Singapore Management University
Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems

School of Information Systems

5-2003

Secure the image-based simulated telesurgery system

Yanjiang YANG
Institute for Infocomm Research, Singapore

Zhenlan WANG
Institute for Infocomm Research, Singapore

Feng BAO
Institute for Infocomm Research, Singapore

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

DOI: https://doi.org/10.1109/ISCAS.2003.1206044

Citation

YANG, Yanjiang; WANG, Zhenlan; BAO, Feng; and DENG, Robert H.. Secure the image-based simulated telesurgery system. (2003). *ISCAS 2003: Proceedings of the IEEE International Symposium on Circuits and Systems, May 25-28, Bangkok, Thailand.* 2, 596-599. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/1084

Secure an Image-based Simulated Telesurgery System

Yanjiang Yang, Feng Bao, Robert Deng

Institute of Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
{yanjiang, baofeng, deng}@i2r.a-star_edu.sg

Abstract. Securing telemedicine services is essentially a critical and urgent topic. However, in many existing telemedicine systems security related issues are seldom seriously considered. In this paper, we introduce an image-based simulated system for kyphoplasty telesurgery, wherein special attentions are drawn to address the security problems. Among others, various security requirements of the system are formalised, and solutions to meet these requirements are presented. Consequently, we implement the system to work in a secure way. In fact, our methods can be applied to a class of similar telemedicine services. To implement this system, we take efficiency as our premier consideration.

Keyword: Simulated System; Telemedicine; Telesurgery; Kyphoplasty; Digital Signature; Authentication, Hash Function; Image Hashing Function; Symmetric Cipher; Public-key Cryptosystem.

1 Introduction

Accelerated by the advances of information technology as well as the wide deployment of high-speed computer networks especially Internet, telemedicine services have gained great progress in recent years. Telemedicine refers to the provision of clinical care, education and many other clinically significant value-added services over a distance, using advanced telecommunication infrastructures. Its main goal is set to share valuable expertise and resources to a wider extent by providing different levels of support for remote monitoring, diagnostic and therapeutic medical procedures. The environment in which telemedicine services can be provided is summarized in [1] as a tri-layered structure, named from top to bottom as services layer, application layer and infrastructure layer. These layers well define the constituting elements of telemedicine: medical applications (procedures), information technology such as image processing, audio, video, database, etc., underlying hardware infrastructures including computer networks and service-specific appliances. Clinical applications of telemedicine are now found in virtually every specialty, among which telediagnosis, telemonitoring, teleconsultation, telemanagement, tele-education [2] are an assortment of typical telematic services. Telemedicine reflects the convergence of technological advances in a number of fields, including medical procedures and medicine.

Just like e-commerce, etc., telemedicine is a product and then a valuable tool of information society. We are more or less familiar with the traditional health care paradigm: a patient must first go to the hospital and the treatment can only recur to the doctors and experts within that hospital, and if needed the patient will be kept hospitalized. We note that actually not all cases are serious enough to undergo the same stubborn routines. Therefore, such kind of working style is destined to be costly, in terms of both money and time. More importantly, with it there are not convenient ways to share expertise and resources to a wider extent. To see this, suppose a scenario that doctors in the local hospital are unable to tackle a case of a particular patient, they need to seek help from an abroad hospital. Most possibly, an expert has to travel a long way to help while the ultimate help proves to be just an analysis of certain MRIs of the patient. Telemedicine changes such embarrassing circumstances significantly. In this case, the abroad expert can stay home to examine the patient's MRIs delivered through telemedicine services, avoiding long way journey, and responds accordingly also through telemedicine services. It is evident that compared with conventional health care protocols, telemedicine works in a more cost-effective and timely fashion. Telemedicine extends existing health care system and revolutionizes traditional working paradigms, benefiting both medical community and patients. Take chronic wounds healing in [3] as an example: according to the authors, in U.S. approximately 5 million patients generate annual costs for chronic wound care in excess of $20 billion in 1996, growing 10% annually. They estimated that by using the home-oriented tele-WMS (wound management system), there can be totoally $5.7 billion or an estimated cost of $37,825/client savings, coming primarily from (1) cost savings for hospitals by shifting patients to the home care environment and thus increasing patient population by sharing resources such as doctors, nurses and medical facilities. (2) Less expense of patients for shortened lengths of hospitalisation and less emotional costs at home-setting. They thus conclude that chronic wound care through telemedicine promises to be competitive in the managed care environment and will provide organizational, technological, and financial incentives. In summary, potential benefits of telemedicine services include improved access to diagnostic facilities, reduced costs (less travel and work-leave expenditure, etc.), reduced isolation for both patients and medical personnel, improved quality of health care through real-time diagnosis, increased collaboration and continuous education, and direct access to remote computational facilities for advanced image processing and 3D visualization [1, 4, 5]. Therefore, despite it is far from maturity as there are a multitude of regulatory, legal, ethical issues and technical impediments it has to wrestle with [6], telemedicine is substantially expected to be valuable and indispensable assistance to the medical community.

