MULTI-ROLE AUTHENTICATION TECHNOLOGY USES FINGERPRINTS APPLYING TO POWER STATION MANAGEMENT

Tran Thien Chinh[1*], Tran Huy Long[2], Nguyen Canh Minh[3]

Abstract: *In the field of power grid or substation safety, there are always strict requirements for access to or from the power station for handling and operating equipment, as well as complying with the process of manipulating electrical equipment in the power system is carried out through the process "write and approving the action sheet". It requires the people involved to be confirmed at the same time to perform a particular job. This manual work proved to be ineffective in management, supervision, operation and tracking in the electricity industry. For applications that access/exit important areas, requiring high security, a multi-role authentication system using fingerprints is considered an effective and feasible solution. This article proposes the application of multi-role security authentication technology using fingerprints in power station management, on the basis of inheriting the results of scientific research [1].*

Keywords: Fingerprint; Fingerprint authentication; Fingerprint database; Multi-role fingerprint authentication; Authentication conditions; Fingerprint comparison.

1. INTRODUCTION

Biometric authentication method is a technology that uses physical attributes or behavior patterns, characteristic of human biological features such as fingerprints, iris patterns, speech patterns, and patterns. face, gait,... for identification. In the methods of identification by biometric characteristics, fingerprint identification has been widely used in many fields of life - economy - society. Because a human gait, face or signature can change with time and can be forged or imitated, but fingerprints are the texture of the skin on the tips of human fingers and palms, has unique individual perfect characteristics and is stable over time, easy to store. Each person's fingerprints have unique features that are kept intact and fixed from birth to death. This exclusivity proves that fingerprint recognition is more accurate and effective than other identification methods. Furthermore, fingerprints can be photographed, digitized by a low-cost device, and efficiently compressed, so it only takes a small capacity of space to store large amounts of fingerprint information.

In the field of electrical safety, for example, according to the regulations for the jobs that require a mission letter to ensure safety at work, the people responsible for the safety of the mission letter include: the person who issued the vote (or person ordering the work), the person who leads the work, the direct commander (or the supervisor), the person who allows the to work (or the operator), the employee of the work unit. As such, those who participate in the safety process while working on the electrical network require permission or participate in the concurrent implementation through the "Mission Letter". But if applying a multi-role authentication system that uses fingerprints in the participation management of these stakeholders, the identification can use the fingerprints (instead of the mission letter) of the people involved (which is a multi-role factor in mission letter management) and furthermore each involved person can use multiple fingerprints (up to 10 fingerprints) for authentication.

2. MULTI-ROLE AUTHENTICATION SYSTEM USING FINGERPRINTS

Architectural design of multi-role fingerprint authentication system consists of two parts as shown in figure 1 [1]:

- Hardware of fingerprint recognition device (figure 2): With the core component is the application embedded software (firmware) loaded in the microcontroller chip. Besides, there are

other components such as: motherboard processing with microcontroller chips and auxiliary ICs, optical sensor fingerprint reader, display screen, speakers, keyboards, access control ports, communication network interface ports. In addition, the hardware may also include a central server system installed with a web interface application, communicating over the network with the processor motherboard to be able to remotely monitor and configure the motherboard and other devices. Software embedded custom dynamic applications including: multi-role security authentication, local and central alerts, record local tracking information, support 10 fingerprints per user, support at least 50 users, add, edit, delete, and assign user roles, continuous registration during a registration session, password security, configurable via Web interface, cancel authentication session, data conservation when power is lost, display information, check the network connection, authentication is valid when simultaneously multiple users with multiple roles are fingerprint authenticated, invalid session authentication after a period of time.

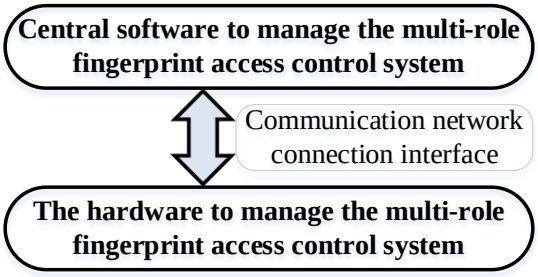


Figure 1. *Multi-role fingerprint authentication system architecture.*



Figure 2. *UCS-MFA-Fix multi-role fingerprint authentication device.*

- Central software to manage multi-role fingerprint access control system performing functions: manage user groups, decentralized use for users, import and prioritize each role (component) in the authentication groups, instant monitoring and warning of access components and time of access authentication, generate access data reports, alerts (by time and access code), filter data by time and extract archived files as ".pdf" with date and time of extracting files from the system, data storage for 1 year (12 months), configure remote fingerprint authentication device via Internet connection, ability to manage at least 300 multi-role fingerprint security authentication devices.

