SECURITY BIOSIGNAL TRANSMISSION BASED ON FACE RECOGNITION FOR TELEMEDICINE

Jen-Chien Chien*, Jeng-Pang Wang*, Chien-Lung Cho* and Fok-Ching Chong[†]

**Institute of Electrical Engineering, National Taiwan University, Taipei, Taiwan*

[†]fcchong@cc.ee.ntu.edu.tw

Accepted 31 January 2007

ABSTRACT

In telemedicine, an insecure and vulnerability medicine information system is important for nursing staff and patients. Relatively private information stolen by others still can be corrected. However, if attacked by hackers, mistakes in diagnosis can threaten the patient's life. In order to simplify the procedures in the authentication of telemedicine and to emphasize security in the patient's data, this paper proposes utilizing the symmetric key cryptography and the biometric authentication. We use a face eigenvector to insert the patient's physiological signals and to combine symmetric key cryptography thus protecting the integrity of the patient's data and improving the mode of operations.

Keywords: Telemedicine; Authentication; Eigenvector; Symmetric key cryptography.

INTRODUCTION

In early 1986, in order to meet the requirements for the transportation information system to increase traffic transportation efficiency, Europe developed the radio data system (RDS) that utilized FM radio to transmit radio signal.¹ The RDS is the predecessor of the Data Radio Channel (DARC). The mobile information system is integrated with the intelligent transportation system (ITS). Jayaram, Shamala and Srikanta used the Personal Digital Assistant (PDA) and wireless technique for conveying medical information in 1996.² In 1998, Robert addresses a real-time biosignal system using Global System for Mobile communications (GSM) to transmit an Electro-Cardiogram (ECG) signal.³ In the same year, Shin-Ichi assessed and tested a patient monitoring system using mobile computers and a wireless connection.⁴ A real-time monitoring system for the coronary care unit (CCU) combined the ideas from internet works published by Presedo.^{5,6} This article contains applications using the PDA. In 2001, Pollard

generalized a concept and a structure for an active medical monitoring system.⁷ Although the technology of medical monitoring is well-developed today, the safety and issues concerning ease of using the monitoring system still need further improvement.

In a network application, its operation procedure can be divided into roughly two parts: login and data exchange. The purpose of login is to carry out identity authentication to confirm the user's identity, in order to offer the proper level of service and prevent the user from going beyond his behavior by abusing the authority. Signals in the network physical layer are transmitted by radio, so that every host computer in the regional network can get the data package which other host computers have transmitted. Therefore, it is easy for the hacker to steal these data packages if the transmitted packages are not encrypted. Thus, our system is designed to be an effective and useful system for telemedicine to protect the integrity of the patient's medical data.

[†]Corresponding author: Dr. Fok-Ching Chong, Institute of Electrical Engineering, National Taiwan University, Taipei, Taiwan.

METHOD

System Structure

As shown in Fig. 1, there are four parts in our system, medical information structure, server application, doctor client application and patient client application.

The medical information structure

This structure follows the regulations of Health Level Seven (HL7). Health Level Seven is one of several American National Standards Institute (ANSI)-accredited Standards Developing Organizations (SDOs) in healthcare. Most SDOs produce standards (sometimes called specifications or protocols) for a particular healthcare

domain such as pharmacy, medical devices, imaging or insurance (claims processing) transactions. HL7 domain is the clinical and administrative data. It is an international community of healthcare subject matter experts and information scientists collaborating to create standards for the exchange, management and integration of electronic healthcare information. It promotes the use of such standards within and among healthcare organizations to increase the effectiveness and efficiency of healthcare delivery for the benefit of all. Figure 2 shows how to save the patient's biosignals to the database.

The physiologic signals are collected by variable recorder machines, such as the ECG, EEG, temperature, blood pressure... etc. These signals are monitored by client or server application programs such as IE browser. These signals were transferred via HL7 transfer machine to our database.

Server application

There are three major functions in our server application program. Firstly, identity login at the Client side authenticates to avoid jurisdiction user. Secondly, it records the status of the client site and transmits the information to other client sites that needed.

