an intruder, casual or with malicious intent, to tamper the image data over open networks or to slip right into the heart of the hospital network through the communication tunnel piggybacking on an entrusted user. Conventional Internet security methods are not sufficient to guarantee that medical image had not been compromised during data transmission. Techniques including virtual private network (VPN), data encryption, and data embedding are being used for additional data protection in other fields of applications like financing, banking, and reservation systems. However, these techniques have not been systematically applied to medical imaging partly because of the lack of urgency until the recent HIPAA proposed requirements in patient data security (Health Insurance Portability and Accountability Act).

Three major organizations related to medical image/data security have issued guidelines, mandates, and standards for

* Corresponding author. Tel.: +1-323-671-3848; fax: +1-323-671-1588.
E-mail addresses: fcao@pacbell.net (F. Cao), hkhuang@aol.com (H.K. Huang).

0895-6111/03/$ - see front matter © 2002 Elsevier Science Ltd. All rights reserved.
PII: S0895-6111(02)00073-3

image/data security. The ACR (American College of Radiology) Standard for Teleradiology, adopted in 1994, defines guidelines for 'qualifications of both physician and nonphysician personnel, equipment specifications, quality improvement, licensure, staff credentialing, and liability' [4–7]. HIPAA of 1996, Public Law 104–191, which amends the Internal Revenue Service Code of 1986 [8,9] requires certain patient privacy and data security. Part 15 of the DICOM Standard specifies security profiles and technical means for application entities involved in exchanging information to implement security policies (PS 3.15-2001) [10]. In addition, SCAR (Society of Computer Applications in Radiology) issued a premier on 'Security issues in digital medical Enterprise' during the 86th RSNA 2000 (Radiological Society of North America), to emphasize the urgency and importance of this critical matter [11]. Despite these initiatives, to our knowledge, there have not been active systematic research and development efforts in the medical imaging community to seriously tackle this issue.

Generally, trust in digital data is characterized in terms of confidentiality, authenticity, and integrity (ISO 7498-2) [12]. Confidentiality is 'the property that information is not made available or disclosed to unauthorized individuals, entities or processes.' Authenticity is defined as 'the corroboration that the source of data received is as claimed.' Integrity is the 'the property that data has not been altered or destroyed in an unauthorized manner.' Medical digital image often consists of two parts, a nominative image header and an anonymous image body. The nominative data containing the sensitive patient information needs to be well protected by all security means while the most concerned issue for the anonymous image body is image integrity. Medical image security is to maintain privacy (confidentiality) of the patient information in the image and to assure data integrity that prevents others from tempering the image.

With current technology and know how, it is not difficult to get access to the network and to insert artifacts within the image and defy its detection. As a result, image could be compromised during its transmission. We give two examples in digital mammography (projection image) and chest CT (sectional image) to illustrate how easy it is to change medical digital images. Fig. 1 is a digital mammogram with 2D artificial calcifications inserted [13]. Fig. 1(a) is the original mammogram, (b) the mammogram with artificial calcifications added, (c) the magnification of a region containing some added artifacts, and (d) is the subtracted images between the original and the modified mammogram. Calcifications are very small subtle objects within a mammogram. If inserted, artifacts would create confusion during diagnosis. Fig. 2(a) shows a CT scan of the chest, and Fig. 2(b) with a 3D artificial lesion inserted. With the artificial lesion camouflaged by pulmonary vessels, it requires some efforts for its detection. For this reason, image integrity becomes a critical issue in a public network environment.

Encryption is the most useful approach to assure data security during its transmission through public communication networks [14,15]. A cryptography system, known as Public-key cryptography (asymmetric cryptography) provides the technical foundation that is commonly used to assure the data security in terms of confidentiality, authenticity and integrity [16–19]. Cryptography in general is the science of creating and identifying code systems intended to scramble a message so that the message cannot be understood by anyone other than an intended party. In the Public-key system, a pair of codes (also called a public key and a private key) is used to encrypt and decrypt the message. The two keys are mathematically related, but it is computationally infeasible to deduce the private key from the public key. The sender uses the *public* key of the person (or system) he wants to communicate with to encrypt the message. The scrambled message can be decrypted and read only by the recipient who owns the private key. This encryption method secures the message from being used by an unauthorized third party, thus achieving confidentiality. Using the same technology, one can create a digital signature (DS) to ensure data authenticity and integrity that are usually tied with each other [20]. In this case, one could 'sign' and 'seal' a message as his, by creating and locking a coded value to the message using his private key. If the message were tampered with, the value changes and the message would not yield the correct code value indicating it has been tampered with. When the recipient receives the message he can check for the correct code value using a 'key' (public key) the sender provides, therefore authenticating the identity of the sender and ensuring the message integrity.

The public-key (asymmetric) cryptography technology is an effective tool for a secure data communication. There are various ways this technology can be implemented to address different security issues. The method has been utilized recently in DICOM Security Profiles for secure communication of DICOM images [10]. The same method has also been extended in our laboratory to create the digital envelope (DE) for medical images [13,21–23]. DE includes the DS of the image as well as the confidential patient information selected from the DICOM image header. The DE can be embedded in an image to form an invisible digital watermarking as a permanent signed record or encrypted and sent over open networks for a secure communication of medical images. The new DICOM security profiles have specified the encryption algorithms and provided the technical means to implement the image security in transit. But the standard does not maintain the image data security before or after the transition. The standard depends on the PACS to authenticate users and maintain the local image security. By comparison the image-embedded DE method, though no standard and difficult to implement, can provide

