SCIENCE CHINA
Information Sciences

• LETTER •

May 2018, Vol. 61 059103:1–059103:3
doi: 10.1007/s11432-017-9188-8

Fingerprint-based access to personally controlled health records in emergency situations

Shaopeng GUAN[1,3*], Yongyu WANG[1] & Jian SHEN[2]

[1]*School of Information and Electronic Engineering, Shandong Institute of Business and Technology, Yantai* 264005*, China;*
[2]*School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing* 210044*, China;*
[3]*Haian High-Tech Research Institute of Nanjing University, Haian* 226600*, China*

Received 21 January 2017/Accepted 19 July 2017/Published online 9 November 2017

Citation Guan S P, Wang Y Y, Shen J. Fingerprint-based access to personally controlled health records in emergency situations. Sci China Inf Sci, 2018, 61(5): 059103, doi: 10.1007/s11432-017-9188-8

Dear editor,

Medical records are the original diagnosis and treatment calendar of the patient in medical institutions, including the patient's personal information, diagnosis results, treatment methods, prescriptions, and medical history. Medical records not only form the basis for the treatment of patients, but also provide a reference for future diagnosis. Traditionally, medical records are handwritten by doctors. With the application of information and network technology in the medical field, Electronic Health Records (EHRs) replace handwritten medical records.

Compared with handwritten medical records, EHRs possess many merits. They break through the geographical constraints to provide a great convenience for different medical institutions to share the patients' medical information. However, EHRs are doctor-centered and used to facilitate medical institutions. According to the U.S. Health Insurance Portability and Accountability Act (HIPAA), patients are entitled to know their medical records. Therefore, Personally Controlled Health Records (PCHRs) emerged in recent years.

PCHRs are special web-based systems of electronic medical records. The server of PHCRs stores all copies of patients' EHRs from different medical institutions in the database. Patients can securely access to the EHRs anytime and anywhere through the network. Personal control of EHRs well protects the privacy of patients. But, in some special occasions, it will be inconvenient and even result in serious consequences. For instance, if a patient is in a coma, the doctor need to access the patient's PCHRs immediately to take effective aid measures. In this case, obviously, the patient cannot personally access PCHRs or issue access authorization to the doctor.

In this letter, we put forward a scheme of temporary access to the PHCRs.

Scheme. When the patient accesses the medical records over the network, the server should have a robust authentication mechanism and an access control mechanism. In addition, medical records should be kept intact and confidential during the transmission over the network. These problems can be addressed by conventional network security technologies such as data encryption and electronic signature [1–4]. But new problems emerge along with the popularization and application of various PCHRs, one of which is the unconventional access authorization mechanism in case of a special occasion. In other words, how one can get access authorization of PCHRs without the participation

* Corresponding author (email: konexgsp@gmail.com)
The authors declare that they have no conflict of interest.

of the patient in an emergency situation. If this problem is not addressed properly, some serious consequences may occur. Nevertheless, there is little research on this problem [5, 6].

We proposed a scheme leveraging the fingerprints of patients to aid doctors to get temporary access authorization of PCHRs. The basic idea is as follows. The doctor collects the fingerprint of the patient as the authorization key and uploads it with the basic information of the patient such as the name and the ID number to the server of PCHRs. The server conducts a match between the submitted information and the original data stored in the database. If the data are confirmed, the doctor is authorized temporary access to the PCHRs. In order to reduce the space occupied by the fingerprint and improve the authentication efficiency, we further propose adopting the Principal Components Analysis (PCA) method to store and match the fingerprint.

PCA is a method commonly used in multivariate statistical analysis to simplify the data set. It reduces the dimension of the data by replacing a p-dimensional X-space with an m-dimensional Y-space ($m < p$) with little loss of information. The calculation process of PCA is illustrated as follows [7].