Telemedicine by definition are services involving exchange of text files, medical diagnostic imaging modalities, audio, video-clips over computer networks (even Internet) to a regional, national, or global scale, so it faces the same security challenges during information transmission as the interbank electronic transfer of funds. In fact, data security and information privacy is not a new issue in health care community. For example, There have been a great number of standards, models, policies and proposals to regulate the management of personal patient data and information (among others, for example [7-16]). However, they are more on the protection of confidentiality and integrity of stored clinical data (records) or information flow in the context of clinical information system than safeguarding the delivery of clinical data in multimedia form or the communication itself as needed in telemedicine. Medical data and services are essentially security and integrity sensitive, which determines security considerations are inevitable in telemedcine or in other forms of comprehensive communication and co-operative environment for health care. With the advent of substantial development in telemedcine, more and more attentions are drawn to those issues such as privacy, security, integrity, authentication, access control and etc., in both communication and applications. Health care Informatics Standards Board (ANSI HISM), American Health Information Management Association (AHIMA), American Medical Association (AMA), European Standardization of Health Informatics Enabling Health Care Communication and many other organisations around the world are dedicated to standards establishment and management for health informatics security, focusing on those adaptable to the Internet era. In the meantime, a large amount of literature begins to discuss securing health care services, applications and systems over Internet [1, 17-22]. Security is growing into a hot topic in the field of telemedicine.

Contrast to the high academic research enthusiasm for security, it seems the developers of telemedicine applications and systems are sluggish to follow suit. There have many telemedicine systems been developed [3, 23-28], wherein security issues were rarely considered, so as to even some systems that began to touch such issues merely restricted themselves to some simple forms of protection such as password protection. For example, once a user inputs correct passwords to use the system in [28], he can use it without any further restriction. These systems impliedly assume that the information transmission channels are safe, which we know it is not the case in practice. We owe this situation mainly to the following reasons. First, most of the developers' efforts were gone into solving service-specific technical problems of these systems. Whatever types of these systems, they each face technical difficulties and immaturity in their fields. Take teleradiology, the most common application among telemedicine for instance, advanced techniques for data fusion, synthetic imaging, visualisation, efficient and intelligent management of huge volume of multimedia patient data will remain a challenge [1]. Second, security implementation will inevitably impose additional cost as well efficiency penalty. Efficiency of the hardware infrastructure such as medical workstations, transmission networks has long been the endeavouring direction. Third, problems within the field of cryptography and security themselves prevent effective security implementation. For example, establishment of PKI, involvement of Trust Third Parties (TTPs) in some cryptographic protocols are practically hard. Despite these challenges, as technology advances we optimistically believe that security implementation will eventually be an integrant part of the telemedicine engineering in the near future, gaining the same importance as in electronic banking transactions and in e-commerce.

In this paper, we present an image-based simulated system for kyphoplasty surgery, categorised into telesurgery, an important kind of telemedicine service. What differentiate ours from other literature describing telesurgery systems in that we instead concentrate dominantly to solve the security issues involved in this system. In what follows, we describe the system framework from functionality perspective in section 2. Section 3 gives methods and implementation of the system, with special attentions given to security related issues. Finally, conclusion is drawn in section 4.

2 Functional Framework

We observe that a surgery is normally conducted by a group of co-operative surgeons, each, with necessary expertise for a particular part, in turn performing a step. Therefore, for simulation purpose, a real-world surgery process can be modelled as a series of sequential steps, each completed by one of the several participating surgeons who are in collaboration to perform the surgery. Motivated by this, our image-based telesurgery system simulates the sequential steps involved in a typical kyphoplasty surgery, allowing several surgeons in turn to complete his work. To this end, a surgery room originating, managing and monitoring the simulated surgery process and several remote participants constitute our system.

A kyphoplasty surgery is literally a minimally invasive surgical procedure for treating osteoporotic fractures, aiming to stabilise the bone, and to restore some or all of the lost vertebral body height due to the compression fracture. Three sequential steps constitute the whole surgery process.

- Step 1: A small incision is made in the back through which a surgeon places a narrow tube. Using fluoroscopy to guide it to the correct position, the tube creates a path through the back into the fractured area through the pedicle of the involved vertebrae.

