BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LX No. 3B/2008	97 - 102	Seria Tehnică

Biometric RFID Card - A Solution for Securing Industrial Control

Toader Melinte*, Emil Pricop**

* S.C. SEEKTRON S.R.L., Şos. Vestului nr. 33, Ploieşti
e-mail: office@seektron.ro

** Universitatea Petrol – Gaze din Ploieşti, B-dul Bucureşti nr. 39, Ploieşti

Abstract

Ensuring the security of industrial control systems is a new and important research topic. In this paper we will present an innovative solution for a access control system based on biometric and RFID card identification. The template is stored on a RFID card together with permitted operation codes, identifiers for zones where the access is granted and the expiration date of the card. We will describe how the RFID card and a fingerprint reader could be integrated and used to increase the security of industrial process control systems by adding user access control and precise operator identification.

Key words: *biometrics, fingerprint, RFID card, security*

Introduction

Ensuring the security of industrial control systems is a new and important research topic. The users of modern control systems have to use powerful control access systems for the central rooms, HMI, operator consoles. Also they need to identify in real-time the person who issue a command. For these reasons we propose a biometric RFID card that could be used for person identification applications. That card has 1 KB memory that can store up to 3 fingerprint templates and additional user data such as: authorized operation codes, authorized zones codes, personal information, etc.

Biometrics represents automated methods for person identification based on a physiological or behavioral characteristic. Among the features measured are: facial features, fingerprints, iris and retina features, hand veins, hand geometry, handwritten signature, keystroke dynamics and voiceprint.

Among all biometrics, fingerprint based identification is the oldest, well documented and often used method. Sir Francis Galton proposed the use of fingerprint for identification purposes in the late 19th century. He wrote a detailed study in which he presented a classification system using all ten fingerprints. Automatic fingerprint-based identification systems have been available since 1960s, but only in the last few years these methods have been used on a large scale due to exceptional development in electronics and computer science.

A General Algorithm for Generating Fingerprint Templates

Fingerprints are represented by the pattern of ridges and furrows on the surface of a fingertip. The fingerprints are unique and the patterns remain unchanged throughout life. Fingerprints are so distinct that even the ones of identical twins are different. The prints of each finger of the same person are also different.

Generally speaking a fingerprint analysis algorithm has the following steps:

- loading the fingerprint image for an sensor or from a file;
- enhancing the quality of the image by modifying the contrast and some filtering;
- image binarization;
- final image processing and selection of characteristic points;
- generation of fingerprint template.

Each step of this algorithm contains complex math problems. The execution of this algorithm needs a large number arithmetic and logic operations, so it can be done in a minimum time, frequently less than 1 second, only using specialized and powerful processors. This paper is focused in the operations with the fingerprint template that is generated by any equipments using an algorithm similar to the one described below. For that reason we must do some considerations regarding the fingerprint template seen as a data file.

The images have 8 bit grayscale color depth, so there is needed the binarization operation, that has the role to convert the image from 8 bpp (grayscale) to 1 bpp (black/white). The simplest binarization algorithm is to choose a threshold value and classify all pixels with values above this threshold as white and all other pixels as black. In many situations, finding one threshold compatible to the entire image is very difficult or even impossible. For that reason is used adaptive image binarization, when an optimal threshold is chosen for each image area. This process is very important in fingerprint analysis because it differentiate between ridges and furrows.

Final image processing has the role to filter the noises and to reveal the ridges and the furrows. The false distinct points are eliminated in this point. The algorithms used to detect the false distinct points are described in literature, well-known being [3], [5] and do not make the subject of our paper. Selection of characteristic points could be done using many distinct algorithms. These algorithms are described very well in specialty books and scientific papers [1, 3, 4, 5, and 7].

The last step of the algorithm is generation of fingerprint template. The template’s size depends on the number of distinct points that have been selected and memorized and is between 100 and 480 bytes. For the system described in this paper we used a simple algorithm that implements the steps described before. The size of generated template is 256 bytes, containing a sufficient quantity of information for usage in access control systems and operator identification tasks.