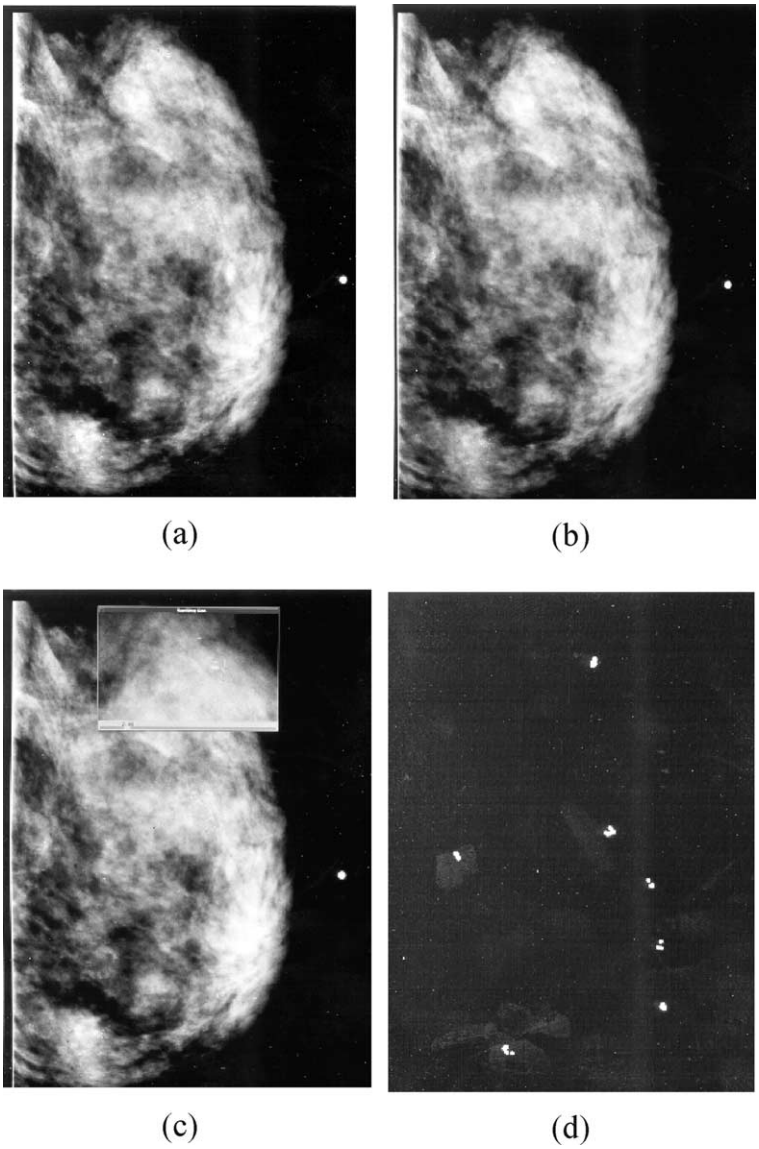
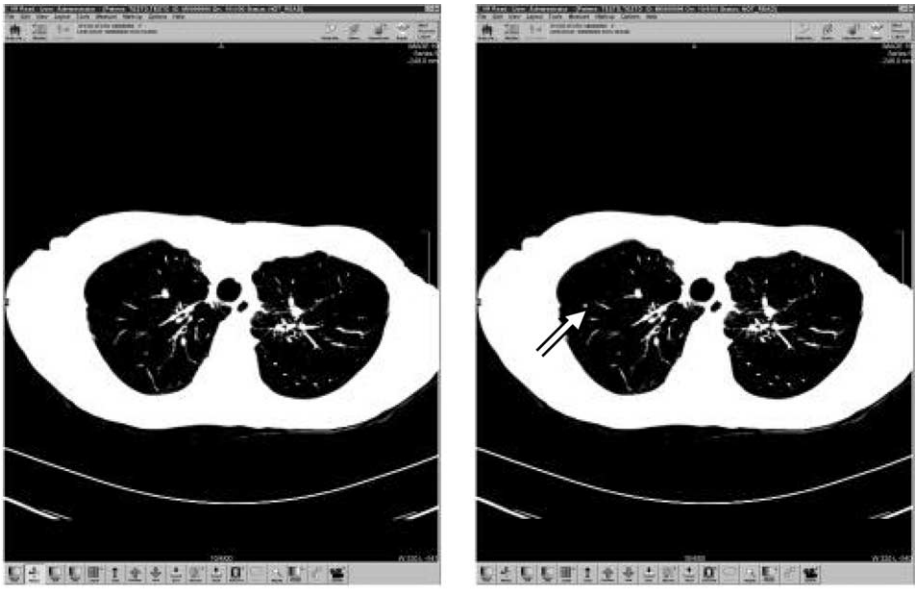


Fig. 1. An example of a digital mammogram with inserted artificial calcifications. (a) Original mammogram; (b) with artifacts; (c) magnification of some artifacts; (d) subtracted between (a) and (b). The artifacts are highlighted with overexposure during display [13].

a permanent assurance of image data security no matter when and how the image has been manipulated.

In this paper, an image security system based on the DE concept will be proposed to assure data integrity, authenticity, and confidentiality in a PACS environment. In this system, medical images from modalities will be first digitally signed, embedded in with the DE that includes the DS and patient information relevant to the image, and then archived to the PACS server. An image security server, sitting between the local PACS server and outside users, will response to all image security issues during image transmission through public networks. The server will act as (1) a DICOM Gateway to the outside for DICOM-compliant secure communications, (2) a PACS monitoring system that logs the security information to support hospital-wide HIPAA compliance, (3) an Image Authority to certificate an image origin and integrity.

In telemedicine and teleradiology [24–33], image data cannot be limited within a private local area network protected by a firewall. Therefore, DE-based security system proposed here offers the most useful security assurance of patient information privacy and image integrity. The paper is organized as follows. In Section 2, we will describe an image-embedded DE method for image security. Section 3 gives an introduction of the newly released DICOM security profiles. Section 4 summarizes the HIPAA impacts on PACS security. Section 5 proposes a DE-based PACS security infrastructure that is DICOM compliant and can provide an additional HIPAA support as well.



(a) (b)

Fig. 2. (a) A CT chest, (b) same CT with an artificial lesion inserted (arrow). (Courtesy of Michael Zhou).

2. Medical image security using digital envelope

We have developed in our laboratory a method to generate DE and embed it in mammogram and MR sectional images [13,22,23]. DS is a major application of public-key cryptography [16]. DE includes the DS of the image as well as decoded patient information from the DICOM image header. The concept of DE is that someone can 'seal' a message (DS plus patient information) in such a way that no one other than the intended recipient can 'open' the sealed message. The DE method can be revamped as a general method to assure data security for communication of medical images over public networks.

