1-2010

TeleOph: A secure real-time teleophthalmology system

Yongdong WU

Zhou Wei

Haixia Yao

Zhigang ZHAO

Lek Heng Ngoh

See next page for additional authors

DOI: https://doi.org/10.1109/TITB.2010.2058124

Published in IEEE Transactions on Information Technology in Biomedicine, 2010 September, Volume 14, Issue 5, Pages 1259-1266
https://doi.org/10.1109/TITB.2010.2058124

TeleOph: A Secure Real-Time Teleophthalmology System

Yongdong Wu, Zhou Wei, Haixia Yao, Zhigang Zhao, Lek Heng Ngoh, Robert H. Deng, and Shengsheng Yu

***Abstract*—Teleophthalmology (TeleOph) is an electronic counterpart of today's face-to-face, patient-to-specialist ophthalmology system. It enables one or more ophthalmologists to remotely examine a patient's condition via a confidential and authentic communication channel. Specifically, TeleOph allows a trained nonspecialist in a primary clinic to screen the patients with digital instruments (e.g., camera, ophthalmoscope). The acquired medical data are delivered to the hospital where an ophthalmologist will review the data collected and, if required, provide further consultation for the patient through a real-time secure channel established over a public Internet network. If necessary, the ophthalmologist is able to further sample the images/video of the patient's eyes remotely. In order to increase the productivity of the ophthalmologist in terms of number of patients reviewed, and to increase the efficiency of network resource, we manage the network bandwidth based on a Poisson model to estimate patient arrival at the clinics, and the rate of ophthalmologist consultation service for better overall system efficiency. The main objective of TeleOph is therefore to provide the remote patients with a cost-effective access to specialist's eye checkups at primary healthcare clinics, and at the same time, minimize unnecessary face-to-face consultation at the hospital specialist's center.**

***Index Terms*—Teleconferencing, telemedicine.**

I. Introduction

EYE is one of the most important organs of human body as it provides us most of information daily. Regretfully, "*According to WHO estimates, approximately 314 million people worldwide live with low vision and blindness. Of these, 45 million people are blind and 269 million have low vision*" [1]. Undoubtedly, blindness results in both physical and emotional trauma for every patient. This unfortunate situation is probably due to: 1) an acute shortage of ophthalmology specialists in many countries (e.g., fewer than one ophthalmologist for 100 000 population [2], or only about 12 000 ophthalmologists out of the 1.1 billion population in India [3]); and 2) the distribution of ophthalmologists is far from uniform such that there are much more eye disease patients in the rural or poor regions, e.g., in India, 79% eye patients reside in rural areas. As it takes time to train a lot of ophthalmologists, thus sharing of ophthalmology medical knowledge must be promoted to as far remote places as possible.

Typically, a hierarchical-based healthcare delivery system optimizes the use of medical resource. This usually comprises primary healthcare provision at outpatient clinics, and secondary and tertiary specialist cares in the hospitals. Typically, patients can walk in for a consultation at any clinic, and may be referred to more costly hospital care when it is deemed necessary to follow-up with secondary and tertiary specialist care. However, due to the shortage or unavailability of ophthalmologists in the primary clinics, nearly all patients with eye-related medical conditions are referred to the hospital. For example, eye center of Tan Tock Seng Hospital (TTSH, Singapore) has to treat over 1300 new cases per month, but about 30% of all referrals are later found to be unnecessary as if having their cases reviewed by a qualified ophthalmologist, they can be easily treated by general practitioners at the clinics. To solve this problem, more ophthalmologists were previously attached to clinics on a part-time basis to see the patients and at the same time provide further training to clinic medical officers. Unfortunately, this arrangement did not yield the desirable outcome, in terms of best use of specialists' time, due mainly to the difficulty in estimating the patient's load in a clinic each day.

As an emerging technology-based solution, telemedicine [4], [5] enables the doctor to consult the patient remotely so as to reduce the unnecessary referrals and travel cost. In conventional ophthalmology, most of the diagnostic ophthalmic instrumentations are adapted to mount still and/or video cameras to acquire images so that ophthalmologists make diagnostic inferences. With state-of-the-art telecommunication infrastructure, ophthalmology is readily amenable to a telemedicine system based on medical image exchange [6], [7], i.e. to say, a teleophthalmology (TeleOph) system will provide eye consultation by delivering high-quality eye images and videos over a public broadband network, so as to exploit the use of communication technologies to render ophthalmology services, share and optimize medical expertise locally, as well as globally.

A. Related Work

For ease of exposition, in the rest of this paper, `Alice` represents the eye patient, `Bob` as the ophthalmologist, and `Clark` as the trained clinic physician who helps the patient in the clinic.

Manuscript received March 11, 2008; revised April 26, 2010; accepted July 2, 2010. Date of publication July 26, 2010; date of current version September 3, 2010. This work was supported by the Enterprise Challenge, Singapore.

Y. Wu, H. Yao, Z. Zhao, and L. H. Ngoh are with the Institute for Infocomm Research, Singapore 138632 (e-mail: wydong@i2r.a-star.edu.sg; hxyao@i2r.a-star.edu.sg; zzhao@i2r.a-star.edu.sg; lhn@i2r.a-star.edu.sg).

Z. Wei and S. Yu are with the Computer Science School, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: phdzwei@gmail.com; ssyu@mail.hust.edu.cn).

R. H. Deng is with the School of Information Systems, Singapore Management University, Singapore 178902 (e-mail: robertdeng@smu.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITB.2010.2058124

Up to now, there have been a number of similar telemedicine systems [8]. However, many of these systems employ a store-and-forward offline scheme.