Proposed Biometric RFID Card System Structure

The fingerprint template will be stored in the memory of an RFID card. RFID stands for Radio Frequency Identification and is the ultimate tracking technology for goods, animals or any object that could be marked using an active or passive radio transponder called RFID tag. The tag has two sections: one for radio communication and a memory used for storing data and custom fields. There are mainly two categories of RFID tags: active and passive. The active tags are writeable and readable and have an internal power source (a battery), so the lifetime of an active tag is limited. The passive tags obtain the energy from the magnetic field of the reader. These types of tags are smaller, cheaper and could be used an unlimited time. The functionality of RFID passive tags is very simple: when a tag is in the nearby of a reader, it detects the radio signals generated by the reader and starts to transmit the data stored in the memory. The radio signal generated by the reader offers the power needed to function and the synchronization data for communication between the two entities.

The cards used in this system are passive tags and are working on 13,56 MHz (High Frequency), having the reading distance between 1 and 3 meters. The tag has a write-once read-many memory of about 1 KB, which could be programmed only when the card is issued to the user and could be read by any compatible reader.

The system is based on the analysis of the fingerprint, the encryption of the template and its storage in the memory of the RFID card. When a person wants to use the control system he must place the RFID card in the nearby of the reader, which is mounted in the control console or HMI, then the system reads the data on the card and asks the user to put the finger on the fingerprint sensor. The fingerprint reader scan the finger of the user and then a template is created in real time. After that the generated template is compared with the one stored in the card's memory. If the templates match and the comparison score is better than a threshold value, then the person is identified and has access granted. The cycle of operation takes not more than 5 seconds, which is a good time for authentication in a process control system.

The RFID card could store not only the fingerprint templates, but other information such as permitted or restricted operation codes, zone codes where the user has access, the expiration date of the card. Using this card there can be established a unique system for access control, time & attendance, privilege management and operation tracking.

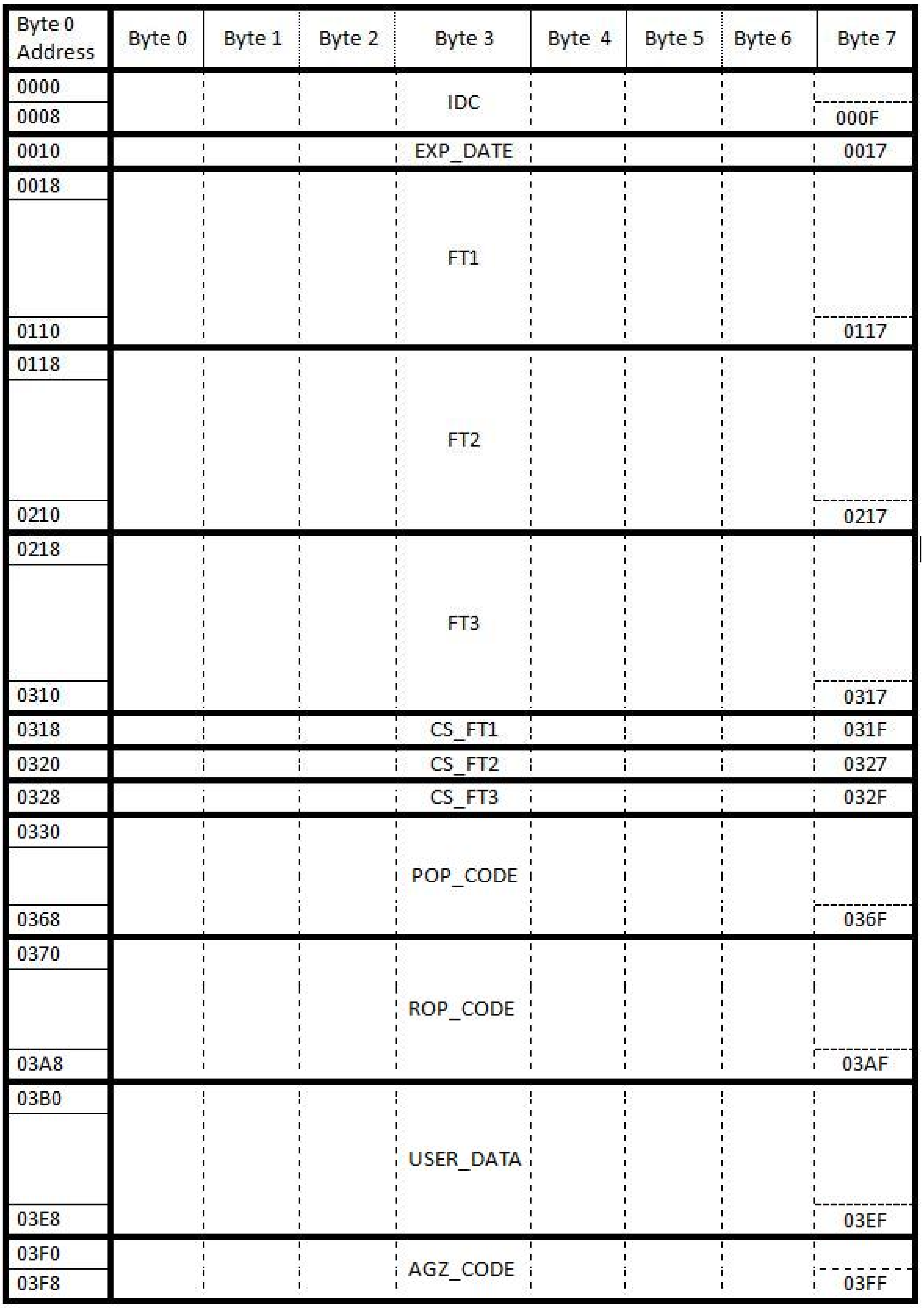
The standard memory of a RFID card is composed by 128 blocks of 8 octets each, totalizing 1 KB of storage space. Each byte is addressable; the address interval is 0000h – 03FFh. For usage in process control systems we defined the following fields in the memory of the RFID card, as seen in Table 1.