2.1. General methodology

Fig. 3 describes a general methodology and the principles as listed below:

At sender

1. The image is first segmented with background removed or cropped by finding the minimum rectangle that covers the image object.
2. A DS for the segmented image is produced using the sender's private key.
3. Patient information, if needed, is appended to the signature to form the DE.
4. The DE is converted to a bit stream and randomly distributed in the background.
5. The distributed bits are embedded outside of the rectangle that covers the image.
6. The embedded image is encrypted using the receiver's public key and then sent out via public networks.

At receiver

1. The encrypted image is decrypted using the receiver's private key.
2. The embedded image is separated into two parts, inside and outside of the rectangle
3. The bit stream outside of the rectangle is collected to rebuild the DE and reveal the original DS.
4. A second image signature is computed from the image inside the rectangle.
5. The two signatures are compared.
6. If the transmitted image had been altered in any way, the two signatures would differ, the transmitted image is discarded, and a request for the image to be resent.

2.2. DE-based security system

The DE-based security system consists of four modules: image preprocessing, image digest and DS, DE, and image embedding. There are two major categories of medical images: projection radiography (CR and Digitized Film), and sectional images (CT, MRI, and US). In sectional images, the DE method can be developed both for single slice images and for 3D volume images.

2.2.1. Image pre-processing

Image pre-processing consists of background removal and segmentation. The purpose is to reduce the necessary size of the image in order to speed up the image digest

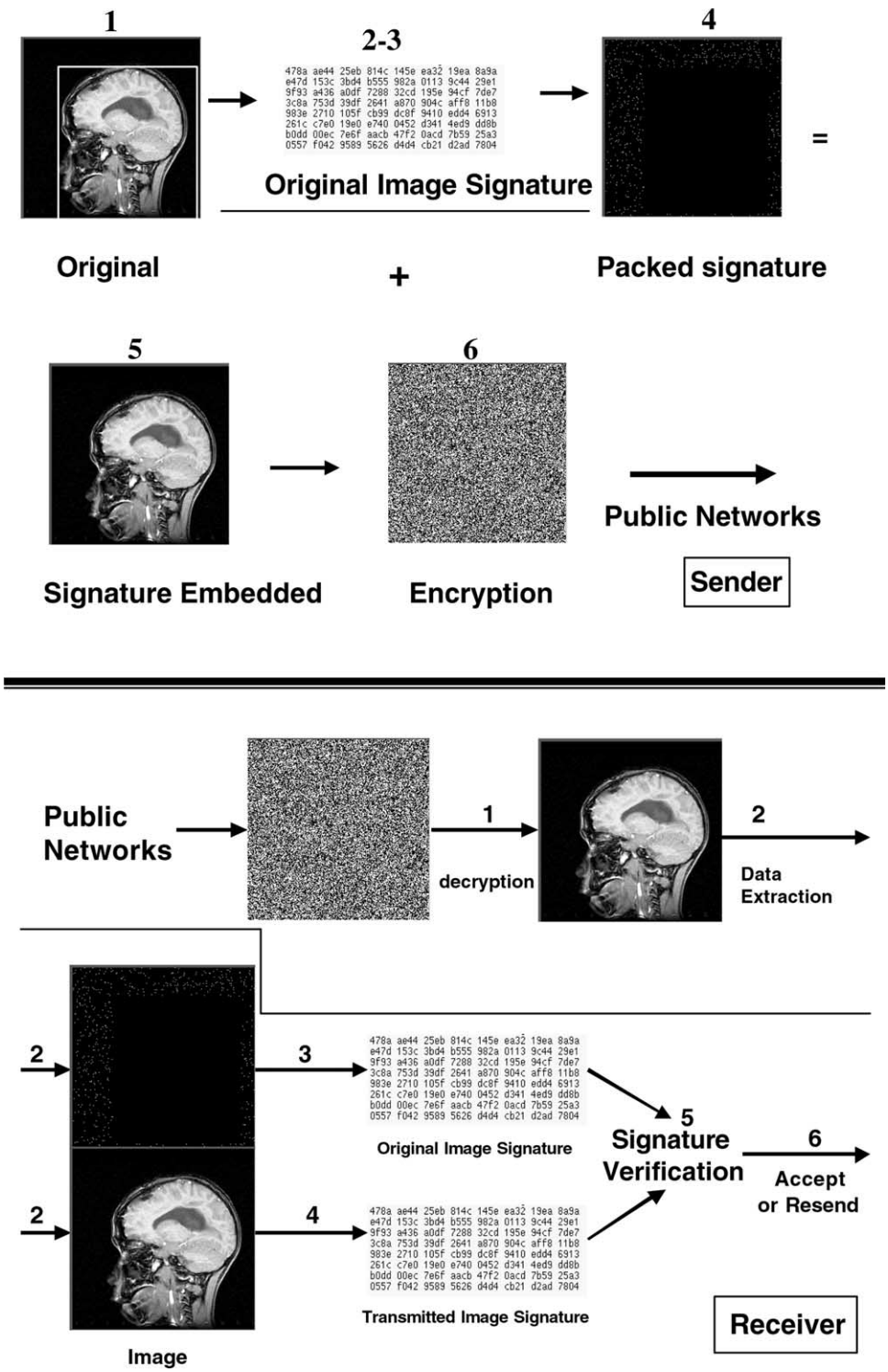
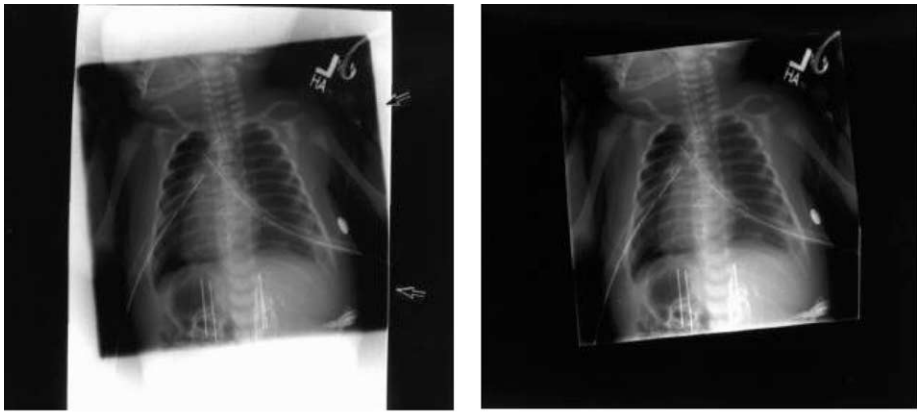


Fig. 3. Principles of image integrity check using image signature.

process, and to allow a region outside of the image object for data embedding.