In a store-and-forward TeleOph system, `Clark` captures the medical images of a patient in a clinic, uploads them into a hospital database or sends them to an ophthalmologist `Bob` directly. `Bob's` job is to analyze these medical images, make diagnostic inferences, and send the diagnosis result to the clinics. In many of the existing store-and-forward solutions, schemes [9]–[11] just deliver the medical data by email, while schemes [12]–[14] enable offline upload/download images based on web technology. Although the above store-and-forward method is advantageous from the aspects of cost, complexity, and convenience, it is unsatisfactory in terms of consultation effectiveness, patient satisfaction, and diagnosis accuracy [15]. Furthermore, as some schemes (e.g., [9]–[11]) deliver data in clear text, the patients' records may be intercepted and tampered by malicious attackers in the transmission channel. Nowadays, it is increasingly important for patient privacy be protected in the telemedicine systems by being compliant with Health Insurance Portability and Accountability Act (HIPAA) [16].

B. Our Contribution

TeleOph aims to achieve the practice of medicine without the usual physician–patient face-to-face meetings, enable good ophthalmology-related medical services in a cost-effective way, and technically overcome the shortcomings of existing TeleOph systems. In all, it has the following merits.

1) *Optimization of specialists' time:* TeleOph helps to optimize the specialists' time by eliminating travel time (local or overseas travels), attachments to clinics, as well as allow the consultation to be carried out at "anytime" that best suits the specialists, thus resulting maximum flexibility. TeleOph further ensures that patients are referred to the eye center for further treatment only after they have been screened by the specialists using TeleOph. Hereby, TeleOph eliminates unnecessary referrals so that TeleOph maximizes senior specialists' time at the hospitals, and enables both delayed/offline (i.e., at a convenient time of the specialist) case-by-case examination of prerecorded patient's data, as well as instantaneous remote real-time follow-on examination with selected patients if necessary.
2) *Cost reduction:* By connecting ophthalmologists and patients securely and remotely, TeleOph overcomes the geographical barrier and puts patients and specialists in a virtual clinic. As a result, it reduces patient's medical cost. Extra patient's cost is incurred whenever a patient has been referred to see a specialist for further examinations. The amount incurred can range from few dollars (local transportation fees) to hundreds of dollars (airline tickets for overseas consultation) [17].

The rest of the paper is organized as follows. Section II describes the TeleOph design. Section III introduces our implementation of TeleOph. Section IV discusses network parameter and evaluation. Section V draws our conclusions.

II. Design of TeleOph System

The proposed system is a novel telemedicine application, which meets the special requirements of tele-ophthalmologic field using secure videoconferencing via public Internet networks. It alleviates the network bandwidth bottleneck by modeling the network bandwidth usage, and addresses the issue of maintaining the privacy and confidentiality of patient's medical data during and after the TeleOph session.

A. TeleOph Diagram

The infrastructure of the present TeleOph system includes two kinds of sites. Without loss of generality, one site is called clinic and another is called hospital. The patient's medical data will be captured by instruments (e.g., camera and ophthalmoscope) in the clinic. At the other end, the ophthalmologist will receive the patient's medical data and provide consultation advice in the hospital.

B. TeleOph Module

As TeleOph enables real-time examination and diagnosis, any patient at clinic can expect to receive diagnosis and follow-up treatment in a timely manner. To this end, the clinic will set up a secure communication channel with the target hospital such that all the subsequent network traffics are authenticated and confidential. In either clinic or hospital, TeleOph includes five major modules described as follows.

1) *Registration:* Records the biodata of the patient and creates a directory according to the patient ID at both the clinic and hospital.
2) *Examination and analysis:* Captures the medical data such as real-time images for pupil reaction, and retina examination, etc.
3) *Data upload:* Transmits the patient data to the remote hospital system so that the ophthalmologist can make a first-cut diagnosis since all the medical data and bio-data of the patient are obtained in clinic for remote consultation.
4) *Consultation:* Facilitates consultation and discussion of patients' conditions between the ophthalmologist and the patient with text, picture, graphics, and video/audio. If necessary, the ophthalmologist will sample the patient's eye remotely and directly through TeleOph.
5) *Medical records:* Enable to record the medical data (e.g., retina images, visual fields, etc.), diagnosis notes and results. To be compliant with HIPAA, the records will be encrypted and signed by the ophthalmologist. Data should be retrievable by both sides, with proper security and authorized access to safeguard patients' confidentiality and privacy.

C. TeleOph Queue

By extending the general client/server model that handles requests with one-level first-in-first-out (FIFO) queue, TeleOph responses to patient's request based on a two-level queue model because one hospital will provide service to many clinics. As shown in Fig. 1, TeleOph creates two queues: one is patient-

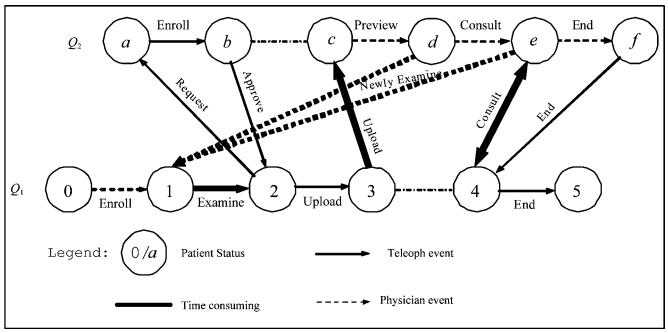

Fig. 1. Patient state-transition map in clinic and hospital.

arrival queue Q_1, which is managed in clinic, and another is data-arrival queue Q_2, which is managed in hospital. Both queues represent the latest state of the patient after a processing event.

In the TeleOph system, each patient may have up to 12 states. Half of these states are in clinic queue Q_1 and another half are in hospital queue Q_2. The state transition is activated by either the physician or TeleOph. Fig. 1 describes the patient state transition corresponding to the events.

