ATLANTIS PRESS
Advances in Computer Science Research, volume 58
Modeling, Simulation and Optimization Technologies and Applications (MSOTA 2016)

The Design of Smart Grid Identity Authentication System Based on Fingerprint Identification

Xiuqing Wang*, Jimin Zhao, Xueying Qiao and Fangyuan Che
No.1038 Dagu South Road Hexi District Tianjin, China.
*Corresponding author

***Abstract*—For the problem of the safe integration between Internet and the smart grid, a server based on C/S mode of fingerprint information and user information registration was used in power system and a fingerprint acquisition system based on C/S mode was designed, realizing the collection of fingerprint image processing and extraction of characteristic value. A database was established on the server, using ADO.NET technology to access the database and operate it. The smart grid authenticated access login information management system based on B/S pattern was designed by invoking the ActiveX controls library through the web page.**

Keywords-smart grid; C/S mode; fingerprint identification; B/S mode; double certification

I. INTRODUCTION

There are 4 main types of smart grid information management system platform: Host terminal mode, File server mode, Client / Server Mode, and Browser / Server Mode. With the increasing demand of users, the smart grid information management system needs to be developed from the traditional single access to a diversified way. Therefore, the traditional C/S (client / server) mode is needed to be extended to B/S (Browser / server) mode. In addition, the reliable identity authentication between the user and the equipment is even more important. When the power system external users access to the system, the way by user name and password for routine authentication is not reliable. Therefore, the user account related data, customer files, electricity and other sensitive information on the site are confronted with big secure hidden trouble. In this paper, based on the current mature biometric fingerprint identification technology, a dual authentication access system for smart grid information management with higher accuracy is proposed [1].This system uses the fingerprint and password double authentication to the external users who access the smart grid system for reliable authentication through the browser.

II. SYSTEM DESIGN

This system mainly consists of two parts. The first part is the fingerprint and user information registration module of the smart grid information management server that based on the C/S model. The fingerprint image and the characteristic information of the user is extracted, and then saved in the server database. The second part is the dual authentication access module based on B/S mode. It uses the fingerprint and password double authentication method to carry on the reliable authentication to the user identity when the external users access the system through the browser Web server. The user input information and collected the fingerprint image to extract the fingerprint characteristic information through the website login screen, making it match with the user and the fingerprint information stored in the database [2]. We take measures to control user accessing to the system and protect sensitive information from being damaged. The system block diagram is shown in figure 1:

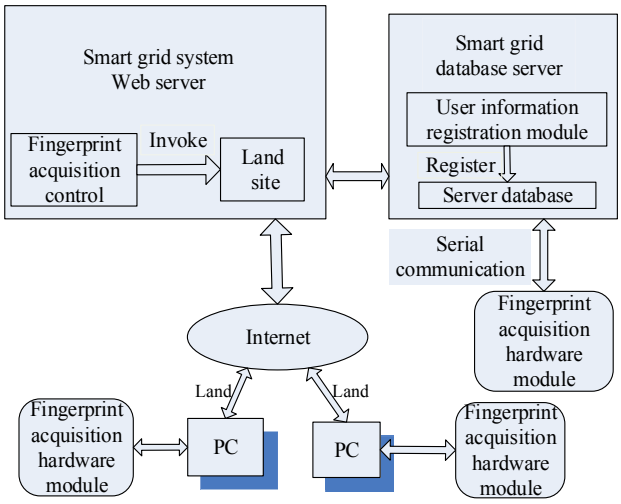

FIGURE I. SYSTEM BLOCK DIAGRAM

III. ACQUISITION AND PROCESSING OF FINGERPRINT IMAGE

In the process of fingerprint acquisition, the hardware module of the fingerprint acquisition TFS-M71 is used as the slave device, and PC is used as the main equipment. The system is controlled by PC to send commands to the fingerprint acquisition hardware module.

A. Processing of Fingerprint Image

In this paper, the Gabor filter is used to enhance the image. Firstly, ridge frequency estimation is used to calculate the ridge frequency of the fingerprint image, and the least mean square direction estimation algorithm is used to calculate the direction of fingerprint. In order to increase the robustness of the rotation of the direction map, direction angle is divided into 8 directions. The fingerprint image is processed by Gabor filter in 8 directions [3]. At last, the final enhanced image is obtained after the superposition of the 8 filtered directional images.

Local adaptive method is used to binarization in this paper. At first, a fingerprint image is divided into sub blocks of w*w, and then find the threshold of each sub block. According to the

fixed threshold value of each sub block, the gray value of the pixel points of each sub block is determined. OPTA (single connected thinning algorithm) is used to thinning. Figure 2(a), (b), (c) are the original image, enhancement image and thinning image.