3. PROPOSED APPLICATION OF MULTI-ROLE AUTHORIZATION TECHNOLOGY IN MANAGEMENT OF POWER STATION

3.1. Model of Automatic Fingerprint Identification System (AFIS)

The Automatic Fingerprint Identification System (AFIS) model shown in figure 3 shows the three main steps of AFIS, Step (1) "Fingerprint image enhancement technique", Step 2 "Characterization extraction technique", Step 3 "Characteristic matching technique" [2].

1) Step (1) "Fingerprint image enhancement technique": Fingerprint image capture by sensor device, image quality may vary depending on the type of sensor device or noise of the environment. Therefore, the basic goal of image enhancement technique is to improve image quality and eliminate noise by using two techniques: i) "Technique of Classic Gabor Filtering" includes 6 steps for better image quality as standardization, fast Fourier transform (FFT) filter, segmentation, ridge orientation, ridge Frequency, Gabor filtering; ii) "Quick Fourier Transform Filter Technique".

2) Step 2 “Feature extraction technique”: Once the fingerprint image is enhanced; fingerprint features can be extracted and represented in minutiae and ridge points. This technique has 3 main steps: binaryization, thinning, feature points extractionextraction.

3) Step 3 “Feature Matching Technique”: This technique is the final step in AFIS and is used to decide if two fingerprints are matched or not by comparing its features.

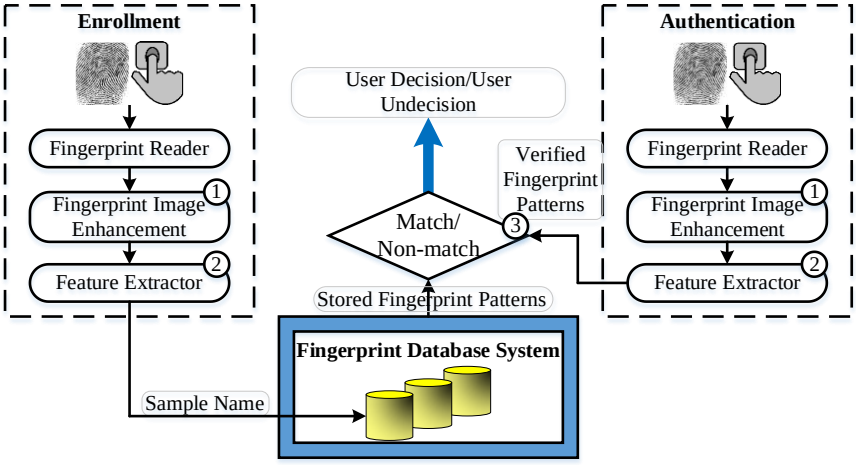


Figure 3. *Model of Automatic Fingerprint Identification System (AFIS).*

3.2. Proposing to build the architecture of automatic fingerprint recognition system in power station management (AFIS-PSM)

AFIS-PSM architecture for power station management is proposed in two aspects: Centralized AFIS-PSM System for National/Regional Management (AFIS-PSM-NRM) and Centralized AFIS-PSM System for National/Regional and Combined with Local Management (AFIS-PSM-NRCLM) [3].