- Step 2: Using X-ray images, a surgeon inserts a special balloon through the tube and into the vertebrae, then gently and carefully inflates it. As the balloon inflates, it elevates the fracture, returning the pieces to a more normal position. It also compacts the soft inner bone to create a cavity inside the vertebrae.
- Step 3: The balloon is removed and a surgeon uses specially designed instruments under low pressure to fill the cavity with a cement-like material called polymethylmethacrylate (PMMA). After being injected, the pasty material hardens quickly, stabilising the bone.

Based on this, our system provides a simulated environment for three participants (front-end terminals together with participating surgeons), apart from the surgery room, to complete the 3-step procedure, each responsible for a step. Within the context of the simulated system, we obscure the difference between a participant and a surgeon. The participants conceptually locate separately as the system is intended for telesurgery purpose. The reason justifying our design of multi-participants involvement is that we conjecture our system as a generalised framework of a class of similar telesurgery services. In this sense, this system can be quite easily adapted to the case of "surgery room-to-one participant". Moreover, we presume that the participant of each step is only experienced in that particular step. In fact, it is relatively hard to find someone who is good at everything. So our design is especially conducive for those managing the surgery room to collect expertise from different participants. This is exactly a key goal of the system. Central to our system are: (a) the three steps must be completed in sequence, i.e., only after step 1 is finished can step 2 begins and step 3 does not proceed until step 2 ends. (b) Each participant is strictly restricted to complete the functionality of his step only. This restriction aims to avoid random operations by the participants as we assume a participant is only expertised in his step. Suppose the three participants are Surgeon A (to perform step 1), Surgeon B (to perform step 2) and Surgeon C (to perform step 3), respectively, the functional framework of the system is sketched in Fig. 1.

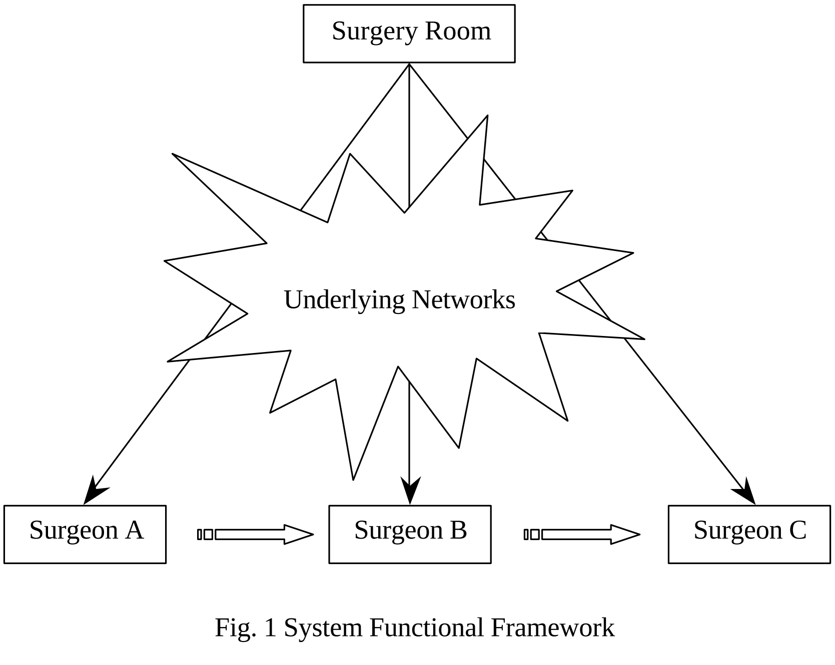

Fig. 1 System Functional Framework

In this simulated environment, three participants, presumably Surgeon A, B, C are performing a "kyphoplasty surgery" originated by Surgery room. It works as follows. Surgery room simultaneously distributes patient data (3D images) to the participating surgeons. Real-word operations on the patient by the surgeons are simulated by means of their modifications to the patient data (images). Each image is segmented (preferably by pre-processing) by automatic segmentation [29-31] or simply manual segmentation methods into parts so that each surgeon is restrained his privilege (modifications) to his own part. A surgeon cannot modify outside his part. Simulated surgery procedures are done in a sequential manner. Surgeon A takes the first turn to modify the image, completing above step 1. Afterwards Surgeon B continues to complete step 2 upon verifying that prior modifications are indeed made by Surgeon A and within the allowed range. Surgeon C takes step 3 following the work by B in a similar way. In the end, Surgery Room gets a complete simulated process for a kyphoplasty surgery after three participants finishing their steps respectively.

Our simulated system has many applications. It serves the following purposes.

