

A Hierarchical Security Solution for Medical Image Transmissions

Author

Awrangjeb, M, Hossain, MS

Published

2004

Conference Title

International Conference on Computer and Information Technology (ICCIT)

Version

Accepted Manuscript (AM)

Rights statement

© 2004 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Downloaded from

<http://hdl.handle.net/10072/392040>

Link to published version

<http://www.iccit.org/>

Griffith Research Online

<https://research-repository.griffith.edu.au>

A Hierarchical Security Solution for Medical Image Transmissions

Mohammad Awrangjeb

Department of Computer Science
American International University – Bangladesh
Dhaka, Bangladesh
e-mail awrangjeb@aiub.edu

Mohammad Sazzad Hossain

Department of Computer Science
American International University – Bangladesh
Dhaka, Bangladesh
e-mail sazzad@aiub.edu

Abstract

Security in medical data communications through the open network is one of the greatest problems in modern health information systems. However, little attention has been given in last few years to solve this security problem. In this paper we propose a hierarchical security solution based on watermarking and cryptographic tools. We use lossless watermarking technique to hide confidential patient information inside the medical image and to get the exact copy of the original image when necessary. In addition, we use hash of the original image as a part of watermark to ensure integrity, and public key cryptography to maintain security services like authentication, non-repudiation, and confidentiality. To avoid the cost of establishing Public Key Infrastructure (PKI) we propose hospital authority to act as local Trusted Third Party (TTP) and Diffie-Hellman key exchange protocol to establish secret session key. Only software tools are required to implement this proposed security solution.

Keywords

Security, medical image, watermarking, cryptographic, hospital information system

INTRODUCTION

Due to the advances of information technology and high speed computer networks, medical services such as production of different kinds of digital medical images, *Electronic Patient Record* (EPR), and their secure communications have gained a great attention of the people working in the medical hospitals as well as the people working in the information technology systems [1]. For digital information management there are *Hospital Information Systems* (HIS), *Radiology Information Systems* (RIS), and *Picture Archiving and Communication Systems* (PACS) that form the information infrastructure of modern health care systems [2]. Teleconsulting, telediagnosis, and telesurgery are the rapid growing fields within HIS, RIS, and PACS because of incredible advance of research in Multimedia systems and Internet. Modern information technology systems allow store, access, and distribution of medical images, EPR, documents etc. to various users from doctors, experts within the hospitals to the researchers, students studying in universities. Patients can access their own medical images, information staying at their homes.

Let us think about a traditional health care system where a patient goes to hospital, treatment is done by the doctors

within that hospital, he may be sent to a laboratory to do necessary tests, if needed he is kept hospitalized. All the cases of diseases are not serious; however, they take almost equal amount of efforts in terms of time and money. In traditional systems, there are not enough opportunities to discuss and share information by the medical experts, especially when the case is dangerous. If a doctor in a local hospital is unable to treat a case of a patient, he needs to discuss and seek help from other doctors staying away or in abroad. An expert has to travel a long way to help the local doctor where ultimate decision may out from a MRI image of certain organ of the patient. Alternatively, think when a patient goes abroad for advance treatment for a complex disease, the experts in abroad may need the life medical-history, documents, and images of the patient in order to take the right decision in a complex situation. Moreover, we can think of a person who has got a job in abroad and the job will be started two months later. But he has to go abroad now only to have the medical test there and then to come back. All the situations we present here are time consuming, embarrassing and financially expensive.

Modern health care system aims to give complete solution to such problems. The external expert could stay abroad, access the MRI of the patient and give on-line advice to the local doctor. The image archive kept personally by the patient in his desktop computer at home or by local hospitals could send all the documents, life medical history and images to abroad in the case of a complex disease. The new foreign job holder could send his medical images and documents through an authorized way by local hospitals. Hence the modern health care system helps both doctors and patients by saving a lot of efforts in terms of both time and money.