For example, when a doctor is monitoring a certain remote patient and the on-line server breaks off, the server must transmit this status to the patient. Thirdly, the server site is linked to the Open Database Connectivity (ODBC) and the medical information database. The setting of the data source, calling the API of the

Fig. 1 Chart of four parts in telemedicine system.

Fig. 2 The medical information structure.

ODBC and the linking to data server are all carried out by the server application program and host computer. Thus, the loading of the doctor application and the PDA can be substantially reduced.

Doctor client application

This program includes four main operations: way of setting access parameter, build connection and login to the server, access database and receiving subject's instant mental signal and parameter.

1. Way of setting access parameter

It saves the patient information's service item and process. Once login, the user is allowed to choose hospital, department, user or environment. In order to improve the program's flexibility and convenient during use, these information changes will be checked with the latest version in the database and updated automatically.

2. Build connection and login to the server

The purpose is to build a reliable connection with the server to access the patient's static information. At the same time, when the patient and the doctor are login, the server site would send the IP address and the encrypted value of the patient to the doctor and show the IP address of the doctor to the patient. This achievement obeys the Transmission Control Protocol standard.

3. Access patient's static information

The doctor can access the patient's data from the server with SQL commands. However, users just need to use the graphic user interface or input any keyword to access any knowledge database and the system can automatically make and send the SQL command to the server site.

4. Receive and set patient's instant mental signal and parameter

The doctor's application program will set the PDA internet interface once it receives the login message from the patient site. Instant mental message is received, via User Datagram Protocol (UDP); for an effectiveness period of time. However, if some of information are lost during delivery; even it has been resent, the information has already lost its effectiveness; it can also be the cause of delay of sending another instant information.

Patient client application program

To receive the patient's bio-signals and bio-parameters from the medical device is the major task of the patient

client application program. These signals are transmitted through the internet to the doctor site and vice versa. The patient can check the correctness of these static information.

Recognition

Before receiving the patient's physiological information, the server will first identify the patient's status. The webcam will first capture the patient's face. Then an algorithm is used to calculate his eigenvalue. This data is sent to the server and the transmitted signal is a composite eigenvalue of the patient's face and is to be compared with the data bank's picture information which was built earlier. This authentication process will secure the interaction of patient to relative service and diagnostic practice. "Face recognition" is used here as biological authentication for the following:

- High identifiable rate of face recognition.
- Ease of getting relative instrument.
- High acceptability for user.

Firstly, Principal Component Analysis (PCA) is used to analyze and code into digital values. These digitally-represented faces of a certain eigenvalue are embed into the recorded biologic face figure. Secondly, recognize a person's status by Face information shall comply with relative safe guards which are mentioned as follow, therefore ensuring that the relative information have already been totally protected.

Encryption

The algorithm of the encryption is 512 bits Rehabilitation Services Administration (RSA) and the Hash Function is Secure Hash Algorithm (SHA). We use the face of eigenvalue and collocate it with the RSA to encrypt the biosignal data. This prevents any cracking method.

MATH

Recognition

Most face detection schemes can be divided into two different strategies. The first method is based on the detection of facial features (e.g. Yow and Cippola⁸), whereas the second approach tries to detect a face pattern as a whole unit (e.g. Sung and Poggio,⁹ Moghaddam and Pentland¹⁰). Following the second approach, each image pattern of dimension I by J can be considered as a vector x in $N = I * J$ dimensional space. Obviously, images of faces will not be randomly distributed in this high-dimensional images space. A suitable means to reduce

the dimensionality of the data set is the principal components analysis (PCA). The central idea of principal components analysis is to find a low-dimensional subspace (the feature space) which captures most of the variation within the data set and therefore allows the best least square approximation (Jolliffe¹¹). When used for face detection and recognition, this principal subspace is often called the “face space” which is spanned by the “eigenfaces”.¹²

Given a set of training vectors $\{x\}$ (face samples) with sample covariance matrix Σ , the Karhunen Lve Transform (KLT) basis can be computed by solving the eigenvalue problem.

$$\Lambda = P^T \Sigma P \quad (1)$$

where P is the eigenvector matrix of Σ and Λ the diagonal matrix of the eigenvalues.