- ♦ Training and education. With the development of information technology in both hardware and software, especially multimedia processing techniques, training using simulation systems for students, practitioners, and medical staffs more and more becomes a common practice. Obviously our system can provide a simulated environment for kyphoplasty surgery for the purpose of training and educaiton.
- ♦ Pre-surgery practice and planing. Prior to a real surgery, doctors or surgeons can learn to work in co-operation, can practise to plan the real surgery process, can gain enough proficiency and confidence, by using our system as a practising platform. Moreover, the doctors managing Surgeon Room are able to share expertise and experiences through the system from remote experts.
- ♦ On-line assistance to a real-world surgery. Imagine this scenario: a real surgery is going on, paralleled by our simulated system. Real-time patient data are continuing to be delivered over the system to remote experts who are joining in the system as participants. In this way, doctors in the real surgery are easy to get hints and guidance from the remote experts, which are especially useful when they are got trapped into dilemma.

3 Methods and Implementation

Security is a critical issue in our system. For example, suppose doctors, to plan a surgery process, use the system to accumulate knowledge from other experts. If the patient data transferred over the network were changed by malicious accesses, then the doctors would definitely be misguided and disastrous sequences are highly possible. For another use of our system, namely real-time assistance to an ongoing surgery process, security implementation is obviously in a more urgent demand.

3.1 Security Requirements

Key issues in the design and development of a telemedicine system include information integrity during transmission, authentication of submitted images and related data, and protection from unauthorised access [2]. In particular, we formalise security requirements for our systems in the following ways.

- ❑ **R1**: Encryption

Information flow between Surgery Room and participants, participants and participants must be encrypted to avoid inappropriate disclosure of patient data and to protect privacy and confidentiality of communication content.

- ❑ **R2**: Integrity

Measures must be taken to ensure that data travel safely against active and passive attacks during transmission, without being altered and compromised.

- **R3**: Identification and Authentication

Provision must be provided to ensure authenticity of all involving parties. In particular, all participants can verify the images (patient data) distributed to them are indeed from Surgery Room; Surgery Room and other participants must be guaranteed that modifications to the images (patient data) are done by the desired person as described later.

- **R4**: Sequential Operations

Recall that a central point of our system is that operations are done in a sequential manner. Thus ways must be supplied to guarantee every participant takes his turn to complete the functionality of his step.

- **R5**: Access Control

Another uniqueness of our system is that we restrict each participant to operate only in his part. In other words, a participant can only modify the patient data within the part to which he has been assigned privilege. Modifications outside his range are presumed to be illegitimate accesses.

3.2 Implementation

In this section, we present detailed implementation of the system, fulfilling above security requirements. Note that efficiency is a major concern to implement this system. In what follows, we will first in turn examine our considerations and solutions to the system security requirements listed above.

Solution to **R1** (**S1**): We choose a symmetric cipher rather than a public-key cipher to protect data and information privacy in our system for the former transcends the latter in terms of efficiency. We refer to encryption algorithm and decryption algorithm of the symmetric cipher as $E_K(.)$ and $D_K(.)$ respectively, and the secret key as K. All communications over the system are protected under this symmetric cipher. K, essentially a session key, does not keep fix, whereas varies from session to session. A *session* starts with Surgery Room beginning to dispatch an image to the participants and ends with every participant finishing his operations. Normally Surgery Room determines K and distributes it to the participants via a secure channel. Key distribution is a problem as we assume communication channels of the system are insecure. As we will see later, secure channels can be established by the public-key cryptosystem employed for authentication.

Solution to **R2** (**S2**): Normally, one-way hash functions are used to guarantee integrity of the data being transferred in such a way that hash value of the message is appended to the original message and they are transferred together. Upon checking, the receiver computes the hash value using the message and then compares it with the appended hash value, if the two are same, then the message is safely transferred. A characteristic of hash functions makes them extremely suitable to ensure data integrity, that is even one bit of input alteration will result in drastic changes in their outputs. However, in our system exactly this property hinders standard hash functions such as MD5 and SHA directly applied. For one thing, we know our system involves transmission of medical images over long-range telecommunication networks, thus transmission error is inevitable despite error detection mechanisms provided by the various levels of the network architecture [32]. For the other, these medical images possibly undergo various nonmalicious manipulations such as enhancement, format changes, etc., so small changes are assumed to be acceptable. With these, it makes sense to allow our system for insignificant changes to uncritical parts of the images. In fact, within a patient data image, only parts around the fractured area are of real interest (ROI, Region of Interest) and need to be strictly protected (see for example in Fig. 2, we arbitrarily define the content between two lines to be ROI). Therefore, we hash our image data in a special way: apply a standard hash function to ROI and use an *image hashing function* [33, 34] to hash the remaining content. Let M be an image, m be the ROI and M' = (M - m) the remaining content, a standard hash function $h(.)$ and an image hashing function $f(.)$, then we refer to our hashing method as $H^{+}(M) = f(M', h(m))$.