However, it creates several issues to be considered and security problems to be solved. Medical resources such as doctors, nurses, and equipments etc. are to be shared among several hospitals that access patient's images, records, and documents. All the information they access are in digital form in modern health systems. Digital images, documents are easily manipulateable using software. Consider a recruitment system that notices the candidates to submit personal life medical-history, documents, and images to the host organization. Potential candidates may manipulate their information by bribing the hospital stuffs or themselves. Thus severe security problem arise circulating patient's personal records, images in open networks being accessible through

Internet. The EPR should be kept secret and cannot be revealed to unauthorized persons without prior permission of the patient. Therefore, security solution to modern medical systems is urgent, but security issues are considered too little in past few years.

The rest of the article goes as follows: section 2 describes security services, security tools, and users in the medical information system, section 3 presents the proposed security solution, how it ensures complete security, how to avoid expenses to establish PKI and TTP, and finally section 4 concludes our article.

SECURITY SERVICES

The most important security services are confidentiality, authentication, integrity, non-repudiation, and availability.

- *Confidentiality* ensures the medical information stored in a computer system as well as medical data transmitted through the Internet are accessible only for reading by authorized parties. Threats to confidentiality are disclosures of secret information to, and re-routing by, unauthorized parties.
- *Authentication* ensures that the origin of a medical-image or document is correctly identified. An unauthorized party may insert false medical-images or document in the medical information system as a threat to authentication.
- *Integrity* ensures only the authorized persons are able to change the medical information. Threats to integrity are destruction and modification of medical files and records.
- *Non-repudiation* requires neither the sender nor the receiver of some medical file or data is able to deny the transmission.
- *Availability* requires that access of medical information and digital resources are available to the authorized persons. Destruction of information system, disabling of file information system etc. are threats to availability.

Security systems proposed so far in the literature of medical information systems are unable to provide complete security. Some of them emphasize on integrity and confidentiality of information. Yang et al. [1] introduce an image-based simulated system for kyphoplasty telesurgery giving attention to security problems. Their system allows remote experts in turn to work in a secured surgery room. Cryptographic security tools are used for token management among the surgeons. Coatrieux et al. [2] suggest using watermarking techniques to protect medical images. They discuss security issues and concentrate on solution to authentication and integrity of medical data. Anand et al. [3] propose to insert encrypted EPR in the LSB of the gray levels of medical-image pixel. Though the change to the medical image is less, however the LSB-embedding system is fragile. Macq et al. [4] propose security system by watermarking the root part of medical image inside the medical data-file. Existing security systems create problems and cannot provide complete security to the modern medical health care system. Firewalls provide a

certain level of isolation between the intra-net and Internet, but easily bypassed by hackers [2]. For storage and transmission cryptographic tools are very efficient, but once the sensitive data is decrypted, the information is not protected. Watermarking techniques provide authentication of images, but they are also fail to provide complete security, especially there may be some loss of information by compression-decompression system.

The complete security can be provided by using all types of security tools (dedicated security infrastructures, watermarking, and cryptographic tools) in medical information system. The security solution to a huge system like medical information system is highly expensive, establishment of *Public Key Infrastructure* (PKI), *Trusted Third Party* (TTP) are hard. Despite these challenges, we hope that with the advance of information technology the security tools such as PKI, TTP will be cost-effective and become part and parcel of a complete security solution to medical information systems.

Cryptographic Tools

Cryptographic tools provide effective security (confidentiality) systems. There are two types of cryptography: symmetric key cryptography and public key cryptography. The symmetric key cryptography (see Figure 1) encrypts message M (say an image) by a secret key K and return the cipher text encrypted message C : $C = E_K(M)$, where E is encryption algorithm. The decryption process is opposite of the encryption process: $M = D_K(C)$, where D is decryption algorithm. There are several symmetric key encryption algorithms among which *Data Encryption Standard* (DES), triple-DES, *International Data Encryption Algorithm* (IDEA) are well known.