(1) *Projection radiography*. In background removal, foreign objects that do not belong to the images like the compression plate in a mammography [13], patient's label and ID, other non-clinical related foreign objects will be automatically removed. Background due to X-ray collimation like in lateral chest, extremities, and pediatric radiography, should also be removed. We have developed a very effective automatic background removal algorithm for this purpose (Fig. 4) [34–36].In segmentation, the idea is to segment only the content within the image required for



(a) (b)

Fig. 4. (a) The original CR pediatric image with X-ray collimator (arrows), (b) automatic background removed image. Collimator has been removed [34].

DS. A minimum rectangular algorithm has been developed for digital mammogram after background removal [28]. However, other images from projection radiography may not be able to fit into a minimum rectangle like a conventional P-A chest image. In this case, the embedding will be done in the least significant bit of the image object.

(2) *Sectional Images*. In sectional images, normally no background removal is necessary. Segmentation with a minimum rectangle (step 1 in Fig. 3 top) is sufficient to discard most pixels outside of the image.

2.2.2. Image digest and signature

DS identifies the signer and ensures the integrity of the signed data. It is a bit stream, generated by a mathematical algorithm and is a unique representation of the data. If one were to change just one bit in the data stream, the corresponding signature would be different. To create a DS for the image, the sender first computes a condensed representation of the image known as an image hash value (or image digest) that is then encrypted (signed) using the sender's private key. It should be noted that only the digest instead of the image itself is encrypted. This makes sense because the actual image (like digital mammograms) can be very large and public key operations can be extremely slow. DS are usually time-stamped before they are actually signed. This ensures that the receiver would also be able to verify when the data was actually signed.

Any party with access to the sender's public key, image, and signature can verify the signature by the following procedure: first compute the image hash value with the same algorithm for the received image, decrypt the signature with the sender's public key to obtain the hash value computed by the owner, and compare the two image hash values. This is due to the fact that the mechanism of obtaining the hash is designed in such a way that even a single data bit change in the input string would cause the hash value to change drastically. If the two hash values are the same, the receiver (or any other party) has the confidence that the image had been signed off by the owner of the private key and that the image had not been altered after it was signed off. Thus, it assures the image integrity.

2.2.3. Digital envelope

DE is the wrapped (sealed) bulk data. After concatenating the DS of the image and the patient data into a data stream, the DE is generated by encrypting the data stream using the receiver's public key. The DE generated in this way ensures not only the privacy of data through encryption but also the image authenticity and the integrity that are the features passed on from the image signature wrapped with it. At the receiver's side, the signature can be viewed or verified only by authorized person because only he would have access to the corresponding private key to unwrap the envelop. Both DS and DE are the applications of public-key cryptography technology. The DE with the image signature and patient data wrapped with it provides an effective tool to ensure image security in a PACS environment.

2.2.4. Data embedding

Data embedding is a form of steganography that conceals the DE in the image so that the visual quality of the image is not perceptually affected. We have explored data embedding techniques by embedding the encrypted DE data bit stream either in the background outside the minimum rectangle that encloses the image or in the least significant bit (LSB) of randomly selected pixels [37] if the LSB is just background noise and its change will not affect diagnostic quality of the image [13].

To embed the data, a random walk sequence in the whole segmented image is obtained, the bit stream data to be embedded replace LSB of each of these randomly selected pixels along the walk sequence, bit-by-bit. Each dot in Fig. 3 top (step 4) shows the location of the pixel in which data has been embedded in the LSB.

Data embedding in an image has two advantages over by placing the encrypted DE in the DICOM image header

because: (1) the image-embedded DE is difficult to detect from the image, and (2) there is no need to send the DICOM image header with the image since it has already been embedded. Sending the DICOM image header in public networks without certain security assurance is compromising data security. By comparison, the DE in the DICOM header that is separated from the image data can be easily deleted and recreated by a hacker when the image is available to him.

2.3. Current limitations

The DE embedding in an image is a time consuming and CPU-intensive process. The time required each on the sending and receiving sites for processing a digital mammogram can range from 40 s for the segmented (background removed) image of 7Mb to 2–3 min for the original one of 36 Mb, based on our previous evaluation in 1998 on an old Sun Sparc 690MP multiprocessor machine [13]. It is expected that even with the current CPU power of 1 GHz, algorithm optimization and revamp of the DE method are needed in order to speed up the whole process for real-time image transmission. Three criteria for evaluation of the DE method will be (1) the robustness of the hash algorithm in computing the image DS, (2) the percentage of the pixel changed in data embedding, and (3) times required at the sending site for signing the signature, sealing the envelop, and embedding the data; as well as the reverse processes at the receiving site including verifying the signature, opening the envelop, and extracting the data. The goal is to minimize the total time required at both the SS (sending site) and the RS (receiving site).

The method we developed so far can only detect if any pixel or any bit in the data stream had been altered, but it does not know exactly which pixel(s) or bit(s) has been compromised. It would be very expensive, in term of computation, to determine exactly where the change had occurred. Current data assurance practice is that once the RS determines the image/data had been altered, it will discard the image, notify and alert the SS, and request the information to be retransmitted.

3. DICOM security

3.1. Current DICOM security profiles

The digital image and communication in medicine (DICOM) standard Part 15 (PS 3.15-2001) has recently been released to provide a standardized method for secure communication and DS [10]. It specifies technical means (selection of security standards, algorithms and parameters) for application entities involved in exchanging information to implement security policies. In this part, four security profiles that have been added to the DICOM standard are secure use profiles, secure transport connection profiles, DS profiles and media storage secure profiles. These address issues like use of attributes, security on associations, authentication of objects and security on files.