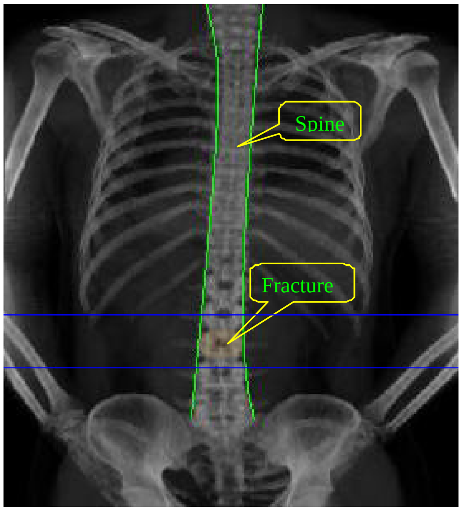

Fig. 2 A Patient Data Image

Image hashing functions are a special class of functions applicable to hash images in such a way that the hash values are expected to be invariant under perceptually insignificant changes to an image, whereas on perceptually distinct images the hash values need to be different. By applying $H^{+}(M)$, we mange to keep data integrity in our system in a flexible way that the sensitive data (ROI) are stringently protected while the less sensitive data are allowed for minor changes.

Solution to **R3** (**S3**): An involved party identifies himself using his distinct information such as IP address, by which other parties can reach him. Here we refer to Surgery Room as H_0, and surgeon A as H_a, surgeon B as H_b, and so on.

For authentication, we can choose between MAC and digital signature and we know using MAC is usually more efficient than using digital signature. Basically, there are two kinds of authenticating tasks in our system. First, the participants are able to ensure that the images they receive are indeed distributed by Surgery Room. We use MAC to this end, namely $H^{+}(M, K)$ with secret key K declaring the authenticity of Surgery Room. Second, it is important that a participant is able to identify some particular operations are indeed done by the surgeon as it claims. To this end, we choose digital signature instead of MAC to authenticate the operations as a particular signature can be generated only by the authorised holder. In particular, we choose a public-key system that can be used for both purposes of encryption and signature (such as RSA). We utilise its functionality of encryption as a secure channel for key distribution in S1. Also it will be used in S4. Each participant has a private key (sk) and a public key (pk), and we refer to the signing algorithm as $Sig_{sk}(.)$ and the verification algorithm as $Ver_{pk}(.)$, encryption algorithm as $E_{pk}(.)$ and decryption algorithm as $D_{sk}(.)$.

Solution to **R4** (**S4**): This is by definition a synchronisation problem. We use the concept of "token" as used in Token-Bus LAN [35] and Token-Ring LAN [36] to keep the surgeons operating in sequence. Generally, a participating surgeon does not know when it is his turn to work in advance, instead, Surgery Room manages this kind of things. We define a secret label, referred to as TOKEN, for the synchronisation purpose in our system. TOKEN is chosen by Surgery Room and distributed to the first participant. The first participant passes TOKEN to the second participant notifying the latter to operate after he has finished his task. Other participants work in a similar way. A participant cannot begin his operations without TOKEN. In the meantime, a participant always submits his operations together with TOKEN to prove that it is really his turn to operate.
To avoid operation chaos, we design the current TOKEN holder cannot know beyond next TOKEN holder in the operation chain. In other words, the first participant knows the second one only, and the second participant knows the third one only, and so on. We adapt the scheme protecting sequence itineraries of mobile agents [37] to our case. Surgery Room encrypts TOKEN in a nested way:

$$C_3 = E_{pk(c)}(H_b, H_c, H_0, \text{TOKEN})$$
$$C_2 = E_{pk(b)}(Ha, H_b, H_c, \text{TOKEN}, C_3)$$
$$C_1 = E_{pk(a)}(H_0, H_a, H_b, \text{TOKEN}, C_2)$$

$pk(a)$, $pk(b)$, $pk(c)$ are public keys of Surgeon A, B, C respectively as described in S3. When the system begins, Surgery Room sends C_1 to Surgeon A. Upon receiving it, A computes $D_{sk(a)}(C_1)$ to get (H_0, H_a, H_b, TOKEN, C_2) and checks C_1 indeed comes from H_0 and H_a is indeed the intended participant (himself). Next, Surgeon A passes C_2 to H_b after his operations. Once Surgeon B receives C_2, he computes (Ha, H_b, H_c, TOKEN, C_3) = $D_{sk(b)}(C_2)$ to get TOKEN and do similar verifications as Surgeon A does, and afterwards sends C_3 to Surgeon C. Similarly, C computes (H_b, H_c, H_0, TOKEN) = $D_{sk(c)}(C_3)$ and learns he is at the end of the operation chain, thus he returns TOKEN to Surgery Room who finally revokes TOKEN and ends current session.