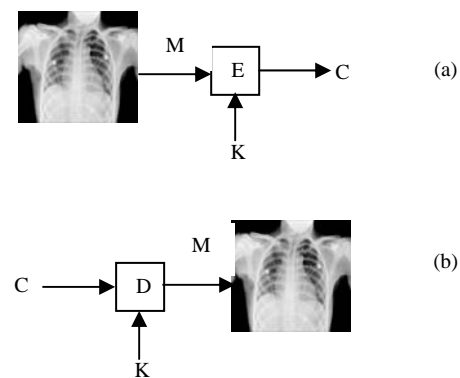


Figure 1: Symmetric key cryptography (a) encryption and (b) decryption

The public key cryptography requires two keys: public key K_u and private key K_r . The public key is known to all and people use this key to send information destined to the holder of the key: $C = E_{K_u}(M)$. The decryption algorithm is essentially same as the encryption algorithm. The private key is only known to the holder of the key. Upon receiving a message, the holder uses his private key to decrypt it: $M = D_{K_r}(C)$. The sender also sends (signs) messages by encrypting with his private key. Among the public key cryptographic tools *Rivest-Shamir-Adleman*

(RSA) algorithm [5] and *Diffie-Hellman* key exchange algorithm [6] are the most useful. The public key cryptography can ensure confidentiality, authentication and non-repudiation. From Figure 2, for example, user A encrypts an image X first with his private key K_{ra} (gets intermediate encrypted message Y) and then with B 's public key K_{ub} (gets final encrypted message Z); user B upon receiving Z decrypts the message first with his private key K_{rb} (gets Y) and then with A 's public key K_{ua} (gets original image X). Due to encryption with B 's public key by A , nobody except B can decrypt it (confidentiality), since A encrypts with his private key he cannot refuse the transmission (non-repudiation), also since B decrypts message with A 's public key the sender must be A (authentication). In Figure 2, E means encryption algorithm, whereas D means decryption algorithm. The public key cryptography is also useful for secret or session key distributions and digital signatures to sign digital data.

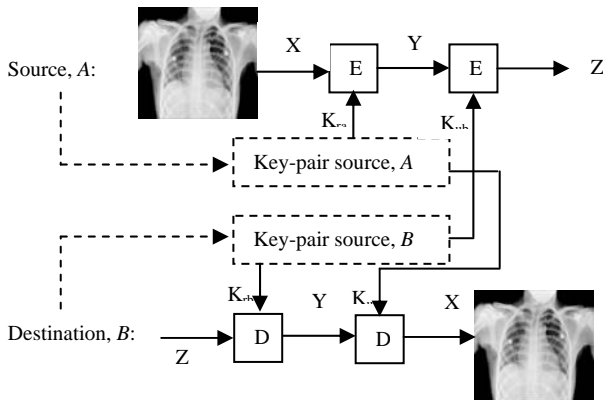


Figure 2: Public key cryptography

One-way hash (message digest) functions are helpful to generate digital signatures or *Message Authentication Code* (MAC): $h = H(M)$. A long message M is signed by a unique short message h (128-bit or 160-bit) and we cannot get back M from h anyway. Two most useful hash functions are *Message Digest Algorithm 5* (MD5 algorithm), gives 128-bit message digest [7], and *Secure Hash Function* (SHA-1), gives 160-bit message digest [8]. To check the integrity of a message hash is a highly useful tool.

The problem with public key cryptography is who takes the responsibility to create and distribute private-public key pair for each entity, and how to publish public keys. The establishment of public key authority or trusted third party is needed to have a public key infrastructure by issuing and validating public key certificates. In Figure 3, we see a certificate authority works as the TTP between two parties A and B. Entity A generates its private-public key pair and sends the public key (K_{ua}) to TTP which, thereafter, sends a certificate, $C_a = E_{krAuth}(Time1, Id_a, K_{ua})$, back to A. $Time1$ is used to evaluate the age of the certificate; if a certificate is sufficiently old, then it is assumed to be obsolete. A periodically generates new key-pair and certifies with the TTP. Id_a is the information about A and $krAuth$ is the private key of the TTP. Anybody

that knows the TTP's public key (K_{rAuth}) can verify A's public key: $D_{K_{uAuth}}(C_a) = D_{K_{uAuth}}(E_{krAuth}(Time1, Id_a, K_{ua})) = (Time1, Id_a, K_{ua})$. B goes through the same process. Then A and B exchange their certificates and they can start their secure communication.