Let Q_i^x represent that the patient is at state x of queue Q_i. Initially, the patient state is Q_1^0. When patient `Alice` is enrolled, her state is changed into Q_1^1. After she is examined, her state evolved as Q_1^2. In this case, TeleOph/clinic will send a registration request to the selected hospital, such that she enters into entrance state Q_2^a. As long as TeleOph/clinic fills in the registration information, her state is Q_2^b. When the hospital has enough bandwidth and `Alice` is the first one whose data are not uploaded, TeleOph/hospital will issue a control instruction to approve data uploading, such that `Alice`'s state is changed to Q_1^3.

Usually, it may take some time to transit from state Q_1^3 to Q_2^c since the medical data are so big that it takes some long transmission time. Q_2^c indicates that all the information of `Alice` are uploaded and are ready for preview by doctor `Bob`. If `Bob` does not satisfy the examination data after previewing the patient data in state Q_2^d, the next state may be back to Q_1^1 so as to obtain new examination data, otherwise, the states in two queues are Q_2^e and Q_1^4 for consulting via videoconferencing and whiteboard. Possibly, the doctor may ask for real-time examination of the patient such that the patient status is back to Q_1^1 tentatively. Once the real-time examination is complete, the patient state will be back to consultation state.

The last event is activated by the doctor so as to terminate the consultation. It will clear the patient entry in two queues, and prepare the record for future purpose. Optionally, the doctor may review the records at any time, i.e., the patient state is Q_2^d if her record is available.

III. Implementation of TeleOph System

It is widely agreed that user acceptance is very important for any telemedicine system. Hence, TeleOph should provide video of high quality in the videoconferencing process; otherwise, the patient may dislike the remote consultation, and instead prefer face-to-face consultation. This means a larger network bandwidth would be required. On the other hand, TeleOph should schedule the tasks or state queues properly so as to increase the productivity of the ophthalmologist.

A. Configuration

In our implementation, both hospital and clinic are equipped with Pentium Duo 2.4-GHz, 2-GB RAM, the sampling device includes with one firewire IEEE-1394 card for capturing medical videos (high-definition TV (HDTV) quality), two USB interfaces for capturing medical image, and a videoconferencing unit. To be cost-effective, we select the higher resolution 704-line camera for the ophthalmologist video (standard-definition TV (SDTV) quality) since the patient desires to view the video of the ophthalmologist in high quality, but only 352-line camera for the video of the patient (TV quality) since the ophthalmologist may not require the same video quality on his patient.

In order to improve the productivity of ophthalmologist, two channels are used for medical data and video, respectively. The medical data are transmitted over transmission control protocol (TCP) network at bit-rate 587 kb/s (see Section IV-A), while the video data are MPEG4 bitstream at bit-rate 800 kb/s–1.2 Mb/s. The total network bandwidth required is, therefore, 2 Mb/s that is used for both medical data, control instruction, videoconferencing, etc.

B. Clinic System

The clinic system is responsible for patient registration, medical examination, and patient consultation. It is equipped with three monitors. The first monitor enables a clinic physician to register the patient biodata and capture the medical data in real time. The second monitor shows the patients medical image and video that are synchronized with those at the hospital site, and the third monitor displays the real-time video of the ophthalmologist in the form of videoconferencing.

1) Registration: When a patient `Alice` approaches the clinic physician, her particulars will be recorded for correctly processing. Note that the hospital also has the registration interface so that the outpatient can be consulted.

2) Examination: After registering patient `Alice`, clinic physician `Clark` will perform basic examination such as weight, temperature, blood pressure, and then capture the medical images with medical devices such as slit-lamp photo system which a camera is installed on. Generally, each patient will be examined with the still image cameras and video cameras. For the sake of interoperability, DICOM conversion tool is also provided because the medical image standard format DICOM is not supported by most cameras.

TeleOph video-capturing process has three modes: previewing, recording, and replaying. The previewing mode displays the eye image sequence in real time for the purpose of adjusting position, focus etc.; the recording mode enables the physician to record the image sequence if the video quality is satisfactory, while the replaying mode helps the physician to check and confirm the video quality. If necessary, the physician will resample the medical video and overwrite the previous recordings.

3) Uploading: With the on-site photo system and cameras, TeleOph can be used to obtain several kinds of medical images on the spot. However, the sampled images may be insufficient for correct consultation. To support interdisciplinary cooperations, besides capturing the medical data, TeleOph enables the retrieval of medical data from other departments via shared directories or removable tokens.

After capturing the images/videos, the physician `Clark` summarizes medical data including both locally sampled images/videos and remotely retrieved ones. If the physician is interested in a specific image, he/she may double check the image file name, and get the preview of the selected picture so as to make sure that all the medical images are of sufficient quality.

If `Clark` decides to register patient `Alice` in a hospital with her particular, TeleOph will fill in an entry of the queue Q_1 based on FIFO queue principle. The entry must have the following elements:

$$\{\text{PatientID } \mathrm{P_{id}}, \text{Clinic } \mathrm{C_{id}}, \text{ Hospital } \mathrm{H_{id}}, \text{ Session } \mathrm{S_{id}}\}$$

where $\mathrm{S_{id}}$ represents the secure channel between Clinic $\mathrm{C_{id}}$ and Hospital $\mathrm{H_{id}}$, and is used for all the following traffic till the session key is refreshed (Section IV-B will introduce the processes of building and refreshing secure channel). If there is no secure channel $\mathrm{S_{id}}$ between Clinic $\mathrm{C_{id}}$ and selected Hospital $\mathrm{H_{id}}$, both sides will negotiate the secure channel with secure socket layer (SSL, http://www.openssl.org/) protocol.