Solution to **R5** (**S5**): To meet access control requirement, all image data need to be segmented by pro-processing as mentioned above. In Fig. 2, a patient data image is roughly segmented into the *spine* and the *rest part*. Among them, the fracture is again segmented as a special part out of the spine. Consequently, an *access control rule* for the image is set as Surgeon A is assigned privilege to the rest part plus the fracture while Surgeon B and C are restricted their operations within the spine. Surgery Room maintains an *access control table* whose entries are the above *access control rules*, each for a patient data image. When Surgery Room distributes an image to a surgeon, the corresponding access control rule related to him is sent too. The concept of access control rule facilitates access control check-up required in our system. In fact, a complete access control check-up comprises two steps: a preliminary access control check-up is conducted in the local site and a further check-up is done by Surgery Room. The latter aims to countermeasure against deliberate alterations of the local access control rule by a surgeon. As we will see later, only after the two-step check-up, can operations by a surgeon indeed take effect.

We know that managing many cryptographic keys practically is not an easy thing, so in our implementation, we intend to equip the participants with as few keys as possible. For example, the public-key cryptosystem employed in this system is used to its most, for digital signature as well as several encryption purposes.

In our system, the role Surgery Room playing is special, thus we differentiate it from participants. It originates the system and monitors entire simulated surgery process, i.e., validates every operation by the participants. More importantly, we design remote expertise sharing to be a main goal of the system, which is realised by managing Surgery Room. Integrating above solutions, our system works in a secure way as follows.

1. Pre-processing and initialisation.

Prior to the system beginning, all patient data images are segmented and access control rule for each image is set up. Surgery Room determines a secret key (K) for the symmetric key cryptosystem. Every participant chooses his private key (sk) and its corresponding public key (pk) for the public-key cryptosystem and makes public his public key. Once every participant logins into the system, Surgery Room sends him K through a secure channel defined by his pk, namely $C = E_{pk}(K)$. Each participant obtains $K = D_{sk}(C)$ using his sk.

2. Surgery Room originates the system by distributing a patient data image to all participants.

Surgery Room computes $C = E_K(M, H^+(M, K))$ and distributes C to every participant, where M is the image. Once receiving it, the participants decrypts $D_K(C) = (M, H^+(M, K))$ and checks integrity of the data image. In addition, distinct access control rule is sent to individual surgeon too, in the form of ciphertext by K. In what follows, all communications are assumed to be encrypted by K although we do not explicitly point out. $H^+(M, K)$ serves dual roles. First, as a MAC it undergoes integrity checking. Second, it is intended to prove the authenticity of M to the participants. We point out here that $H^+(M, K)$ authenticating M has a weakness: a cheating surgeon can dispatch images to other surgeons in the name of Surgery Room as every surgeon knows K so far. However, as we will see later, this is not a real problem because before operations by a surgeon come into effect, they will undergo a ultimate access control check-up by Surgery Room and then Surgery Room can easily detect such kind of cheating behaviour.

3. Each surgeon in turn finishes his operations.

It is essential that operations by a surgeon (modifications to his local image) simultaneously change other remote copies in Surgery Room and all other surgeons too. So subsequent surgeons can continue to accomplish their own operations on the basis of previous results and Surgery Room can acquire an entire simulated surgery process when every surgeon finishes his step. There are two viable ways to achieve this. One straightforward way is that the surgeon sends his resulted image to others. The other way is that the surgeon sends his actions taken in the local site to others and these actions are re-rendered there. We prefer the latter as the amount of data in communication will be significantly reduced. To do this, we formalise actions into a uniform form understandable to all involved parties. For example, a tube insertion action in step 1 is modelled as <*start point*, *angle*, *distance*>; a balloon inflation action in step 2 is <*colour changed*, {*a set of points*}> and cavity filling actions in step 3 can be expressed in an analogous way. We refer to a semantic <.> as an ACTION. ACTIONs are surrendered in the form of transaction [38]. A *transaction* comprises transaction ID, time marker T and a series of ACTIONs, namely (ID, T, {ACTION}). T serves to synchronise operations among surgeons (as described later) as well as prevent replay attack. After a transaction is submitted, local site will lead a preliminary accesses control check-up according to the local access control rule. Once confirmed positively, the transaction will be signed as Sig_{sk} ((ID, T, {ACTION})) by the surgeon's sk and then sent to Surgery Room as well as the transaction queues of all other surgeons. Each surgeon gets the transaction out of his transaction queue, verifies it using $Ver_{pk}(.)$ and waits for the transaction confirmation from Surgery Room. In the meantime, Surgery Room does the ultimate access control check-up and then multicasts positive confirmation as (ID, YES) or negative confirmation as (ID, NO) to every surgeon. Surgeons will *commit* their received transactions if (ID, YES) is received. A transaction will be *rolled back* or *aborted* in case of such two events: one is that (ID, NO) is received and the other is that within a prescribed time period, counting from T, (ID, YES) has not been received. Although this design keeps Surgery Room involved in every transaction commitment, it does help to prevent surgeons from unnecessarily committing transactions in case of network failures while waiting for the corresponding confirmations from Surgery Room.