The orthogonal projection matrix PM into the M -dimensional principal subspace ($M \ll N$) is given by the M eigenvectors corresponding to the largest eigenvalues. These eigenvectors (“eigenfaces”) form the columns of the projection matrix PM . The principal components vector y is obtained by projecting the image into the face space:

$$y = P_M^T (x - \bar{x}). \quad (2)$$

where $\bar{x}$ denotes the mean face image.

The classification of the image pattern containing N pixels as “face” or “non-face” is only based on its M principal components y_i .

The approximation of a face using M “eigenfaces” is given by $\hat{x} = P_M y + \bar{x}$. The residual reconstruction error ε^2

$$\begin{aligned} \varepsilon^2 &= \|(x - \hat{x})\|^2 \\ &= \|(x - \bar{x}) - P_M y\|^2 \\ &= \|x - \bar{x}\|^2 - \sum_{i=1}^M y_i^2 \end{aligned} \quad (3)$$

indicates how well the test pattern can be approximated in the face space. Thus, the “distance from face space” (DFFS) defined by Eq. (3) can be used to determine if the image pattern represents a face.¹²

The distance between the projected image and the mean face image in the feature space is given by the norm of the principal component vector. Since the variance of a principal component y_i is given by the associated eigenvalue λ_i , the squared Mahalanobis distance d^2 provides a suitable measure of the difference between

the projection of the test image and the mean face:

$$d^2 = y^T \Lambda^{-1} y = \sum_{i=1}^M \frac{y_i^2}{\lambda_i}. \quad (4)$$

For the detection task, it is customary to use only the DFFS for the decision criterion.¹² As shown in the next section, the incorporation of the “distance in face space” (DIFS) defined by Eq. (4) improves the robustness of the detection significantly if the detection is performed on the skin probability image.

Encryption

As for safety requirement for real-time ECG transmission, since there is not any possibility for patient willfulness to send wrong ECG signals to the doctor; therefore the non-repudiation can be except, however any other possibility attacking way and relative safety requirement shall be achieve. Due to non-repudiation which can be accepted, therefore the mechanism can be achieved only by paired encryption key. The expression of encryption key can be via downloading through USB or series port from the server host. This mechanism is shown in Fig. 3.

- (1) Patient key in his identification number to the server and the server will extract user’s secret encryption key (K_{client}) from the setting file or data bank by identification.
- (2) Server will return one piece but non-repeatable information to patient’s site.
- (3) After the patient’s site replies its hash value, the server will check it with its original hash value

Fig. 3 Diagram of encryption mechanism process.

to ensure customer's site really knows the correct K_{client} ; its "Right identification".

- (4) The system will repeat step 2 and step 3, thus in case of malfunction or wrong login.

After identification is completed, it uses K_{client} for decoding and then start delivering information. The most important process in the progress which is mentioned before is item (2), (3) or (4); it means to ask the question from one site and confirm whether reply information is correct or not to precede authentication. Since this way of authentication does not have any repeatability, therefore can avoid any attack by resend.

RESULT

We select 10 men and take 18 pictures each. Every gray level picture size is 92×112 pixels. We divide them into two classes and four sub-classes:

Two class: with or without glasses.

Four sub-class: normal face, head position (up, down, right, left), face motion (happy, surprise, anger) and with eyes closed.

Therefore, each man has 18 pictures and there are total of 180 pictures in our image database. As shown in Fig. 4 using the PCA algorithm, we can get 20 eigen-vectors representing these eigenfaces. The first eigenface keeps the most ingredients of these image databases and it is difficult to discriminate in the twentieth eigenface.