After receiving the uploading request from Clinic $\mathrm{C_{id}}$, the TeleOph/hospital will fill in a new entry in the queue Q_2. If the network is busy, TeleOph/hospital will postpone receiving the medical data, instead, it sends a reply to TeleOph/clinic for acknowledgement. As long as the Hospital $\mathrm{H_{id}}$ has enough bandwidth, TeleOph/hospital will select the first entry in Q_2 as to which medical data has not been uploaded, and ask the TeleOph/clinic of the entry to transmit medical data.

4) Consultation: When a patient is selected for consulting, the clinic monitor will show a banner to announce the patient name and identity $\mathrm{P_{id}}$ such that the patient can be brought in to sit before the clinic monitors. The real-time images of the ophthalmologist will be shown on the screen so as to visualize the face-to-face consulting. In order to protect the privacy and confidentiality, the video channel is encrypted with a session key generated from the SSL session channel $\mathrm{S_{id}}$.

TeleOph provides secure videoconferencing and secure synchronized whiteboard for both patient and doctor. When the ophthalmologist performs any operation $\mathcal{O}$ such as loading a medical image, zooming in/out images, and drawing on his monitor, the same view will be shown in the clinic monitor simultaneously. Technically, for each operation $\mathcal{O}$, TeleOph represents it with a flag $\mathcal{O}_f$ and its parameters $\mathcal{O}_p$ (e.g., the coordinates of the mouse movement), and passes the pair $(\mathcal{O}_f, \mathcal{O}_p)$ to the clinic end. Since the clinic has the same medical data as the hospital, both sides are enabled to have the same view at the same time (albeit with small network delay) since no medical data need delivery in consultation state Q_2^e.

In order to have a gross measure of illness severity, we represent the length of the defective region in pixels where the ophthalmologist marks. If the ophthalmologist gets two measures such as the sizes of defective region and whole eye, he can draw a conclusion on the percentage of defective area. Furthermore, if the ophthalmologist can get the calibration parameter (focus, object distance, etc.) of the camera, he could therefore tell the patient the exact length of damaged area in centimeters.

C. Hospital System

The hospital system is a platform that enables the ophthalmologist to manage patient queue, analyze patient information, and to communicate with patient.

1) Managing Patient Queue: As a multiclinic multihospital (i.e., many-to-many) system, TeleOph aims to enable a hospital to handle simultaneous consultation requests from different patients of different clinics. To this end, TeleOph/hospital will create and maintain a queue Q_2 based on FIFO principle, i.e., for every clinic's registration request, TeleOph/hospital will create an entry in Q_2 as

$$\{\text{PatientID } \mathrm{P_{id}}, \text{ Clinic } \mathrm{C_{id}}, \text{ Hospital } \mathrm{H_{id}}, \text{ SessionID } \mathrm{S_{id}}\}$$

and send an acknowledgement indicating the waiting queue length to the Clinic $\mathrm{C_{id}}$ such that the state is changed from Q_2^a to Q_2^b.

When at least one entry is at state Q_2^b and the hospital network has enough bandwidth, TeleOph/hospital will select the first entry of them, and send a control message such that the TeleOph/clinic can upload the patient data. The general data-transmission protocol enables a multiple of clinics send media data simultaneously, it may improve the network efficiency as a whole. Nonetheless, since each clinic has only a fraction of bandwidth available to TeleOph, it is of high probability that none of patient medical data are uploaded completely for a long time. As a consequence, the doctor has to wait till at least one patient is at state Q_2^c. To reduce the waiting time of the doctor, our transmission protocol is that a clinic-hospital pair will monopolize the data channel till all the medical data of the patient is transmitted completely as long as it starts to send medical data. This monopoly strategy enables that the doctor has at least one patient for consulting as soon as possible.

2) Analyzing Patient Data: If there is at least one entry at state Q_2^c, `Bob` will select one patient. The TeleOph preview interface enables that `Bob` analyzes the images in any order and combination, and zooms in/out the images for more details. When `Bob` likes to consult with the patient, he will send an instruction (e.g., showing a banner or calling the patient) to the TeleOph/clinic such that the patient sits before the clinic consulting monitors.

3) Consultation: During the period of consultation, `Bob` and the patient `Alice` can communicate via videoconferencing and whiteboard. For example, if `Bob` concludes that an eye of `Alice` is defective, he will load the image into the whiteboard, this image will be shown in the clinic screen. When `Bob` likes to tell the defected area to `Alice`, he can highlight the region of the image, as shown in Fig. 2. All the results of `Bob`'s operations are simultaneously shown on the clinic monitor. At any time, `Bob` can input his note for future reference.

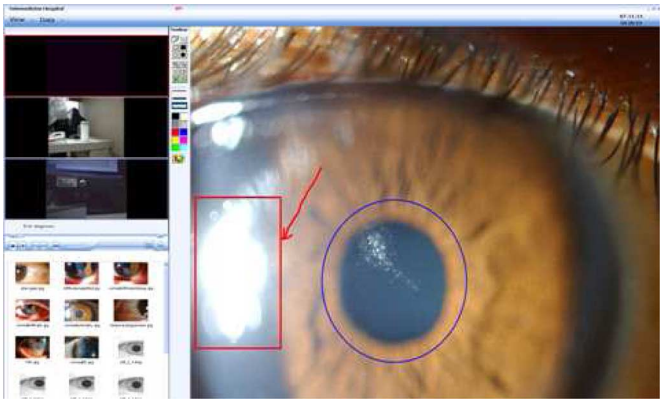

Fig. 2. Consultation page. The ophthalmologist can highlight the impaired area of the patient's eye, and introduces her about the normal eye.