(1) *Secure use profiles*. The profiles outline how to use of attributes and other Security Profiles in a specific fashion. The profiles include secure use of online electronic storage, basic and bit-preserving DS.

(2) *Secure transport connection profiles*. The profiles published in 2000 specify the technological means to allow DICOM applications to negotiate and establish the secure data exchange over a network. The secure transport connection is similar to the secure socket layer (SSL) commonly used in the secure Web online processing [38] and VPN encryption often used to extend internal enterprise network to the remote branches. It is an application of Public-key cryptography that the scrambled message by the sender can only be read by the receiver and no one else in the middle would be able to decode it. Currently, the profiles specify two possible mechanisms for implementing secure transport connections over a network, TLS (Transport Layer Security 1.0) and ISCL (Integrated Secure Communication Layer V1.00). It endows DICOM with a limited set of features that are required to implement with.

(3) *Digital signature profiles*. While the secure transport connection protects the data during transit, it did not provide any lifetime integrity checks for DICOM SOP (service–object pair) Instances. The DS Profiles published in 2001 provide mechanisms for lifetime integrity checks by using DS. DS allow authentication of the identity entity that created, authorized, or modified a DICOM Dataset. This authentication is in addition to any authentication done when exchanging messages over a secure transport connection. Except a few attributes, the profiles do not specify any particular dataset to sign. The creator of a DS should first identify the DICOM data subset, calculate its message authentication code (MAC), hash value, and then sign the MAC into a DS. As with any DS, the receiver can verify the integrity of this DICOM data subset by recalculating the MAC and then comparing it with the one recorded in the DS. Typically the creator of the DS would only include data elements that had been verified in the MAC calculation for the DS. The profiles currently specify three possible ways of implementing DS depending on what to be included in the DICOM dataset to be signed: base (methodology), creator (for modality and image creator) and authorization (approval by technician or physician) DS profile.

(4) *Media security profiles*. The DICOM media security also published in 2001 provides a secure mechanism to protect the un-authorized access to this information on the media using encryption. It defines a framework for the protection of DICOM Files for Media Interchange by means of an encapsulation with a cryptographic ‘envelope’. This concept can be called *protected DICOM file*. It, as an application of Public-key cryptography, follows the similar steps to the DE method in Section 2. The DICOM file to be protected is first digested, signed with DS (optional in

the profiles) and then sealed (encrypted) in a cryptographic envelope, ready for media interchange.

3.2. What's coming next for DICOM security

The security needs in DICOM are under rapid development. Specifying a mechanism to secure parts of a DICOM image header by attribute level encryption is probably a next step towards satisfying the patient privacy requirements by HIPAA. The principle is that any DICOM data elements that contain patient identifying information should be replaced from the DICOM object with dummy values. Instead of simple removal, the dummy values of patient information, such as Patient ID and Names are required so that images can still be communicated and processed with existing DICOM implementations, security aware or not. The original values can be encrypted in an envelope and stored (embedded) as a new data element in the DICOM header. Using public-key cryptography, the attribute level encrypted envelope can be designed to allow only selected recipients to open it, or different subsets can be held for different recipients. In this way, the implementation secures the confidential patient information and controls the recipient's access to what part of patient data they allow to see. This selective protection of individual attributes within DICOM can be an effective tool to support HIPAA's emphasis that patient information is only provided to people who have a professional need.

4. HIPAA and its impacts on PACS security

HIPAA [8,9], put in place by Congress in 1996, and with a formal compliance date of April 14th, 2003, provides a conceptual framework for healthcare data security and integrity and sets out strict and significant federal penalties for non-compliance. However, the guidelines as they have been released (including the most recent technical assistance materials, July 6, 2001 modifying parts 160 and 164) do not mandate specific technical solutions, rather there is a repeated emphasis on the need for scalable compliance solutions appropriate to variety of clinical scenarios covered by HIPAA language.

The term 'HIPAA Compliant' can only refer to a company, institution or hospital. Policies on patient privacy must be implemented institution-wide. Software or hardware implementation for image data security by itself is not sufficient. Communication of DICOM images in a PACS environment is only a part of the information system in the hospital. One cannot just implement the image security using DICOM or our image-embedded DE method and assume that the PAC system is HIPAA compliant. All other security measures, such as user authorization using passwords, user training, physical access constraints, auditing, etc. are as important as the secure communication [39]. However, image security, which provides a means for protecting the image and corresponding patient information when exchanging this information among devices and healthcare providers, is definitely a critical and essential part of the provisions that can be used to support the institution-wide compliance with the HIPAA privacy and security regulations.

The Department of Health and Human Services (DHHS) publishes the HIPAA requirements in so-called Notice of Proposed Rule Makings (NPRM). There are currently four key areas

- Electronic transactions and code Sets (compliance date: October 16, 2002)
- Privacy (compliance date: April 14, 2003)
- Unique identifies
- Security.

Transactions relate to such items as claims, enrollment, eligibility, payment and referrals whereas code sets relate to items such as diseases, procedures, equipment drugs, transportation and ethnicity. HIPAA mandates the use of unique identifiers for providers, health plans, employers, and individuals receiving health care services. The transactions, code sets and unique identifies are mainly a concern for users and manufacturers of hospital information systems (HIS), and in a much lesser extent for radiology information system (RIS) users and manufacturers, whereas it has little or no consequences for users and manufacturers of PACS. Privacy and security regulations will have an impact for all HIS, RIS, and PACS users and manufacturers. Although HIPAA compliance is an institution-wide implementation, PACS and its applications should have a high interest in making them helpful to become HIPAA supportive.