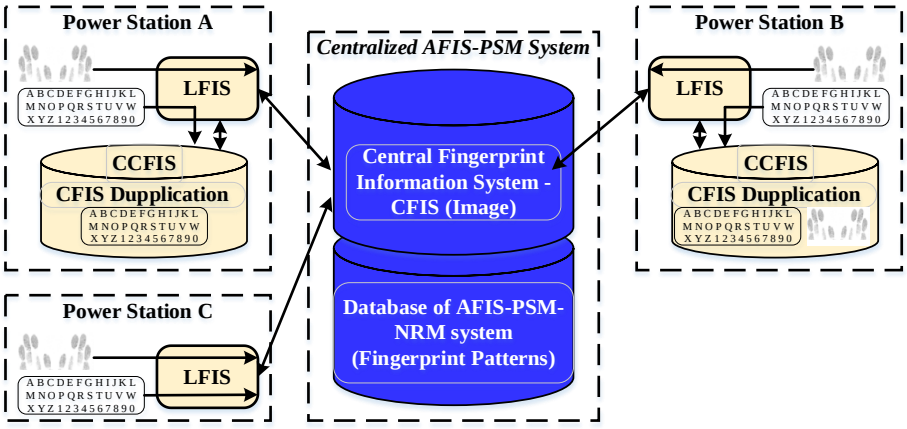


Figure 4. *Model of Centralized AFIS-PSM System for National/Regional Management.*

1) Proposition 1 “Only one Centralized AFIS-PSM System for National/Regional Management (AFIS-PSM-NRM) as figure 4. In this proposal only the AFIS-PSM-NRM function will be provided by Centralized Fingerprint Information System (CFIS). For B power station with a dupplication of the centralized fingerprint information system (DCFIS), queries into AFIS-PSM-NRM system whenever fingerprint identification is required through the Local Fingerprint Information System (LFIS). For A power station only having alphanumeric data copy, or C power station even without dupplication data, it will rely entirely on AFIS-PSM-NRM System through LFIS access system. DCFIS only contains fingerprint images, while the AFIS-PSM-NRM system will store all fingerprint samples (encrypted fingerprints) of all power stations.

2) Proposal 2 "Architecture of Fingerprint Authentication System Applying for Power Station Management": Figure 5 depicts the architecture of fingerprint authentication system used in

power station management. The system is implemented in two forms, fixed fingerprint authentication (at the centralized national/regional point, local,...) and mobile fingerprint authentication (at the power station). In case of fixed fingerprint authentication, if in the database of the local automatic fingerprint identification information system (the power station) already contains a full fingerprint dupplication of the persons concerned, the system will automatical fingerprint quality check with latent and flat fingerprint, scroll fingerprint to automatically identify the people involved. If in the system database of the power station there is no full fingerprint dupplication or there is but not enough or must be queried from the database of AFIS-PSM-NRM system, the system will check the fingerprint quality manually. with latent and flat fingerprints to identify the person involved in need of authentication. In case of mobile fingerprint authentication, the system will automatically check fingerprint quality with flat fingerprint to identify the relevant person.

3) Proposal 3 "Combining fingerprint authentication system with facial recognition system applied in power station management": Accordingly, in addition to using fingerprint authentication system according to the above recommendations, will combine/integrate with facial recognition camera system to further increase accuracy, safety of authentication and security for power stations.