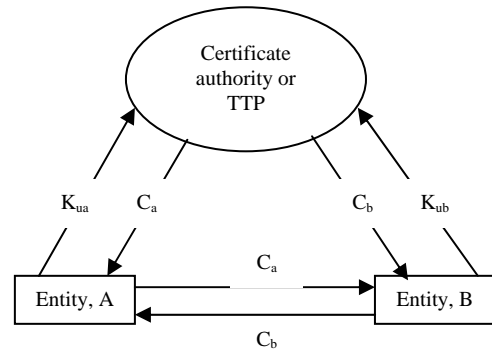


Figure 3: Exchange of public-key certificates

Nevertheless, such infrastructure of TTP and PKI is highly expensive. As an effective solution we propose the hospital authority to be the local-TTP to establish PKI inside the hospital.

The Lossless Watermarking

Lossless watermarking or reversible data hiding is a branch of fragile watermarking that hides authentication information (say hash) and private data inside the original (medical) image. When needed the hidden data can be retrieved and the exact copy of the original image can be found from the watermarked image.

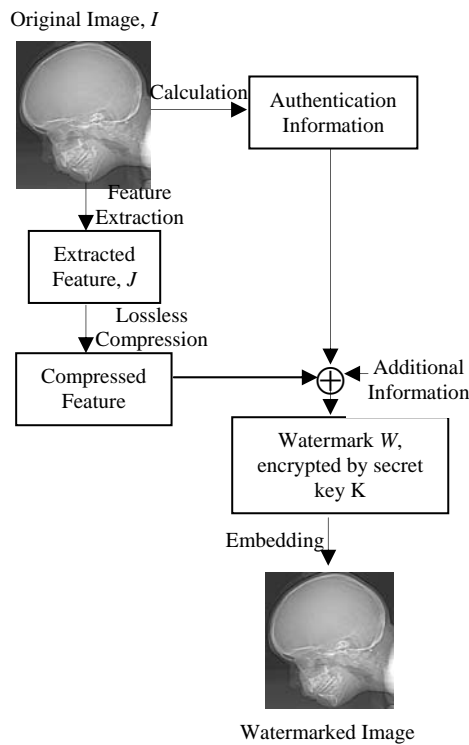


Figure 4: The general principle of lossless watermarking

The general principle [9] (see Figure 4) of reversible data hiding is that for a digital object (say a JPEG image file)

I , a subset J of I ($J \subset I$) is chosen. J has the structural property that it can be easily randomized without changing the essential property of I , and it offers lossless compression itself to have enough space (at least 128 bit) to embed the authentication message (say hash of I). During embedding J is replaced by the authentication message concatenated with compressed J . If J is highly compressible only a subset of J can be used. During the decoding process authentication information together with compressed J is extracted. This extracted J (compressed) is decompressed to replace the modified features in the watermarked image; hence the exact copy of the original image is found.

Encryption of watermark (bit-string to be added) with a secret key K before embedding provides additional security to active attacks. Additional information added with the authentication information (hash) includes patient's id, medical-report, doctor's id, laboratory-id, and so on. Since decoding method is just reverse of embedding method we represent only embedding method. A lot of lossless watermarking algorithms have been proposed in the literature. Some of them are in [9, 10, 11, 12, 13, 14, 15]. To calculate the hash we can use either MD5 (128-bit) [7] or SHA-1 (160-bit) [8] algorithms.

Users in the Medical Information System

To make the medical information system understandable we have to know users inside and outside the medical. Macq et al. [4] define several users of medical information system:

Producer produces medical-images. He creates initial record consists of physical condition, patient name, date of image production etc.

Referring Physician is the diagnostician. He may ask a complement diagnosis from an external specialist, the external diagnostician. He summarizes the whole description in its diagnosis.