In most cases, the medical data are sampled by the clinic physician `Clark` since he has the direct contact with the patient. However, the images acquired by `Clark` are based on the general knowledge or routines. Sometimes, `Bob` likes to obtain more medical data for a specific patient. To do this, he will start the real-time sampling process. That is to say, he will personally take the patient's images/video with the method in Section III-B2. Specifically, with the help of clinic physician `Clark`, `Bob` asks `Alice` to sit before the cameras and instructs her to look at somewhere, and then shoots the images/videos. In this case, `Bob` is able to sample the patient data remotely.

When the ophthalmologist `Bob` finishes the consultation, he will issue the case-complete instruction. As a result, TelepOph will terminate the videoconferencing, and release the resource allocated to manage the patient, and change the patient state as END (Q_2^f, Q_1^5).

4) Archival: In order to understand the patient's case further or educate the students, the ophthalmologist needs to replay the patient record, and display consultation information sometime. Hence, we should enable to securely save the video, and marked images.

D. Collaborative Consultation

For complex disease cases, one ophthalmologist may need to discuss with other ophthalmologists, or even with specialists in other departments. To meet this collaborative-consultation requirement, whenever a hospital sends a collaboration request, the requested partner will regard the request as urgent one, i.e., by putting the request into the foremost position of the waiting queue Q_2, postpone uploading any medical data from any clinic, and read the data from the requesting hospital. As soon as the current consultation in the requested hospital is completed, the specialists of two hospitals will return to analyze their individual patient cases.

IV. Discussion

TeleOph targets to provide a virtual platform for eye consultation. Hence, it should select suitable network bandwidth for balancing the cost and QoS, and tolerate the network bandwidth fluctuation. Besides, security is also an important requirement for TeleOph.

A. Selecting Network Bandwidth

Notations:

- X_i a random variable representing patient-arrival time, thus the arrival interval $\Delta_x^i = X_i - X_{i-1}$;
- Y_i a random variable for the time when patient status is changed to Q_2^c, state of data uploaded;
- Z_i a random variable representing the end time for consulting patient P_i, i.e., the time of entering END state Q_2^f;
- V a random variable representing the medical data size of a patient, which is regarded as a uniform distribution over interval $[V_{\min}, V_{\max}]$;
- b the subscribed network bandwidth;
- t_{i2} end time of offline examining P_i, i.e., the time of entering state Q_1^2;
- t_{ic} end time of transmitting medical data of P_i, i.e., the time of entering state Q_2^c;
- t_{ie} consultation start time for P_i.

1) Bandwidth Selection: Usually, a patient consultation system can be regarded as a Poisson process. That is to say, the patient-arrival interval Δ_x is a Poisson distribution $g_1(t) = \lambda_1 e^{-\lambda_1 t}$ at an arrival rate λ_1, and the actual consultation time Δ_z is also a Poisson distribution $g_2(t) = \lambda_2 e^{-\lambda_2 t}$ at a service rate λ_2. Here, if we assume that the arrival rate is close to the service rate, $\lambda_1 \approx \lambda_2$ such that the productivity of doctor is high. On the other hand, to provide correct diagnosis, `Bob` will not start to consult the patient unless her medical data are complete. Meanwhile, in order to increase the consultation productivity, when an ophthalmologist finishes consulting one patient, the medical data for the next patient should be ready if at least one patient has been examined. Mathematically, we should select bandwidth b such that the probability

$$P(|Q_2^c| = 0 : |Q_1^2| \neq 0) < \epsilon \tag{1}$$

where $|Q_i^x|$ is the length of the queue Q_i in state x, and ϵ is a small number. Equivalently, for ith patient, let us rewrite (1) as

$$P(X_{i+1} \leq Z_i \leq Y_{i+1}) < \epsilon. \tag{2}$$

Nonetheless, it is not easy to determine b from (2) although Y_{i+1} is a function of b. Hence, we present an approximation solution to solve b. Considering that the distribution in queue Q_2 is mainly determined by Q_1, examining time T_i, and network bandwidth, we have

$$Y_{i+1} = \begin{cases} X_{i+1} + T_{i+1} + V_{i+1}/b, & Y_i < X_{i+1} + T_{i+1} \\ Y_i + V_{i+1}/b, & Y_i \geq X_{i+1} + T_{i+1}. \end{cases}$$

For simplicity, we omit T_i in the following. Thus,

$$Y_{i+1} = \max(X_{i+1}, Y_i) + V_{i+1}/b$$
$$Y_{i+1} - Y_i = \max(X_{i+1} - Y_i, 0) + V_{i+1}/b.$$

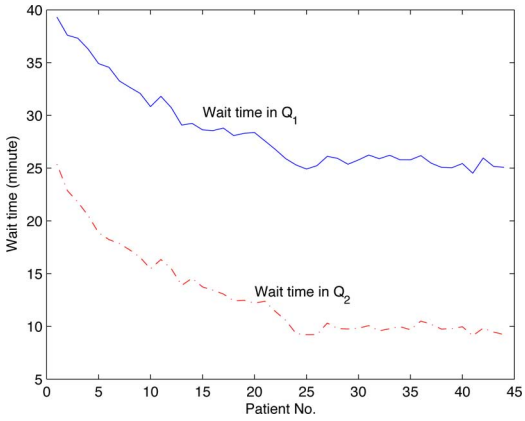

Fig. 3. Patient wait time T_{i1} in queue Q_1 and T_{i2} in queue Q_2.