The image security discussed in previous sections and fault-tolerant PACS server [3,11] we have developed for continuous availability and disaster recovery, support the HIPAA security regulations. In addition to those, the basic requirements for a PACS that will help a hospital to comply with the HIPAA requirement is the ability to generate a list of information on demand, related to the access of clinical information for a specific patient. From an application point of view, there should be a log mechanism to keep track the access information such as,

- Identification of the person that accessed this data
- Date and time when data has been accessed
- Type of access (create, read, modify, delete)
- Status of access (success or failure)
- Identification of the data.

Although each PACS component computer especially Unix machine has its own system functions to collect all user and access controls listed above as well as auditing information and event reporting if enabled, they are scattered around the system, not in a form readily available. Also as accessing of data is typically done from many

workstations, tracking and managing each of them is a difficult task. With this in mind, a PACS should be designed in such a way that a single server can generate the HIPAA information without the need of 'interrogating' other servers or workstations.

An automatic PACS monitoring system (AMS) jointly developed in SITP (Shanghai Institute of Technical Physics) and our laboratory [40] can be revamped as the PACS reporting hub for HIPAA-relevant user access information. The PACS AMS consists of two parts: a small monitoring agents running in each of PACS component computer and a centralized monitor server that monitors the entire PACS operation in real time and keeps tracking of patient and image data flow continuously from image acquisition to final display workstation. The PACS AMS is an ideal system to collect PACS security information and support HIPAA implementation.

The PACS alone cannot be claimed as HIPAA compliant. Secure communication of images using DE and DICOM security standard, and the continuous PACS monitoring have shown HIPAA support functionalities that are indispensable for hospital-wide HIPAA compliance.

5. PACS security server and authority for assuring image authentication and integrity

5.1. Comparison of image-embedded DE method and DICOM security

The image-embedded DE method described in Section 2 provides a strong assurance of image authenticity and integrity. The method has the advantage that the relevant patient information in the DICOM header is embedded in the image. It assures image security for any individual image to be transmitted through public networks without using the DICOM image header. Yet, relevant patient information can be retrieved from the DE after receiving. Meanwhile, since the actual data transfer will occur only after the DE has been successfully created and embedded, the most CPU-intensive cryptography does not have to be performed on the fly like in socket secure layer (SSL) protocol used in Web transaction, or transport layer secure (TLS) and ISCL protocols specified in DICOM Security standards. Both the sender and receiver do not have to be online at the same time to negotiate an online session. So, the image-embedded DE method is particularly suited well for store-forward type of systems like media interchange.

The DE method has been designed and used before in our laboratory for secure communication of images in transit. But there are certain disadvantages of the method, which need to be aware of.

1. *Lack of standards*. It should be noted that this DE method does not cater for the automatic identification of the various algorithms and attributes used (e.g. hashing, encryption and embedding algorithms, DE dataset to be sealed, communication protocols, etc.) while verifying the DE. Unlike the DICOM security profiles that specify the means for the sender and recipient to negotiate the information, in the DE method they either have to agree in advance or the sender needs to somehow transmit this information to the user using some out-of-band methods.
2. *Need further evaluation*. The DE method is considered good for security communication of images only when it satisfies certain criteria, like robustness, percentage of the pixel changed in data embedding, and time required to run the complete image security assurance. The DE method with data embedded in the image is time consuming to perform because of image processing and encryption algorithms that require heavy computation. It is necessary to optimize the DE method and evaluate its performance for real-time applications. It is better to provide the user a choice of selecting less computationally intensive algorithms or bypassing the integrity check altogether since the user's machine may not be powerful enough to handle the heavy DE processing.
3. *Limited capability in image distribution*. The DE method is not very well suited to multicast communication systems or to multi-sites image distributing or for the heavy user traffic. Since the DE is encrypted with the receiver's public key and then embedded in the image, this CPU-intensive process has to be performed all over again for different user or site because of different public key.

The above three shortcomings would limit the image-embedded DE method in a well-controlled environment. Since the DICOM security profiles, described in Section 3, have been released and become the standard, it is preferred that a DICOM-compliant communication should be used to address the secure transmission of images between the sender (last step) and receiver (first step) shown in Fig. 3. But the DICOM standard does not maintain the confidentiality and integrity of image data before or after the transition. Furthermore the DS and DE in the DICOM header that is separated from the image data can be easily deleted and recreated by a hacker when the image is available to him. The image-embedded DE on the other hand is hard to detect from the image and can provide a permanent assurance of confidentiality and integrity of the image no matter when and how the image has been manipulated. In fact, even if one was to lose his key or worse yet, he was no longer in existence, his authentication and signature embedded in the image persists just as his written signature on paper does.

5.2. An image security system in a PACS environment

Based on the above discussion, we propose as shown in Fig. 5 an infrastructure to implement an image security system in a PACS environment. The system is based on our