External Diagnostician is the expert outside the hospital. The referring physician may seek help from him to make the test report complement.

Intra-users are people inside the hospital and complement the information related to the patient from extra-users. They see image file as a dynamic element of computerized patient-records.

Extra-users are authorized persons outside the hospital and have less right on the patient records. They access light proprietary format of medical images.

Packager is responsible for encoding, decoding, and managing the image transmission.

THE PROPOSED HIERARCHICAL MODEL

Figure 5 shows our proposed general hierarchical model. In this tree model each Laboratory Information System (LIS) is a leaf, each Hospital Information System (HIS) is a parent of some LISs and each State Medical Information System (SMIS) is a parent of all hospitals residing inside the State. There is no unique root of the tree, so we avoid the need of establishing global TTP. Often there are many laboratories inside and outside of a

hospital for different kinds of medical testes. Two LISs can communicate directly if their parent HIS is same. If they reside in different HISs then they have to communicate through their parent HISs. Similarly, two HISs under same SMIS can communicate directly but two HISs residing in different States communicate through their SMISs. We will discuss each part of the tree in the following sections.

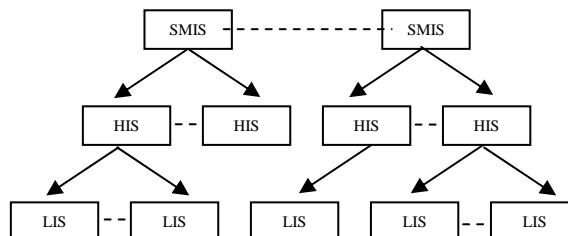


Figure 5: The general hierarchical model of proposed security solution

In the following discussion if nothing is mentioned we assume that any message transmitted through the network is double encrypted by the sender with his private key and receiver's public key. The receiver decrypts the message with his private key and sender's public key. Any personal-id (say patient-id) is the social security number of that person and organization-id (say lab-id) is the registration number of that organization.

The Laboratory Information System (LIS)

Figure 6 shows a proposed laboratory information system (LIS). The patient goes to hospital and the doctor in the hospital sends him to the laboratory if any tests are required.

The *Image Production* unit in the laboratory is a computer based system that generates image as required and sends message $M1$ to *LabDoctor* (*Referring Physician* – specialist of the test being processed). $M1$ consists of medical-image, date and time of image production, image-id, and patient-id. At the same time *Image Production* unit sends $M3$ to *Lossless Watermarking System* and *Check Integrity*. $M3$ is the hash of the image together with date and time of image production, image-id and patient-id. The *LabDoctor* after decrypting message $M1$ appends his own report with decrypted $M1$ and sends $M2$ to *Check Integrity* unit. If he wants the report to be complemented he sends $M2$ to *LabCryptoSystem* unit instead of to *Check Integrity* unit. The *LabCryptoSystem* sends message $M4$ to *External Doctor* (external diagnostician). The *External Doctor* does the same work as the *LabDoctor* and after appending his report to decrypted $M4$ he sends back $M4$ to *LabCryptoSystem* unit. The *LabCryptoSystem* sends back updated $M2$ to *LabDoctor* who summarize the report and sends to *Check Integrity* unit. The *Check Integrity* unit recalculates the hash of the image it received from *LabDoctor* and compares with the hash it received from *Image Production* unit. If comparison says 'yes' it sends $M6$ to *Lossless Watermarking System*

where additional message M5 is provided by *Additional Information* unit. M5 consists of all the information needed to be hidden inside the medical-image such as lab-id, *LabDoctor*-id, *External Doctor*-id, hospital-id, *HosDoctor*-id, state-medical-id etc. The *Lossless Watermarking System* losslessly compresses all the information to be hidden, agrees a secret key (Mk) with *LabCryptoSystem*, and encrypts the compressed information before embedding. After embedding it sends watermarked image (M7) to *Lossless Compression* unit that sends M8 to *LabCryptoSystem* after lossless compression. The *LabCryptoSystem* sends M9 to *LabDatabase* (lab image archive) and M10 to the HIS. The *LabDatabase* stores decrypted M9 after encrypting with a secret key (agreed with *LabCryptoSystem*). M10 consists of decrypted M8 and the secret key used to encrypt watermark before embedding by *Lossless Watermarking System*.