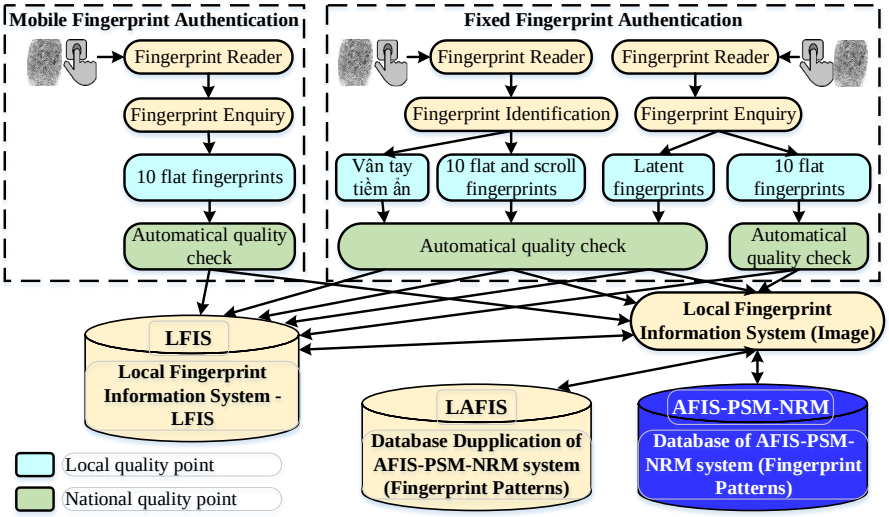


Figure 5. *AFIS architecture applying for power station management.*

The system is implemented in two forms, fixed fingerprint authentication (at the centralized national/regional point, local,...) and mobile fingerprint authentication (at the power station). In case of fixed fingerprint authentication, if in the database of the local automatic fingerprint identification information system (the power station) already contains a full fingerprint dupplication of the persons concerned, the system will automatical fingerprint quality check with latent and flat fingerprint, scroll fingerprint to automatically identify the people involved. If in the system database of the power station there is no full fingerprint dupplication or there is but not enough or must be queried from the database of AFIS-PSM-NRM system, the system will check the fingerprint quality manually. with latent and flat fingerprints to identify the person involved in need of authentication. In case of mobile fingerprint authentication, the system will automatically check fingerprint quality with flat fingerprint to identify the relevant person..

4. CONCLUSIONS

From the research results achieved of the High-Tech Application Project "Development and application of a multi-role security authentication system using fingerprints in the security and

banking sector", code 01/2018/CNC-HDKHCN, under the Program to develop a number of high-tech industries of the Ministry of Industry and Trade, the research group proposed the model and architecture of applying multi-role authentication and security technology using fingerprints in power station management, in order to replace and simplify the process and procedures for implementation on mission letter to ensuring electrical safety. This allows the people involved in the mission letter implementation process to simply register fingerprints (instead of registering, confirming, transferring orders via the mission letter), when performing the power station check process will use their fingerprints to authenticate access to the work area at the power station.

REFERENCES

[1]. Tran Thien Chinh et al., Synthesized report and report on scientific research topics under the high-tech application project "*Development and application of multi-role security authentication system using fingerprints in security and banking sector*", code 01/2018/CNC-HDKHCN, Research Institute of Posts and Telecommunications, 01/2021.

[2]. Ezdihar N. Bifari, Lamiaa A. Elrefaei, Automated Fingerprint Identification System Based on Weighted Feature Points Matching Algorithm, 978-1-4799-3080-7114/$31.00 ©2014 IEEE.

[3]. Laurent Beslay, Javier Galbally, *"Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)"*, JRC Science for Policy Report, JRC 33516-2014.

[4]. Circular 44/2014/TT-BCT dated November 28, 2014 on regulates operating procedures in the national power system

[5]. Electrical safety engineering process in management, operation, repair and construction of power lines and stations - Vietnam Electricity 2002.

[6]. Decide 959/QD-EVN dated August 09, 2018 ngày 09/08/2018 on the issuance of an Electrical Safety Procedure in Vietnam National Electricity Corporation.

TÓM TẮT

ỨNG DỤNG CÔNG NGHỆ XÁC THỰC VÂN TAY ĐA VAI TRÒ TRONG QUẢN LÝ TRẠM ĐIỆN

Trong lĩnh vực an toàn lưới điện/trạm điện luôn đòi hỏi nghiêm ngặt đối với việc truy cập vào/ra trạm điện để xử lý, vận hành thiết bị, cũng như tuân thủ quy trình thao tác thiết bị điện trong hệ thống điện được thực hiện thông qua quy trình "viết và duyệt phiếu thao tác". Ở đó yêu cầu những người có liên quan phải được xác nhận đồng thời "trên giấy" để thực hiện một công việc cụ thể. Việc làm thủ công này tỏ ra không hiệu quả trong quản lý, giám sát, vận hành, lưu vết trong ngành điện. Với ứng dụng truy cập vào/ra các khu vực quan trọng, đòi hỏi an ninh cao, hệ thống xác thực đa vai trò sử dụng vân tay được xem như giải pháp hiệu quả, khả thi. Bài viết này đề xuất ứng dụng công nghệ xác thực bảo mật đa vai trò sử dụng vân tay trong quản lý trạm điện, trên cơ sở kế thừa kết quả nghiên cứu khoa học [1].

Từ khóa: Vân tay; Xác thực vân tay; Nhân dạng vân tay; Cơ sở dữ liệu vân tay; Xác thực vân tay đa vai trò; Điều kiện xác thực; So sánh vân tay; Phiên xác thực.

Received date, 15th March, 2021
Revised manuscript, 11th August, 2021
Published, 05th September, 2021

Author affiliations:
[1] Research Institute of Posts and Telecommunications;
[2] University of Transport and Communications.
*Corresponding author: trthchinh@gmail.com.