Particularly, Surgeon A starts his operations to complete the functionality of step 1 after obtaining TOKEN (in the form as introduced in **S5**) from Surgery Room. Detailed working process is the same as described above. After finishing his operations, Surgeon A will signals an ENDING OPERATIONS command to others and passes TOKEN to the next participant, Surgeon B. Surgery Room and Surgeon B, C change identity of Surgeon A into an obsolete state, which means any transaction within the ongoing session from A will be ignored from then on. This is in accordance with **R4** in the sense that although Surgeon A knows TOKEN, he can no longer pretend to be a TOKEN holder again. Surgeon B and C follow the same way to finish their steps.

4. Surgeon Room starts another session if necessary.

The working process is same and we will not repeat it. But note that all surgeons' states will be reset and the symmetric key *K* and TOKEN will be re-chosen by Surgery Room.

4 Conclusion

Modern telemedicine is a tool physicians and health care organizations can use to increase productivity and access to care, improve the quality of care delivered, keep costs down and gain a competitive advantage [39]. Although various telemedicine systems have been constructed, security related issues are rarely considered. In this paper, we pay special attention to secure an image-based simulated system for kyphoplasty telesurgery. The main goal of the system is to share remote expertise, which is achieved by managing Surgery Room. Two unique requirements characterise the system: one is that each virtual surgeon in turn simulates a step of the surgery process in line with a real world case. The other is that each surgeon is confined his operations within certain particular part of a patient data image, so operations outside his range are presumed to be illegal accesses. To meet the first requirement, a TOKEN encrypted in a nested encapsulation is employed to synchronise operations among participating surgeons. In addition, if a surgeon signals his end of operations, his identity will be changed to an obsolete state in other sites. For the second requirement, patient data images are segmented and access control rules for them are set up accordingly. We manage to solve other security requirements too. For example, to keep data integrity of patient data images during delivery, we combine an image hashing function with a standard hash function to preserve strict data integrity of ROI while relax data integrity guarantee of the remaining parts. We base security of our solutions on the existing cryptography standards. Efficiency is the primary consideration in implementing the system. To alleviate traffic requirement of the system, we intend to send actions by a local surgeon instead of resulted images to simultaneously change other remote copies in various sites. This intention is consequently realised in the form of transaction as the associated concepts such as “rollback”, “commit” are well applicable to our system. Although we confine our discussion to a simulated kyphoplasty telesurgery system, methods used in this system can be generalised to other similar systems without difficulty.

References

[1] S. C. Orphanoudakis, E. Kaldoudi, M. Tsiknakis, *Technological Advances in Teleradiology*, Eur. J. Radiology, vol. 22, pp. 205-217, 1996.

[2] S. C. Orphanoudakis, E. Kaldoudi, M. Zikos, *Telemedicine*, in J. Urban, P. Dasgupta (eds.), *Encyclopedia of Distributed Computing*, Kluwer Academic Press, 1998 (in press)

[3] V. J. Ablaza, J. Fisher, *Teleemedicine and Wound Care Management*, http://www.rubic.com/articles/article2.html.

[4] S. T. Treves et al, *Multimedia communications in medical imaging*, IEEE J Selected Areas Commun, Vol. 10, pp. 1121-1132, 1992.

[5] J. Bernarding et al, *Distributed medical services within the ATM-based berlin regional testbed*, Pro. CAR'95, pp. 735-740.

[6] S. J. Schanz et al, *1997: A Busy Legislative Year For Telemedicine?*, Telemedicine Today, http://www.telemedtoday.com/.

[7] *Health Insurance Portability and Accountability Act (HIPAA)*, U.S., 1996.

[8] R. J. Anderson, *Security in Clinical Information Systems*, published by the British Medical Association, January 1996; also available from http://www.cl.cam.ac.uk/users/rja14/#Med.

[9] R. J. Anderson, *Patient Confidentiality - At Risk from NHS Wide Networking*, Pro. Healthcare, 1996.

[10] *Australian Standard 4400: Personal Privacy protection in health care information systems*, Standard Australia, 1995.

[11] *Keeping Information Confidential, Association of Community Health Councils for England and Wales*, May 1995.