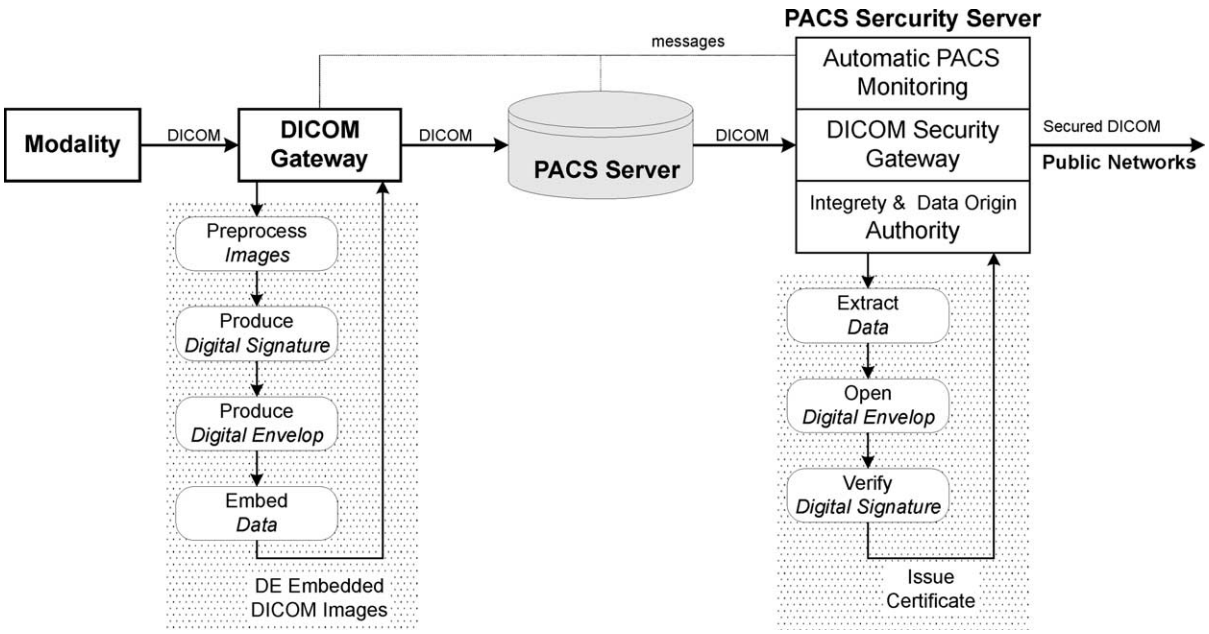


Fig. 5. Image security system in a PACS environment. Shaded boxes are where data embedding and assurance of image authenticity and integrity are implemented.

image-imbedded DE method, to use the modality gateway workstation for image embedding and to use a dedicated server to handle all PACS-related security issues. The PACS security server has the following three major functions and will acts as

(1) *A DICOM secure gateway to the outside connections*, that is in compliance with DICOM security profiles ensuring integrity, authenticity, and confidentiality of medical images in transit. The gateway plays a role in securing communication of DICOM images over public networks. It is important to build a separate DICOM secure gateway for handing the CPU-intensive cryptography so as not to impact the performance of PACS in fulfillment of its daily radiological services. The current DICOM security standards are still evolving. It will take time for the standards to mature and to be fully implemented in PACS. So it is also important that the gateway can provide interoperability with the existing 'non security aware' PACS.

(2) *An image authority for image origin authentication and integrity*. The authority server is designed to take away the limitations of the DE method discussed above and to integrate the method in a PACS environment. First, as a steganographic message, the DE embedded in the image should be permanent, associated only to the image itself and not supposed to change every time with a new user. To solve the issue, we propose to implement a dedicated image authority server whose public key will be used to seal DE of all images acquired locally. In this system, medical images from modalities will be first digitally signed at the modality gateway machine (Fig. 5) by the image creator and/or through physician's authorization or the PACS manufacturer. The signature plus relevant patient information will be sealed in a DE using the authority server's public key instead of using individual user's.

Whenever needed, a remote user can query the Image Authority to verify the origin authenticity and integrity of an image under review. The image authority is the only one who owns the private key that can be used to extract and decrypt the DE embedded permanently in the image. The image authority serves as the authority for checking the image originality and integrity, in the same way as a certificate authority (CA) [19] does for certificating the DS. The heavy computation jobs, steps 2–6 of assuring image authentication and integrity, at receiver side shown in Fig. 3, are now being taken over by the authority server, therefore, reducing the workload at the client side. Meanwhile, it is also relatively easy to keep the DE/embedding algorithms and attributes prearranged between the image authority and the DE creators/senders in a local PACS environment without requiring the open standard to define them.

(3) *A monitoring system for PACS operations*, which at a minimum should keep a user access log and monitors security events, providing support for hospital-wide HIPAA compliance. The major monitoring functions and features [40] currently implemented are (1) real-time capture of all warning, and error messages in the PACS; (2) periodically check PACS components running status; (3) track patient/image dataflow in PACS components, and analyze the image usages; (4) monitor user logon/off on remote display workstations and guarantee images securely read and used; (5) dynamically display the image data flow; (6) warn an administrator of serious errors via pager.

In addition, the PACS security server should also be intelligent to deliver only the relevant information to a user.

As the volume of clinical data, images and reports has significantly increased with digital imaging technology and government regulations continue to emphasis the information privacy, they have imposed an implementation challenge for each individual user to access specific data from a specific location—where and how can he/she access the information in a timely fashion. An intelligent security management is to find a secure way to match relevant information with a particular user. The attribute level DICOM security described in Section 3.2 and the image authority with an ability to check image attribute will definitely be a major step towards developing a smart and secured delivery system for medical images.

6. Summary

Medical image security in a PACS environment has become a pressing issue as communications of images increasingly extends over open networks, and hospitals are hard-pushed by government mandates, and security guidelines to ensure health data security. However, there has not been an infrastructure or systematic method to implement and deploy these standards in a PACS environment.

In this paper, we first discussed the public-key technology commonly used for data encryption, and presented a systematic method for implementing image security based on our image-imbedded DE concept. Then, we briefly reviewed DICOM Part 15, the newly released standard for secure communications of DICOM images, and the HIPAA impacts on PACS security. Finally, we proposed an infrastructure to implement an image security system. When an image is generated at an imaging modality, the image signature is obtained, combined with the DICOM image header, sealed in DE, and then embedded in the original image. The DE embedded in the image can only be opened (extracted and decrypted) by a local PACS security server. The server acts as an image authority that will check and certificate the image origin and integrity upon request by a user, and meanwhile acts also as a secure DICOM gateway to the outside connections and as a PACS operation monitor for HIPAA supporting information.

Acknowledgements

This research is partially supported by a NIH Grant No. R01-LM06270 and the US Army Medical Research and Materiel Command Contract No. DAMD17-99-P-3732.

References

[1] Huang HK. Picture archiving and communication systems: principles and applications. New York: Wiley; 1999. p. 521.

[2] Huang HK, Wong AWK, Lou SL, Bazzill TM, et al. Clincial experience with a second generation PACS. J Digital Imag 1996;9(4): 151–66.

[3] Cao F, Liu BJ, Huang HK, Zhou MZ, Zhang J, Zhang X, Mogel G. Fault-tolerant PACS server. SPIE Med Imaging 2002;4685-44: 316–25.

[4] James Jr. AE, James III E, Johnson B, James J. Legal considerations of medical of medical imaging. Leg Med 1993;87–113.

[5] Berger SB, Cepelewicz BB. Medical–legal issues in teleradiology. Am J Roentgenolo 1996;166:505–10.