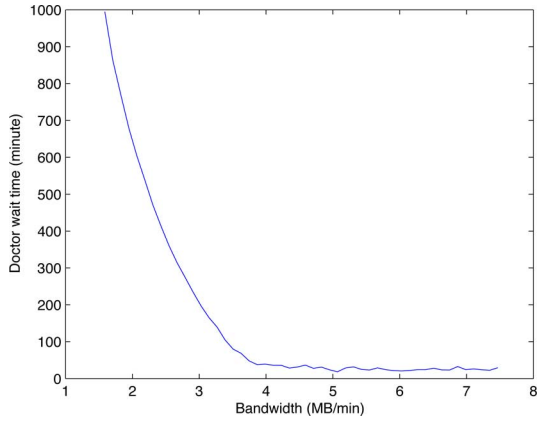

Fig. 4. Daily wait time of doctor versus network bandwidth.

Assuming that TeleOph is highly efficient, i.e., the average value of $\max(X_{i+1} - Y_i, 0)$ is small and $\Delta_{z_{i+1}} \cong Z_{i+1} - Z_i$. Additionally, if the service interval $Z_{i+1} - Z_i \geq Y_{i+1} - Y_i$ is at a high probability, $i = 1, 2, \ldots$, the doctor waiting time will be small such that the doctor productivity is high. Hence,

$$P(Z_{i+1} - Z_i \geq Y_{i+1} - Y_i) \approx P(\Delta_z \geq V/b) \geq 1 - \varepsilon$$

for a small ε. To calculate the required bandwidth, we add a tolerance value for a confidence interval

$$1/\lambda_2 \geq \mu + k\sigma$$
$$\mu = \frac{V_{\max} + V_{\min}}{2b}, \quad \sigma = \frac{V_{\max} - V_{\min}}{\sqrt{12}b} \tag{3}$$

where μ is the average time for transmitting a patient data, and σ is the standard variance of transmission time variable, i.e., μ and σ^2 are the mean and variance of uniform distribution V/b, respectively, and k is the tolerance factor and related to ε. Intuitively, (3) means that an ophthalmologist will wait for patient at a low probability if the consultation time is longer than transmission mean time. To be cost effective, we can derive the smallest bandwidth b from (3) as

$$b = \frac{(\sqrt{3} + k)V_{\max} + (\sqrt{3} - k)V_{\min}}{\sqrt{12}}\lambda_2. \tag{4}$$

2) Experimental Bandwidth Selection: According to the experience of hospital TTSH, consultation rate is about $\lambda_2 = 0.06$ per min, and patient-arrival rate is about λ_1=0.067 per min, or 44 patients on average per day, and average size of the medical data are about 60 MB (excluding HD video). Assume $k = 1.0$, $V_{\min} = 50$ MB, and $V_{\max} = 70$ MB, we have $b = 4.4$ MB/min or 587 kb/s according to (4). The patient waiting time is denoted as $T_{i1} = t_{ie} - t_{i2}$ and $T_{i2} = t_{ie} - t_{ic}$ in queues Q_1 and Q_2, respectively. In order to increase the productivity, an ophthalmologist usually comes to hospital later than the first patient. In the following experiments, let us assume that their arrival-time difference is 60 min.

Experiment 1 (Wait time): Based on the Poisson assumption with the patient-arrival rate λ_1 and consultation rate λ_2, Fig. 3 shows that patient waiting time is 28 min on average, and the average waiting time of doctor is 30 min daily (12 h). In comparison, with the same Poisson model, if there are outpatients for face-to-face conventional consultation in hospital, the waiting time of patient is roughly 28 min, while the waiting time of ophthalmologist is 13 min daily. Hence, with the selected bandwidth, TeleOph only increases the waiting time of doctorby 24 s per patient. Hence, the simulation demonstrates that the waiting time of TeleOph is almost the same as the face-to-face consultation system.

Experiment 2 (Bandwidth variance): This studies the waiting time of the doctor that varies with the network bandwidth, especially in the case of low bandwidth. The simulation result is shown in Fig. 4. According to Fig. 4, the doctor has to wait for long time if bandwidth is smaller than 3.8 MB/min, but the waiting time cannot be reduced significantly if bandwidth is greater than 5 MB/min. Hence, it is reasonable to select $b = 4.4$ MB/min, which is the theoretical result in (4).

B. Handling Secure Channel

1) Setting-Up SSL Channel: In this system, both hospital and clinic have X.509 certificates that are issued by an authority, e.g., the Ministry of Health. When a clinic likes to connect to a hospital, both sites will create a secure channel with SSL protocol assuming that the hospital is the TeleOph server. The major steps in setting-up SSL channel include the following: 1) TeleOph/clinic selects a random number s_1, encrypts s_1 with the hospital's public key, and sends the encryption to TeleOph/hospital; 2) the TeleOph/hospital sends a random s_2 to TeleOph/clinic; 3) both sides calculate the session key as

$$K = \mathcal{H}(s_1, s_2, \mathrm{H_{id}}, \mathrm{C_{id}}, \mathrm{para}) \tag{5}$$

where para represents other parameters, and $\mathcal{H}(\cdot)$ is a one-way function such as SHA-1 [18]. This SSL channel is used to transmit the medical data and the control commands between clinic and hospital. Therefore, each pair (clinic, hospital) has an independent SSL channel. In order to protect the confidentiality of videoconferencing, we generate another video key from the SSL session key for encrypting the video stream.

TABLE I
SURVEY RESULT

Q.1	Did you feel that the TeleOph process was comparable to face-to-face consultation?	91%(YES), 1%(NO)
Q.2	Was the trial effective in achieving your purpose to see an eye specialist?	100% (YES), 0% (NO)
Q.3	What would be your preferred choice if you have an eye problem in the future?	18% (Face-to-face) 82% (TeleOph)
Q.4	Would you recommend TeleOph to your friends and relatives?	91% (YES), 9%(NO)
Q.5	How satisfied are you with the TeleOph?	0% (Unsatisfy), 3% (Neutral), 97% (Satisfy)

2) Refreshing SSL Key: Although TeleOph employs SSL protocol to select the *de facto* standard 128-bit RC4 as a cipher, it is widely believed that a key can be used only for a short time or small number of encryptions to achieve a long-term security. For example, OpenSSL implementation refreshes the session key in minutes. Therefore, it is preferable to refresh the session key for every new patient. Technically, each side selects a new random number that is encrypted with the old channel key, and the encryption of the new random is transmitted to the peer. After receiving the peer's random number, each site updates the session key with (5).