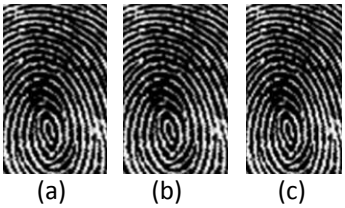

FIGURE II. THE ORIGINAL AND PROCESSED IMAGE

B. *Extraction of Fingerprint Image Feature*

Firstly, we construct the 3*3 neighborhood of the refinement graph, and extract the feature points. After binarization, only leaving black and white two pixels, and the value can only be from 1 to 0 or from 0 to 1. We assume a point P on the ridge line [4]. Cn(p) is the number of the value changes, and Sn(p) is the number of points around which pixel is 1. The fingerprint feature points are extracted by marking each endpoint and bifurcation point.

Pseudo feature points include edge and internal pseudo feature points. The way of eliminating edge feature points is as follows: If an endpoint is in the foreground area, and there's a background block around it, it is on the edge of foreground area which should be removed. If the location block of a endpoint is not adjacent to the upper and lower blocks, it shows that the endpoint is on the edge of the foreground area but no way to remove it by using the segmentation template. Then we should judge the distance from the endpoint to the edge of the fingerprint image. If it is less than the threshold value, remove it [5]. The way of eliminating internal pseudo feature points is as follows: there're 4 types internal pseudo feature points, short - term, burr, bridge and ring. We can track pixel lines according to the ridge tracing method, and then remove the pseudo feature points. Contrast of pseudo feature points as figure 3.

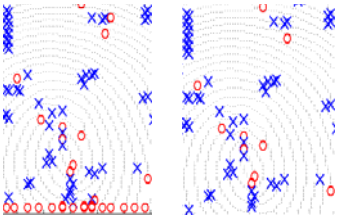

FIGURE III. CONTRAST DIAGRAM OF ELIMINATING PSEUDO FEATURE POINTS

In the process of obtaining the eigenvalue, the maximum curvature point of the image is specified as the center point. The coordinate of the center point is defined as (m, n), and the curvature is Cur (m, n). We set the coordinate of the feature point (i,j),and the curvature is Cur (i,j). The relative distance between the central point and the feature points is d(i,j), and the curvature difference between the center point and the characteristic point is α(i,j). As in:

$$d(i,j)=\sqrt{(m-i)^2+(n-j)^2} \tag{1}$$

$$d(i,j)=\sqrt{(m-i)^2+(n-j)^2} \tag{2}$$

d(i,j) and α(i,j) is used as the eigenvalue to describe each feature point, and then saved in the database.

IV. USER REGISTRATION MODULE IN C/S MODE

When the user is registered, the user information and the fingerprint information are stored in the database, which used as the login authentication information.

Basic data, account data, power customer files, customer electricity and other information are stored in the power system database server. Database management is not only need to meet the interactive demand, but also to meet the requirements of the information security of power system [6]. In this paper, Access is used to design the database that not only contains the basic information such as fingerprint and password, but also contains the user electricity and so on [7]. The user information (user number, user name, password and fingerprint eigenvalue) is stored in the server database by staff, then external users can access the system through the browser. User registration interface is shown in figure 4:

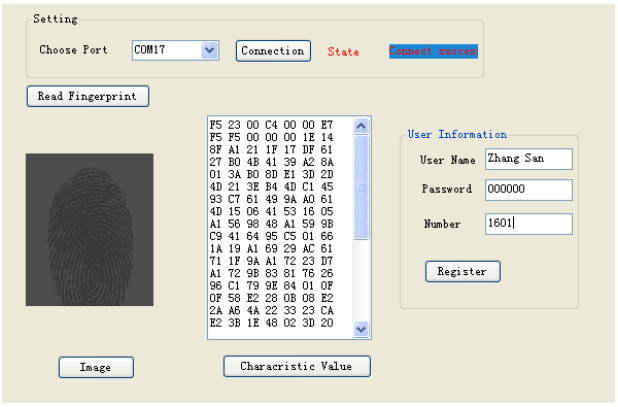

FIGURE IV. USER REGISTRATION INTERFACE

V. DUAL AUTHENTICATION LOGIN MODULE IN B/S MODE

The realization of fingerprint and password dual authentication based in B/S mode includes two aspects. On one hand, when access the site, the user need to input their user name and password. The system will collect fingerprint images and extract eigenvalues after user information matching successfully. On the other hand, the eigenvalues will be matched with the eigenvalues in database. Flow chart of dual authentication login is shown in figure 5:

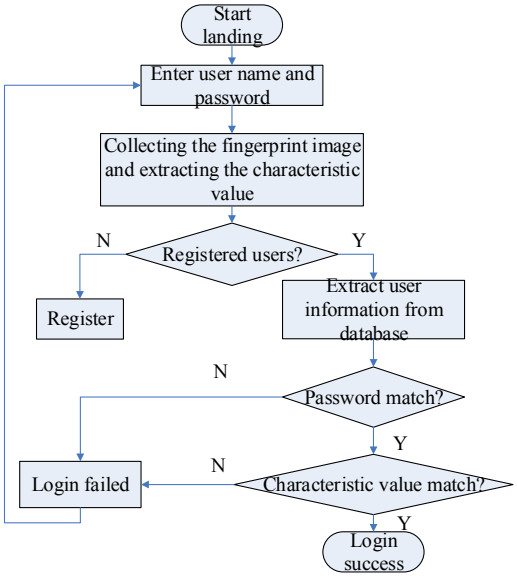

FIGURE V. DOUBLE AUTHENTICATION LOGIN FLOW CHART

In order to get the matching effect of the two fingerprint images, the eigenvalues are matched based on point pattern matching. We set a limit of allowable error when compared. Range error limit is Sd, and angle error limit is $S\alpha$. The eigenvalue of a characteristic point of the fingerprint image to be recognized is $(d_{ide}(i,j),\alpha_{ide}(i,j))$. The eigenvalue of the characteristic point of an image in the database is $(d_{save}(i,j),\alpha_{save}(i,j))$. The distance between feature point and center point is Δd, and the curvature difference between feature point and center point is $\Delta\alpha$.The calculation is shown in:

$$\Delta d = \left| d_{ide}(i,j) - d_{save}(i,j) \right| \tag{3}$$

$$\Delta\alpha = \left| \alpha_{ide}(i,j) - \alpha_{save}(i,j) \right| \tag{4}$$

Due to the difference degree in the process of fingerprint acquisition, the position and angle of the feature points will be changed, and some errors may be introduced in the calculation process. Therefore, when the difference between the fingerprint and the characteristic data stored in the database is less than the allowable error value, the characteristic points can be considered as the same one [8]. After repeated experiments, set the threshold to 10. That is, when the effective feature points have 10 successful comparison, it can be considered to be the same fingerprint. The landing block diagram is shown in figure 6:

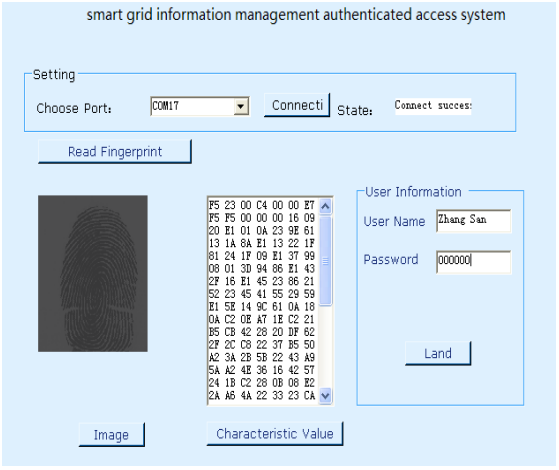

FIGURE VI. LOGIN INTERFACE

VI. CONCLUSION

In this paper, the fingerprint image acquisition, processing and feature extraction based on C/S mode and design of smart grid information management dual authentication system based on B/S mode are completed. The system can allow the user to complete the identity authentication efficiently and accurately through the application case. The authentication system can be widely used in other industries, and improve the level of information security, which has a very high application prospects.

ACKNOWLEDGMENT

Tianjin application foundation and advanced technology research program (14JCZDJC39000).

REFERENCE

[1] Sean Allam,Stephen V Flowerday,Ethan Flowerday. Smartphone information security awareness: A victim of operational pressures[J]. Computers & Security, 2014, 42(5):56-65.

[2] E Kritzinger,E Smith. Information security management:An information security retrieval and awareness model for industry[J]. Computers & Security, 2008, 27(5): 224-231.

[3] T Cervinka, J Hyttinen, H Sievanen. Enhanced bone structural analysis through PQCT image preprocessing[J]. Medical Engineering and Physics, 2010, 32(4): 398-406.

[4] Amjad Rehman, Tanzila Saba. Neural networks for document image preprocessing: state of the art[J]. Artificial Intelligence Review, 2014, 42(2): 253-273.

[5] Efthymia Metalidou,Catherine Marinagi, Panagiotis Trivellas, et al. The Human Factor of Information Security:Unintentional Damage Perspective[J], Procedia Social and Behavioral Sciences, 2014, 147(25): 424-428.

[6] Hyeun-Suk Rhee, Cheongtag Kim, Young U Ryu. Self-efficacy in information security:Its influence on end users' information security practice behavior[J]. Computers & Security, 2009, 28(8): 816-826.

[7] Vivek A Sujan, Michael P Mulqueen. Fingerprint identification using space invariant transforms[J]. Pattern Recognition Letters, 2002, 23(5): 609-619.

[8] Surachai Panich. Method of Fingerprint Identification[J]. Journal of Computer Science, 2010, 6(10): 1062-1064.