Assuming the data are two-dimensional, it can be represented by two vectors as

$$X = [X_1, X_2, \ldots, X_n]^{\mathrm{T}},$$
$$Y = [Y_1, Y_2, \ldots, Y_n]^{\mathrm{T}}.$$

To understand the relationship between the two components, we need calculate their covariance which is defined as [7]

$$\mathrm{cov}(X, Y) = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{n-1},$$

where $\mathrm{cov}(X, Y)$ is the covariance, and $\bar{X} = \frac{\sum_{i=1}^{n} X_i}{n}$, $\bar{Y} = \frac{\sum_{i=1}^{n} Y_i}{n}$ are averages of the two components, respectively. When the data set is multidimensional, the covariance of each pair of dimensional components needs to be computed. The number of covariance will be

$$\frac{n!}{2 \times (n-2)!}.$$

Therefore, we can adopt a matrix to organize the covariance. The definition of the covariance matrix is given by

$$C_{n\times n} = \{c_{i,j} | c_{i,j} = \mathrm{cov}(D_i, D_j)\}.$$

D_i, D_j are the i and j dimensional components. Taking three-dimensional data set $\{X, Y, Z\}$ as an example, the covariance matrix is

$$C_{3\times 3} = \begin{bmatrix} \mathrm{cov}(X,X) & \mathrm{cov}(X,Y) & \mathrm{cov}(X,Z) \\ \mathrm{cov}(Y,X) & \mathrm{cov}(Y,Y) & \mathrm{cov}(Y,Z) \\ \mathrm{cov}(Z,X) & \mathrm{cov}(Z,Y) & \mathrm{cov}(Z,Z) \end{bmatrix}.$$

It can be seen that the covariance matrix is symmetric. Variances of all components lie in the diagonal. We compute eigenvalues and eigenvectors of the covariance matrix and arrange them in ascending order according to the eigenvalues. The former p eigenvectors are selected as feature vectors to form a matrix denoted by V_f. Meanwhile, the original data matrix is normalized and then transposed. The transposed matrix is expressed as M_a. At last, the dimension-reduced data is as follows:

$$F_d = V_f \times M_a.$$

The original data is reduced to be p dimensional. F_d, in place of the original fingerprint data, is stored on the server. The occupied space of the fingerprint becomes smaller.

The designed system prototype is illustrated in Figure 1.

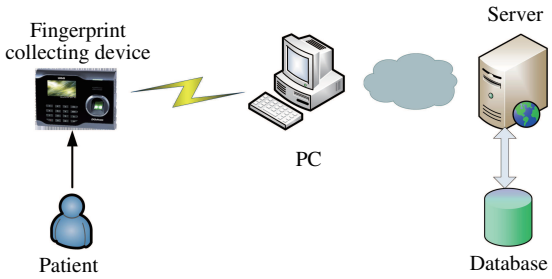

Figure 1 (Color online) System prototype of the scheme.

Experiments. Based on the prototype, we set up a simple experimental environment of server/client architecture and conduce fingerprint-matching experiments on the fingerprint database Db1 of FVC2006 [8]. The finger image format is BMP, 256 gray-levels, uncompressed. Its size is 96 pixels × 96 pixels. The images are acquired by the electric filed sensor.

In essence, fingerprint matching is the comparison of feature areas. Singular points are one of the most important global features of fingerprints. They are located in the middle of fingerprints. The uniqueness of singular points makes them an important basis for fingerprint matching, and the regions around the singular points of different fingers are not exactly the same. Therefore, the regions (marked as region of interest, ROI) can be selected as matching basis [9].

We detect singular points using the classic Poincare Index method. Because the location and

angle varies every time when the user's fingerprint is taken, fingerprint images are slightly different, as well as the coordinates of fingerprint features. Therefore, we need to know the direction of the fingerprint before recognizing the ROI. Firstly, we find the center of the ROI using the singular points [7]. Then, we calculate the gradient of the gray value in different directions from the center. At last, we take the direction along with the maximum gradient direction as the axis, and segment an area of 20 pixels × 25 pixels around the center point as the ROI. We adopt the PCA method on the ROI, and select the first five principal components as the final results.