Since there are one TCP channel and one user datagram protocol (UDP) channel, we should take care of the refreshing time. For example, if one site decrypts the content with the new session key immediately after key refreshing, the content may be useless due to desynchronization caused by the transmission delay. Hence, TeleOph updates TCP channel key when it starts to transmit a new file as both sides know the end time of the previous transmission, and updates UDP channel key when a new consultation session is initialized since video signal is useful only when the consultation is in progress.

C. Evaluating TeleOph

We performed a trial with 100 patients between one clinic and TTSH. One objective of the trial is to evaluate the accuracy of diagnosis through TeleOph. In the trial, one ophthalmologist consulted the patient in the clinic with the conventional face-to-face mode and another ophthalmologist consulted the same patient with TeleOph independently. Based on their diagnosis reports, we observed that both ophthalmologists had arrived at the same conclusion on every eye disease case.

The second objective of the trial is to evaluate the user acceptance of TeleOph. As it is not easy to have an objective measurement on the video/images quality, TTSH management staff performed a survey on the patients who were consulted with TeleOph. Table I shows the major items in the survey. The survey report shows that 91% of the respondents felt that TeleOph process was comparable to face-to-face consultation, 91% of them expressed that they would recommend this current system to their relatives and friends, and over 90% of them were satisfied with the TeleOph System. On the whole, both the patients and the doctors were satisfied with the quality of images and videos.

V. CONCLUSION

TeleOph enables the capturing of the patient medical data and send the medical data to a remote site for specialists review, and also allows instant remote capturing of image/video in real time by the specialist. Hence, it offers great potential of cutting down the overall treatment costs, as it is able to maximize the specialist productivity by having a specialist handling many cases without having to commute to be physically with the patients. Our real trial illustrates that the telemedicine via TeleOph is promising.

ACKNOWLEDGMENT

The authors appreciate TTSH staff E. Poh, W. Lau, M. Tan, and T. Lim who offered the medical data, and conducted the trial and survey.

REFERENCES

[1] (2010, Apr. 16). Blindness and visual impairment: Global facts [Online]. Available: http://www.vision2020.org/main.cfm?type=FACTS

[2] Z. Chen, X. Yu, and D. Feng, "A telemedicine system over the internet," in *Proc. ACM Int. Conf. Proc. Series Sel. Papers Pan-Sydney Workshop Vis. Inf. Process.*, 2001, pp. 113–114.

[3] V. Thulasi Bai, V. Murali, R. Kim, and S. K. Srivatsa, "Teleophthalmology-based rural eye care in India," *Telemed. e-Health*, vol. 13, no. 3, pp. 313–322, 2007.

[4] A.-M. Croteau and D. Vieru, "Telemedicine adoption by different groups of physicians," presented at the 35th Hawaii Int. Conf. Syst. Sci., Big Island, HI, 2002.

[5] B. Tulu, T. Abhichandani, S. Chatterjee, and H. Li, "Secure videoconferencing for telemedicine," in *Proc. 5th Int. Workshop Enterprise Netw. Comput. Healthcare Ind.*, 2003, pp. 61–65.

[6] C. W. Flowers, Jr, R. S. Baker, S. Khanna, B. Ali, G. A. March, C. Scott, and S. Murrillo, "Tele-ophthalmology: Rationale, current issues, future directions," *J. Telemed.*, vol. 3, no. 1, pp. 43–52, 1997.

[7] R. A. Tang, M. Morales, G. Ricur, and J. S. Schiffman, "Telemedicine for eye care," *J. Telemed. Telecare*, vol. 11, no. 8, pp. 391–396, 2005.

[8] H. Lamminen, V. Voipio, K. Ruohonen, and H. Uusitalo, "Telemedicine in ophthalmology," *Acta Ophthalmologica Scandinavica*, 81(2):105–109, May 2003.

[9] L. S. Chen, C. Y. Tsai, T. Y. Liu, T. H. Tung, Y. H Chiu, C. C. Chan, D. M. Liou, and T. H Chen, "Feasibility of tele-ophthalmology for screening for eye disease in remote communities," *J. Telemed. Telecare.*, vol. 10, no. 6, pp. 337–341, 2004.

[10] J. Cuadros and I. Sim, "EyePACS: An open source clinical communication system for eye care," *Studies in health technology and informatics*, 11:207–211, 2004.

[11] EHTO enterprise, "OPHTEL: Telematics in Ophthalmology," Jun. 3, 1997. http://www.ehto.org/ht_projects/initial_project_description/ophtel.html.

[12] C. Kennedy, R. Bowmanw, N. Farizaz, E. Ackuakuy, C. Ntim-Amponsah, and I. Murdoch, "Audit of web-based telemedicine in ophthalmology," *J. Telemed. Telecare*, vol. 12, no. 2, pp. 88–91, 2006.

[13] S. J. Chew, H. M. Cheng, D. S. C. Lam, A. C. K. Cheng, A. T. S. Leung, J. K. H. Chua, C. P. Yu, V. Balakrishnan, and W. K. Chan, "Ophth web-cost-effective telemedicine for ophthalmology," *Hong Kong Med. J.*, vol. 4, no. 3, pp. 300–304, 1998.