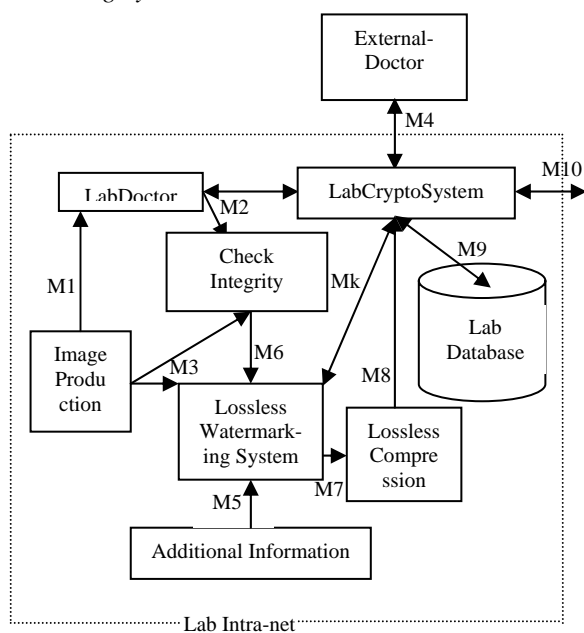


Figure 6: The laboratory information system (LIS)

The Hospital Information System (HIS)

Figure 7 shows a proposed hospital information system (HIS). It receives medical images from LISs residing in or out of the hospital.

The *HosCryptoSystem* upon receiving M10 from the LIS sends Mk to *Lossless Watermarking system*, and M14 to *Lossless Decompression*. Mk contains the secret key used to encrypt watermark by the LIS. M14 is just the compressed watermarked image. The *Lossless Decompression* unit sends decompressed watermarked image to *Lossless Watermarking System* (M11) and *HosCryptoSystem* (M14). The *Lossless Watermarking System* separates the original medical-image, medical-report, hash, and additional information. It sends (M17) hash and original image to *Check Integrity* unit. The *Check Integrity* unit recalculates the hash of the original image and compare with received hash. It sends comparison result to *Lossless Watermarking System* that

upon receiving a positive response sends (M16) patient-id, image-id, medical-report, and original medical image to *Internal Security System*. The *Internal Security System* sends (M18) decrypted M16 to the respective *HosDoctor* to whom the patient first had met before taking the image at the LIS. The *HosDoctor* take necessary decision as prescription for the patient. He also sends his prescription to *HosCryptoSystem* that appends it to the watermark with the help of *Lossless Watermarking System*. The *HosCryptoSystem* sends M12 to *Hospital Database*. M12 contains the compressed watermarked image, and a secret key. The secret key is used to encrypt the compressed watermarked image before storing by *HosDatabase*. The *Lossless Watermarking System* also sends (Mk) medical report, patient-id, and additional information to *HosCryptoSystem* that sends M13 to the *Patient*, and M15 to the *State Medical Information System (SMIS)*. M13 consists of watermarked image, and medical-report. The *Patient* stores it in his computer system for future use, especially for legal case. M15 consists of patient-id, medical-report, lab-id, hospital-id, prescription etc. The SMIS uses this data to exchange information with hospitals and experts in and out of the State, and also stores data for future uses.