Figure 5 is the login program for PDA. The doctor types his number and password and press the "Connect" button. This program shows the status of the

Fig. 5 Login frame of PDA application.

connection. If it is a success, the connection will change to the "Message" frame shown in Fig. 6. The function of the "Message" frame is communication between doctor and patient. In this frame the doctor can change to another frame (Patient List frame and Monitor frame). In the "Patient List" frame, doctor can review the patient basis data and his clinical examine shown in Figs. 7 and 8. Doctor can also monitor the patient's physiologic signal. Figure 9 is the monitoring ECG signal.

DISCUSSION

There are two discussion points in our system, which include EGG signal's aliasing and success rate in face recognition; these two parts can be well controlled above average. In face recognition, there are good recognition rates in these faces image in the database after they are trained via PCA algorithm. We can select the appropriate condition to increase recognition rate. Figure 10 is shows the ECG data that is done with encryption. The top of this picture is the original ECG signal and the middle is the ECG signal done with the encryption and the bottom is recovery of the ECG signal. Therefore, our security method will not let the signal be distorted. However, there is still a problem in security safe guard if any signal contains the zero value; the zero

Fig. 4 Twenty orders of the eigenface.

Fig. 6 Message frame of PDA application.

Fig. 8 Patient's clinical examine frame of PDA application.

Fig. 7 Patient list frame of PDA application.

Fig. 9 Monitor frame of PDA application.

Fig. 10 The diagram of ECG signal before encryption (top), encryption (middle) and after encryption (bottom).

value makes the signal cannot be restored. Even so, we can set another value to change these zero values to improve this deficiency. Therefore, this system can put in use in the telemedicine.

CONCLUSION

The Karhunen–Lòve Transform can reduce complexity computing which is associated with principle component analysis algorithm. Karhunen–Lòve Transform is used to find a lower-dimensional representation that accounts for the variance of the features. The object of factor analysis is to find a lower-dimensional representation that accounts for the correlations among the features. In our system, the user can be accurately identified using PCA algorithm. Furthermore, there is

almost no aliasing the biosignals with our encryption mechanism. This could benefit the telemedicine.

REFERENCES

1. <http://www.wcbn.org/history/wcbntime.html>.
2. Jayaram N, Shamala N, Srikanta, Wireless information perspectives for integrated health care, *IEEE Int Conf Personal Wireless Commun*, pp. 239–241, 1996.
3. Robert SHI Modelling of GSM-based mobile telemedical system, *Proc IEEE Ann EMBS Int Conf*, Vol. 3, pp. 1166–1169, 1998.
4. Shin-ichi N, Koji O, Toshimori H, Katsunori Y *et al.*, Evaluation of the multimedia-multicast-mobile-terminal for hospital patient care, *Proc Int Conf Inf Networking*, 1998.
5. Barro S, Presedo J, Castro D, Fernández-Delgado M, Fraga S, Lama M, Vila J, Intelligent telemonitoring of critical-care patients, *IEEE Eng Med Biol*, 1999.
6. Presedo J, Castro D, Vila J, Fernández-Delgado M, Fraga S, Lama M, Barro S, Wireless interface for monitored patients in coronary care units, *Proc Ann EMBS Int Conf*, 2000.
7. Pollard JK, Rohman S, Fry ME, A web-based mobile medical monitoring system, *Int Workshop Intell Data Acquisition Adv Comput Syst: Technol Appl*, 2001.
8. Yow KC, Cipolla R, Feature-based human face detection. *Image Vision Comput* **15**:713–735, 1997.
9. Sung KK, Poggio T, Example-based learning for view-based human face detection. *IEEE Trans PAMI* **20**:39–51, 1998.
10. Moghaddam B, Pentland A, Probabilistic visual learning for object representation. *IEEE Trans PAMI* **19**:696–710, 1997.
11. Jolliffe IT, *Principal Component Analysis*. Springer, New York, Berlin, Heidelberg, Tokyo, 1986.
12. Turk M, Pentland A, Eigenspaces for recognition, *J Cogn Neurosci* **3**:71–86, 1991.