[14] J. C. Wei, D. J. Valentino, D. S. Bell, and R. S. Baker, "A web-based telemedicine system for diabetic retinopathy screening using digital fundus photography," *Telemed. e-Health*, vol. 12, no. 1, pp. 50–57, 2006.

[15] B. Harnett, "Telemedicine systems and telecommunications," *J. Telemed. Telecare*, vol. 12, no. 1, pp. 4–15, 2006.

[16] B. Tulu and S. Chatterjee, "A new security framework for HIPAA-compliant health information systems," in *Proc. Amer. Conf. Inf. Syst.*, 2003, pp. 929–938.

[17] S. Kumar, M. Tay-Kearneyw, F. Chavesz, I. J Constablew, and K. Yogesan, "Remote ophthalmology services: Cost comparison of telemedicine and alternative service delivery options," *J. Telemed. Telecare*, vol. 12, no. 1, pp. 19–22, 2006.

[18] "Secure Hash Standard (SHS)," National Institute of Standards and Technology, FIPS Publication 180-1, 1995.

Yongdong Wu received the B.A. and M.S. degrees from Beihang University, Beijing, China, in 1991 and 1994 respectively, and the Ph.D. degree from the Institute of Automation, Chinese Academy of Sciences, Beijing, in 1997.

He is currently a Senior Scientist with the Cryptography and Security Department, Institute of Infocomm Research ($\mathbf{I^2R}$), A*STAR, Singapore. His interests include multimedia security, e-Business, digital right management, and network security. He has authored or coauthored more than ten journal papers, more than 70 conference papers, and seven patents. His research results and proposals was incorporated in the ISO/IEC JPEG 2000 Security Standard 15444-8 in 2007.

Dr. Wu won the Tan Kah Kee Young Inventor Award in 2004 and 2005.

Zhou Wei received the B.A. degree from Jilin University, Jilin, China, in 2002 and the M.S. degree in 2007 from Huazhong University of Science and Technology, Wuhan, China, where he is currently working toward the Ph.D. degree.

He is currently with the Institute for Infocomm Research, Singapore. His research interests include image processing and video processing.

Haixia Yao received the Master's degree from the School of Information Technology, George Mason University, VA, in January 2001.

Since 2007, she has been a Research Officer at the Institute for Infocomm Research, Singapore. Her current research interests include tele-ophthalmology system, document protection system, and email-sending protection.

Zhigang Zhao received the B.A. degree from the University of Science and Technology Beijing, Beijing, China, in 1992 and the M.S. degree from the Institute of Software, Chinese Academy of Sciences, Beijing, China, in 1995.

He is currently a Research and Development Senior Engineer with the Cryptography and Security Department, Institute of Infocomm Research (I^2R), Agency for Science Technology and Research (A*STAR), Singapore. His research interests include digital right management, software protection, network security, and multimedia security.

Lek Heng Ngoh received the B.Sc.(Hons.) degree from the University of Kent, Canterbury, U.K., in 1986, and the M.Sc. and Ph.D. degrees from the Victoria University of Manchester, Manchester, U.K., in 1987 and 1989, respectively.

He was the Deputy Director and a member of the Executive Committee of Singapore's next generation Internet project, where his team was involved in the pioneering trials of broadband applications, including tele-education between universities in Singapore and their counter-parts in Asia-pacific, Canada, USA, and Europe, which led to the development and implementation of distance-learning broadband systems between Singapore and USA offering joint postgraduate degree programs. He was involved in a number of early telemedicine trials between hospitals in Singapore and those in Japan, Korea, and Taiwan. He is currently a Senior Research Scientist with the Agency for Science Technology and Research (A*STAR), Institute for Infocomm Research (I^2R), and an Adjunct Associate Professor at the School of Computer Engineering, Nanyang Technological University, Singapore, where he is involved in the research in enhanced services architecture for mobile e-health services and telecommunication networks. He is also involved in the managerial and leadership roles in several national and international advanced broadband network infrastructure initiatives involving broadband network technologies such as ATM, Gigabit IP-overfibre, and pure-optical networking. His research interests include broadband-multimedia communications, multimedia services, network protocols, and wireless-sensor networks, service-oriented computing and networking; multimedia broadband communications, wireless sensor networks and protocols research, Quality of Service (QoS) modeling and architecture of communication processes, vehicular communications, and intelligent transportation. He is the author or coauthor of more than 100 international journal and conference research papers, and is the holder of four patents in these fields.

Robert H. Deng received the Bachelor's degree from the National University of Defense Technology, Changsha, China, the M.Sc. and Ph.D. degrees from the Illinois Institute of Technology, Chicago.

Since 2004, he has been with the Singapore Management University, Singapore, where he is currently a Professor, an Associate Dean for Faculty and Research, School of Information Systems. Prior to this, he was a Principal Scientist and a Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. He is the holder of 26 patents and author or coauthor of more than 200 technical publications in international conferences and journals in the areas of computer networks, network security, and information security.

Prof. Deng is an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, an Associate Editor of *Security and Communication Networks Journal* (John Wiley), and member of Editorial Board of *Journal of Computer Science and Technology* (the Chinese Academy of Sciences). He has served as a General Chair, Program Committee Chair And Program Committee Member of numerous international conferences. He was the recipient of the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006. He was named Community Service Star and Showcased Senior Information Security Professional by $(ISC)^2$ under its Asia-Pacific Information Security Leadership Achievements program in 2010.

Shengsheng Yu was born in 1944. He received the B.E. degree from the Electronic Engineering Department, Huazhong University of Science and Technology, Wuhan, China, in 1966.

He is currently a Professor and a Supervisor of doctor program at Huazhong University of Science and Technology. He had been an Advanced Visiting Scholar in West Germany in 1983. His current research interests include streaming media, computer network, and storage.