[6] Berlin L. Malpractice issue in radiology–teleradiology. Am J Roentgenolo 1998;170:1417–22.

[7] Kamp GH. Medica–legal issues in teleradiology: a commentary. Am J Roentgenolo 1996;166:511–2.

[8] HIPAA, http://aspe.os.dhhs.gov/admnsimp, US Department of Health and Human Services.

[9] HIPAA, http://www.rx2000.org/KnowledgeCenter/hipaa/hipfaq.htm.

[10] Digital Imaging and Communications in Medicine (DICOM). National Electrical Manufacturers Association (NEMA). Rosslyn, VA, http://medical.nema.org/dicom/2001.html, Part 15: Security Profiles, PS 3.15-2001; 2001.

[11] Huang HK, Cao F, Zhang JG, Liu BJ, Tsai ML. Fault tolerant picture archiving and communication system and teleradiology design. In: Reiner B, Siegel EL, Dwyer SJ, editors. Security issues in the digital medical enterprise. SCAR; 2000. p. 57–64. Chapter 8.

[12] ISO 7498-2:1989, Information processing systems, Open Systems Interconnection, Basic Reference Model—Part 2: Security Architecture, http://www.iso.org, International Organization for Standardization; 1989.

[13] Zhou X, Huang HK, Lou SL. Authenticity and integrity of digital mammogrpahy image. IEEE Trans Med Imaging 2001;20(8): 784–91.

[14] Garfinkel S, Spafford G. Practical unix and Internet security. California: O'Reilly & Associates, Inc; 1996. p. 139–90.

[15] Schneier B. Applied cryptography: protocols, algorithms, and source code in C. New York: Wiley; 1995. p. 250–9.

[16] Rivest R. The MD5 message-digest algorithm. Document of MIT Laboratory for computer Science and RSA Data Security, Inc; 1992. ftp://ftp.funet.fi/pub/crypt/hash/papers/md5.txt.

[17] RSA Laboratories, Frequently Asked Questions About Today's Cryptography, version 4.1, http://www.rsasecurity.com/rsalabs/faq/index.html.

[18] Kaliski BS, Jr. An overview of the PKCS standards. An RSA Laboratories Technical Note; 1993.

[19] Public Key Infrastructure (PKI) http://home.xcert.com/~marcnarc/PKI/thesis/characteristics.html.

[20] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21(2): 120–6.

[21] Wong STC, Abundo M, Huang HK. Authenticity techniques for PACS images and records. SPIE Med Imaging 1955;2435: 68–79.

[22] Zhou XQ, Lou SL, Huang HK. Authenticity and integrity of digital mammographic images. Proc SPIE Med Imaging 1999; 3662:138–44.

[23] Zhou XQ, Huang HK, Lou SL. A study of secure method for sectional image archiving and transmission. SPIE Med Imaging 2000;3980: 390–9.

[24] Telemedicine and telecommunications: option for the new century. HPCC Program Review and Summary. Program Book. National Library of Medicine, NIH, Bethesda Md, March 13–14; 2001.

[25] Telemedicine and Advanced Technology Research Center (TATRC) Integrated Research Team Radiology Imaging. Program Review. TATRC, US Army Medical Research and Materiel Command, Fort Detrick, Md, September 20; 2000.

[26] Huang HK, Wong AWK, Zhu X. Performance of asynchronous transfer mode (ATM) local area and wide area networks for medical image transmission in clinical environment. J Comp Med Imag Graph 1997;21(3):165–73.
[27] Huang HK. Teleradiology technologies and some service models. J Comp Med Imag Graph 1996;20(2):59–68.
[28] Lou SL, Sickles EA, Huang HK, Hoogstrate D, Cao F, Wang J, Jahangiri M. Full-field direct digital mammograms: technical components, study protocols, and preliminary results. IEEE Trans Inform Technol Biomed 1997;1(4):270–8.
[29] Huang HK, Lou SL. Telemammography: a technical overview. RSNA Categorical Course Breast Imaging 1999;273–81.
[30] Stahl JN, Zhang J, Zeller C, Pomerantsev EV, Lou SL, Chou TM, Huang HK. Tele-conferencing with dynamic medical images. IEEE Trans Inform Technol Biomed 2000;4(2):88–96.
[31] Zhang J, Stahl JN, Huang HK, Zhou X, Lou SL, Song KS. Real-time teleconsultation with high resolution and large volume medical images for collaborative health care. IEEE Trans Inform Technol Biomed 2000;4(2):178–85.
[32] Stahl JN, Zhang J, Chou TM, Zellner C, Pomerantsev EV, Huang HK. A new approach to tele-conferencing with intravascular ultrasound and cardiac angiography in a low-bandwidth environment. RadioGraphics 2000;20:1495–503.
[33] Yu F, Hwang K, Gill M, Huang HK. Some connectivity and security issues of NGI in medical imaging applications. J High Speed Networks 2000;9:3–13.
[34] Zhang J, Huang HK. Automatic background recognition and removal (ABRR) of computed radiography images. IEEE Trans Med Imaging 1997;16(6):762–71.
[35] Huang HK, Zhang J. Automatic background removal in projection digital radiography images. US Patent No. 5,903,660; May 11, 1999.
[36] Pietka E. Image standardization in PACS. In: Bankman IN, Rangayyan RM, Woods RP, Robb RA, Huang HK, editors. Handbook of medical imaging, New York: Academic Press; 2000. p. 783–801. Chapter 48.
[37] Walton S. Image authentication for a slippery new age. Dr Dobb's J 1995;April.
[38] Introduction to SSL, http://developer.netscape.com/docs/manuals/security/sslin/index.htm.
[39] Dwyer SJ. Requirements for security in medical data. In: Reiner B, Siegel EL, Dwyer SJ, editors. Security issues in the digital medical enterprise, SCAR; 2000. p. 9–14. Chapter 2.
[40] Zhang J, Han R, Wu D, Zhang X, Zhuang J, Huang HK. Automatic monitoring system for PACS management and operation. SPIE Med Imaging 2002;4685-49:348–55.