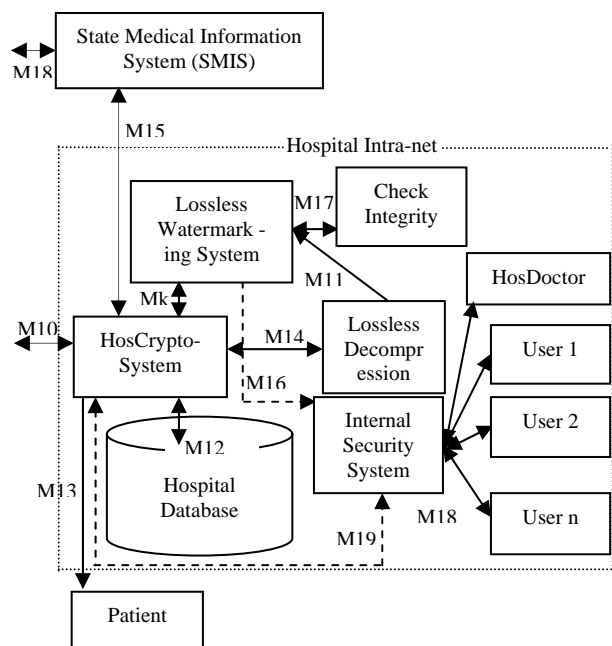


Figure 7: The hospital information system (HIS)

How to Get Help from an Expert Doctor or an Advance Hospital

If the *HosDoctor* wants to get help from an expert in or out of the State he sends a request (M18) to *Internal Security System* with necessary information. The *Internal Security System* forwards this request to the *HosCryptoSystem*. The *HosCryptoSystem* contacts to *Lossless Watermarking System* that encrypt the watermark with a secret key (previously agreed between this hospital and authority of the expert doctor being communicated) before embedding to the original image. If the requested expert is in another hospital of the State,

the *HosCryptosystem* sends corresponding watermarked medical-image (M10) directly to the hospital where the expert resides. If the expert is outside the State it sends (M15) watermarked image to the SMIS together with necessary information about the patient and the external expert. The SMIS takes the necessary actions. It sends the watermarked image to the hospital residing in abroad. It may also send previous medical reports, life medical-history of the patient etc. upon request by the external expert. The SMIS could contact the hospital in abroad either directly or through the SMIS in abroad as defined by the security policy. The external expert sends back his prescription through his hospital to the SMIS that forwards it to *HosDoctor* through *HosCryptoSystem* and *Internal Security System*. The *HosDoctor* prepares the final prescription for the patient. The SMIS and *HoscryptoSystem* also update the medical-report, documents of that patient as necessary with the help of *Lossless Watermarking System* unit.

If it is necessary the local hospital can shift the patient to an advance hospital in or out of the State. Moreover, financially capable patient can go to an advance hospital in abroad. In that case the SMIS does the same actions by sending the necessary watermarked image, documents, life medical-history of the patient.

How the Complete Security is Ensured

We propose to use the public key cryptography for each communication in and out of the hospital and laboratory. The security services like *non-repudiation*, *confidentiality*, and *authentication* are fulfilled by public key cryptography. The transmitted information is confidential because nobody could read it except the senders and receivers. Neither senders nor the receiver could deny the transmission because the transmitted message is double encrypted with sender's private key and receiver's public key, hence non-repudiation service of security is established. Since only the sender holds his private key (secret key) authentication is also maintained. We maintain *integrity* of the medical-image by embedding its hash as a part of the watermark. Moreover, we encrypt the watermark before embedding with a secret key which provides additional security against active attacks to the watermarked image trying to change the watermark.

How to Avoid Expenses to Establish Global PKI and TTP

The authority or authorized system inside the laboratory acts as TTP for this laboratory. It creates (using RSA algorithm [5]) and assigns a pair of private-public keys to each unit or entity within the Laboratory. The TTP also publishes all the public keys used by different entities inside the laboratory. The units working there must abide by the security policy taken by the TTP. Similarly the authority of the hospital is the TTP of the hospital and the SMIS is the TTP for all the hospitals and laboratories of the State. The SMIS creates and assigns a pair of private-public keys to each laboratory or hospital in the State.

While communicating with the hospital or another SMIS outside the State it makes secret shared session key agreement using *Diffie-Hellman Key Exchange* protocol [6]. The key used to encrypt watermark before embedding is assigned by the corresponding TTP (for watermarked image communicating inside the hospital or laboratory) or the receiver's public key (for watermarked image communicating between laboratories and hospitals of the State) or the secret session key being agreed between two States (for watermarked image communicating across the State).