The match of two fingerprints is conducted by computing the Euclidean distance of them. Suppose the fingerprint data in the database is represented as $A[A_1, A_2, \ldots, A_n]$, the fingerprint data to be compared is represented as $B[B_1, B_2, \ldots, B_n]$, then the Euclidean distance is

$$d(B, A) = \|B - A\|.$$

In fact, fingerprint matching is a process of pattern recognition, and the matching criteria is the degree of similarity. The result depends on the threshold set in advance. In the experiment, we set the threshold of Euclidean distance as 10% of the length of $\|\mathrm{A}\|$. That is to say, when $d(B, A)$ is less than the threshold, the match succeeds.

The experimental results have verified the feasibility of the scheme. However, a new problem arises. The electronic fingerprint is easy to store and propagate, and will be kept in the PC or the smartphone after it is used. Once the fingerprint is illegally copied and reused, the medical records of the patient can be arbitrarily accessed and the privacy of the patient is disclosed. To solve this problem, some rules as follows are effective: (1) making it the law that the doctor must delete the fingerprint after the first aid; (2) limiting the access right of the emergency doctor to be "read only"; (3) improving the log function of the PCHRs system to make sure any access to medical records through the fingerprint leaves a detailed log in the server.

Besides the above rules, we also take the privacy problem into consideration when designing the system prototype. The hint of the needed fingerprint is changeable on the login interface. It is controlled by the patient. That is to say, the patient can change the stored fingerprint in the server, and he can also change the hint on the login interface after his recovery. The changing is protected by a password and can only be operated by the patient.

Conclusion. PCHRs are newly emerged management systems of medical records, which are web-based and personally controlled by patients. Personal control of PCHRs protects the privacy of patients, but in some occasions, it may cause inconvenience and even lead to serious consequences. We proposed a fingerprint-based scheme of access to PCHRs in emergency situations. In the scheme, the basic information with the fingerprint of the patient is used to obtain temporary access right of medical records. We designed the prototype of this scheme, discussed existing fingerprint matching methods, and adopted the PCA method to store and match the fingerprint to reduce the occupied server space and improve the authentication efficiency. At last, we conducted experiments on the fingerprint database of FVC2006 to verify the feasibility of the scheme. We also presented some rules to prevent illegal reuse of the fingerprint and protect the privacy of the patient.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61402223, 61300235) and Natural Science Foundation of Shandong Province (Grant No. ZR2014DL008).

References

1 Fu Z J, Ren K, Shu J G, et al. Enabling personalized search over encrypted outsourced data with efficiency improvement. IEEE Trans Parall Distrib Syst, 2016, 27: 2546–2559
2 Xia Z H, Wang X H, Zhang L G, et al. A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing. IEEE Trans Inform Forens Secur, 2016, 11: 2594–2608
3 Wang J W, Lian S G, Shi Y Q. Hybrid multiplicative multi-watermarking in DWT domain. Multidimension Syst Signal Process, 2017, 28: 617–636
4 Zhou Z L, Wang Y L, Wu Q M J, et al. Effective and efficient global context verification for image copy detection. IEEE Trans Inform Forens Secur, 2017, 12: 48–63
5 Chen T T, Zhong S. Emergency access authorization for personally controlled online health care data. J Med Syst, 2012, 36: 291–300
6 Zhang Y, Dhileepan S, Schmidt M, et al. Emergency access for online personally controlled health records system. Inform Health Soc Care, 2012, 37: 190–202
7 Yuan C S, Sun X M, Lv R. Fingerprint liveness detection based on multi-scale LPQ and PCA. China Commun, 2016, 13: 60–65
8 Fierrez J, Ortega-Garcia J, Toledano D T, et al. BioSec baseline corpus: a multimodal biometric database. Patt Recognit, 2007, 40: 1389–1392
9 Chen B J, Yang J H, Jeon B, et al. Kernel quaternion principal component analysis and its application in RGB-D object recognition. Neurocomputing, 2017, 266: 293–303