[12] *Draft Guidance for the NHS on the Confidentiality, Use and Disclosure of Personal Health Information*, N Boyd, DoH, 10 August 1994.

[13] D. Carman, N. Britten, *Confidentiality of Medical Records: the patient's perspective*, British Journal of General Practice, Vol. 45, pp. 485-488, 1995.

[14] B. Bennett, *Medical Records Confidentiality Act of 1995*, U.S. Senate S.1360, 1995.

[15] R. J. Aderson, *A Security Police Model for Clinical Information Systems*, IEEE Symposium on Security and Privacy, pp. 30-45, 1996.

[16] R. Chandramouli, *A Framework for Multiple Authorization Types in a Healthcare Application System*, 17th Annual Computer Security Applications Conference (ACSAC), 2001.

[17] AHIMA, *AHIMA's Recommendations to Ensure Privacy and Quality of Personal Health Information on the Internet*, http://www.ahima.org/infocenter/guidelines/tenets.html#standards.

[18] M. A. Winker et al, Guidelines for Medical and Health Information Sites on the Internet, J. of the American Medical Association, Vol. 283 No. 12, 2002.

[19] C. Ilioudis, G. Pangalos, *A Framework for an Institutional High Level Security Policy for the Processing of Medical Data and their Transmission through the Internet*, J. of Medical Internet Research, Vol. 3, 2001.

[20] B. Blobel, *Hospital Information Systems in Today's Healthcare*, Business Briefing: Hospital Engineering & Facilities Management, pp. 80-83, 2001.

[21] M. M. Medenis, *Security in Teleradiology Systems: Requirements and Proposed Mechanisms*, http://www.ece.arizona.edu/~medenis/hw2/sem_pro.htm.

[22] International Committee of Medical Journal Editors. *Policies for posting biomedical journal information on the Internet*. http://www.icmje.org/index.html#internet.

[23] Cooperative Tele-Surgery, http://web.mit.edu/hmsl/www/markott/cooptelesurg.html.

[24] M. Zikos, E. Kaldoudi, S.C. Orphanoudakis, *Image Processing within an Integrated Teleradiology Services Network*, Pro. CAR'97, pp. 1027-1022, 1997.

[25] N. W. John, M. Riding, A. Sadarjoen, *Bringing 3D to Teleradiology*, Pro. International Conference on Information Visualisation (IV2000), 2000.

[26] I. B. Aris, A. A. E. Wagie, N. B. Mariun, A. B. E. Jammal, *An Internet-based blood pressure monitoring system for patient*, J. of Telemedicine and Telecare, Vol. 7, pp.50-53, 2001.

[27] H. Nagata, H. Mizaushima, *A Remote Collaboration System for Telemedicine Using the Internet*, J. of Telemedicine and Telecare, Vol. 4, pp. 89-94. 1998.

[28] Laboratories for Information Technology.

[29] E. S. Ebbini, *Multimodal image-guidance for noninvasive surgery: registration, segmentation, and statistical imaging models*, Pro. ISSPA '99, Vol. 1, 1999.

[30] L. Vosilla, G. D. Leo, M. Fato, A. Schenone, F. Beltrame, *An interactive tool for the segmentation of multimodal medical images*, Pro. of IEEE EMBS International Conference on Information Technology Applications in Biomedicine, pp. 203 –209, 2000 .

[31] M. Ferrant, *Physics-based Deformable Modeling of Volumes and Surfaces for Medical Image Registration, Segmentation and Visualization*, PhD thesis, Louvain, Belgium: Universite' Catholique de Louvain, 2001.

[32] A. S. Tanenbaum, *Computer Networks, 2nd ed.*, New Jersey: Prentice Hall Inc. 1989.

[33] R. Venkatesan, S. –M. Koon, M. Jakubowski and P. Moulin, *Robust Image Hashing*, Pro. IEEE ICIP, 2000.

[34] M. K. Mihçak and R. Venkatesan, *New Iterative Geometric Methods for Robust Perceptual Image Hashing*, Pro. ACM Workshop on Security and Privacy in Digital Rights Management, 2001.

[35] IEEE: 802.4, *Token-Passing Bus Access Method*, New York: IEEE, 1985b.

[36] IEEE: 802.5, *Token Ring Access Method*, New York: IEEE, 1985c.

[37] J. Mir, J. Borrell, *Protecting General Flexible Itinerraries of Mobile Agents*, ICICS 2001, LNCS 2288, pp. 382-396.

[38] D. Bell, J. Grimson, Disributed Database Systems, Addison-Wesley Publishing Company, 1992.

[39] Hoffman A, *Telemedicine: what's beyond the hype?* Health Care Business Digest, pp. 48-53, 1997.