CONCLUSIONS

In this paper we propose a complete security system for transmitting medical-images through the open network in modern health care system. It ensures the most required security services like integrity, confidentiality, non-repudiation, and authentication. It provides additional security policy to avoid cost of establishing global TTP and PKI. The local TTP and PKI inside the hospitals and laboratories do the necessary works as required. Only necessary software tools like RSA algorithm, *Diffie-Hellman* key exchange protocol, and lossless watermarking algorithm are needed to implement this proposed security solution. We use lossless watermarking technique to hide confidential patient information inside his medical image so that we can make the exact copy of the original image available to the physicians when necessary. The *Diffie-Hellman* key exchange protocol is helpful to establish a secure transmission between two parties. We can avoid global PKI or TTP while communicating two hospitals in different countries by using *Diffie-Hellman* algorithm. The RSA algorithm is helpful to provide private-public key pairs to entities by local TTP.

REFERENCES

- [1] Yang Y, Bao F, Deng R (2003) Secure an image-based simulated telesurgery system. Institute of Infocomm Research, Singapore, URL: http://icsd.i2r.org.sg/publications/BaoFeng_2003_tesurgery.pdf
- [2] Coatrieux G, Maitre H, Sankur B, Rolland Y, Collorec R (2000) Relevance of watermarking in medical imaging. In: Proceedings of the IEEE EMBS International Conference on Information Technology Applications in Biomedicine, pp 250-255, November 9-10, 2000
- [3] Anand D, Niranjana UC (1998) Watermarking medical images with patient information. In: Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, vol 2 pp 703-706, October 29 - November 1, 1998
- [4] Macq B, Deweyand F (1999) Trusted headers for medical images. In: DFG VIII-DII Watermarking Workshop, Erlangen, Germany, October, 1999, URL: citeseer.nj.nec.com/macq99trusted.html
- [5] Stallings W (1999) Cryptography and Network Security. Second Edition, Prentice Hall, New Jersey, pp 173-178

- [6] Stallings W (1999) *Cryptography and Network Security*. Second Edition, Prentice Hall, New Jersey, pp 190-193
- [7] Stallings W (1999) *Cryptography and Network Security*. Second Edition, Prentice Hall, New Jersey, pp 272-278
- [8] Stallings W (1999) *Cryptography and Network Security*. Second Edition, Prentice Hall, New Jersey, pp 281-285
- [9] Fridrich J, Goljan M, Rui D (2002) Lossless data embedding for all image formats. In: *Proceedings of SPIE Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, California, vol 4675 pp 572-583, January, 2002
- [10] Celik MU, Sharma G, Tekalp AM, Saber E (2002) Reversible data hiding. In: *Proceedings of International Conference on Image Processing*, Rochester, New York, vol 2 pp 157-160, September 24, 2002
- [11] Ni Z, Shi YQ, Ansari N, Su W (2003) Reversible data hiding. In: *Proceedings of International Symposium on Circuits and Systems*, Bangkok, Thailand, vol 2 pp 912-915, May 25-28, 2003
- [12] Vleeschouwer CD, Delaigle JF, Macq B (2001) Circular interpretation of histogram for reversible watermarking. In: *The IEEE 4th Workshop Multimedia Signal Processing*, pp 345-350, 2001
- [13] Xuan G, Chen J, Zhu J, Shi YQ, Ni Z, Su W (2002) Lossless data hiding based on integer wavelet transform. In: *The IEEE International Workshop on Multimedia Signal Processing*, Marriott Beach Resort St. Thomas, US Virgin Islands, December 9-11, 2002
- [14] Tian J (2002) Wavelet-based reversible watermarking for authentication. In: *Proceedings Security and Watermarking of Multimedia Contents IV, Electronic Imaging 2002*, vol 4675 pp 679-690, January 20-25, 2002
- [15] Awrangjeb M, Kankanhalli MS (2003) Lossless Watermarking considering the human visual system. In: *International Workshop on Digital Watermarking*, Korea, October 20-22, 2003