Table 1. Field description for the RFID card memory

Start address	Stop address	Offset	Name	Description
0000h	000Fh	16 bytes	CID	Card Identifier
0010h	0017h	8 bytes	EXP_DATA	Card Expiration Date
0018h	0117h	256 bytes	FT1	Fingerprint Template 1
0118h	0217h	256 bytes	FT2	Fingerprint Template 2
0218h	0317h	256 bytes	FT3	Fingerprint Template 3
0318h	031Fh	8 bytes	CS_FT1	Checksum computed for Fingerprint Template 1
0320h	0327h	8 bytes	CS_FT2	Checksum computed for Fingerprint Template 2
0328h	032Fh	8 bytes	CS_FT3	Checksum computed for Fingerprint Template 3
0330h	036Fh	64 bytes	POP_CODE	Permitted operations codes
0370h	03AFh	64 bytes	ROP_CODE	Restricted operations codes
03B0h	03EFh	64 bytes	USER_DATA	User data (Name, Social ID, etc.)
03F0h	03FFh	16 bytes	AGZ_CODE	Access granted zones codes

CID – Card Identifier - is a field of 16 bytes that must be unique at least in each system. The content of this field is automatically generated using a pattern of random numbers.
EXP_DATA - Expiration Date – represent the date when the card become invalid and cannot be used in the system.
In the memory of the RFID card could be stored up to three fingerprint templates, having each a size of 256 bytes. For that reason there are defined three zones: FT1, FT2 and FT3. Each

fingerprint template has a checksum of 8 bytes that is memorized in CS_FT1, CS_FT2 and CS_FT3 fields. Each fingerprint template is encrypted so the fingerprint data is not available in clear text. Even if a card is copied it is not useful because the system require that data on card to match the data read from the fingerprint scanner.



Byte 0 Address	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
0000				IDC				
0008								000F
0010				EXP_DATE				0017
0018				FT1				
0110								0117
0118				FT2				
0210								0217
0218				FT3				
0310								0317
0318				CS_FT1				031F
0320				CS_FT2				0327
0328				CS_FT3				032F
0330				POP_CODE				
0368								036F
0370				ROP_CODE				
03A8								03AF
03B0				USER_DATA				
03E8								03EF
03F0				AGZ_CODE				
03F8								03FF

Fig. 1- RFID Card’s memory map

POP_CODE – Permitted operations codes – is a field of 64 bytes. Each byte signifies a permitted operation code, corresponding to the records in a global privilege database.

ROP_CODE – Restricted operations codes – is a field of 64 bytes. Each byte defines a restricted operation, so we could forbid the access of up to 64 commands.
USER_DATA – User data field – is a zone of 64 bytes of memory where is stored the SSN (Social Security Number), Name, Function of card's user. It could be used along with CID and physical fingerprint to completely identify the user.
AGZ_CODE – Access granted zones codes – is a field of 16 bytes. Each byte is addressable and defines a physical zone where the user has access granted. This field gives another function to the system, the access control in protected areas. It is very important to control who and when has access to the main console or to the control room in a factory, refinery or any other facility.
The memory map is represented in figure 1. We have represented only the bytes, because the whole memory is addressable at byte-level, so the addresses given are in hexadecimal format and are references to bytes no to bits.

The system is not very complicated. It could be implemented with ease in any control console, HMI or control room with adequate software. When a person wants to issue a command, he must place his card in the nearby of the reader, which could be integrated in the console, keyboard, etc. The reader decodes the data in RFID card memory then the user is asked to place the finger on the fingerprint reader which is a component of the console, too. After real-time calculations on the fingerprint image captured by the sensor, the obtained template is compared with the ones stored on the RFID card. If the templates are similar asks the user the command he wants to issue and then the system analyzes the POP_CODE and ROP_CODE fields and identify if the operation that wants to be issued is permitted or restricted. If the operation is permitted it is executed and a log entry, containing date, time, operator name, command and system state, is created to journalize the event. If the operation is forbidden, the system will create only a log entry. Analyzing the log for all the events the system administrator could find out whom and when issued a command to the system and what was the system state before that command.

The RFID card with the memory structure described before is issued using an Enrollment Station. This station includes a fingerprint reader and a RFID card programmer. When the administrator wants to issue a new card the system will ask for the user to read the fingerprint to generate a template that is stored directly in the RFID card memory. Along with the fingerprint templates, auxiliary data, such name, SSN, permitted or restricted operations, is written in the card memory. The main advantage of that system is that the user is not linked to a device mounted in the factory; the whole data needed for authentication is stored in the card. This fact means that we build a unique and universal system for enhancing the security of industrial control process systems.

The software component could be enhanced with components for generating reports for time & attendance statistics. The statistics are generated in real-time so the human resources personnel can view who is at work, who and when entered or left the building.

Conclusions

Biometric techniques seem to be the next step in order to improve the security of a wide range of applications related to identification, verification and recognition of persons, from commercial to law enforcement and criminal investigation. The solution presented here, memorizing fingerprint templates on a RFID card, could bend together the most powerful person identification techniques nowadays. This card is the subject to a pattern in Romania. A biometric system with RFID cards could be implemented with ease and has numerous advantages: rapid and exact operator identification, the possibility of logging all events and all commands issued by any user, establishing a control access system and even a time & attendance system. Having the biometric data on a RFID card represent a step forward, because the number of users for this kind of system is unlimited, and the user is not linked with a device. The proposed system is very secure because the fingerprint template is a data file, not the fingerprint image, and even if the data is accessed it cannot be used to rebuild the original fingerprint image.

References

1. Donahue, M.J, Rokhlin, S.I.- *On the use of level curves in image analysis,* Image Understanding, Vol. 67, p. 652-655, 1992
2. Finkenzeller K., Waddington R. - *RFID Handbook: Fundamentals and applications in contactless Smart Card identification,* 2nd Edition, Wiley, 2003
3. Jain, L.C., Halici, U., Hazashi, I., Tsutsui, S. - *Intelligent biometric techniques in fingerprint and face recognition,* The CRC Press, 1999
4. Lin, H. - *Automatic personal identification using fingerprints,* Ph.D. Thesis, 1998
5. Maio, D., Maltoni, D. - *Direct gray-scale minutiae detection in fingerprints,* IEEE Transactions on Pattern Analysis and Machine Intelligence, p. 27-40, 1997
6. Maltoni, D., Dario, M., Jain, A. - *A Handbook of Fingerprint Recognition,* Springer, 2003
7. Ratha, N., Chen, S., Jain, A. - *Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images,* Pattern Recognition, Vol. 28, p.1657-1672, November 1995

Cardul RFID biometric – o soluție pentru creşterea securității sistemelor de automatizare

Rezumat

Asigurarea securității sistemelor de automatizare a devenit un domeniu de interes pentru lumea ştiințifică, din cauza numeroaselor incidente apărute în astfel de sisteme. Controlul accesului, identificarea precisă a operatorului şi jurnalizarea comenzilor emise sunt doar câteva din problemele ce trebuie rezolvate fără a afecta performanțele sistemului de automatizare. În această lucrare se prezintă un card RFID biometric, cu memoria de 1 KB în care sunt înscrise informații privind utilizatorul şi şabloanele a 3 amprente digitale, utilizate pentru identificarea precisă şi sigură a posesorului cardului.