AN ENHANCED SECURITY FOR GOVERNMENT BASE ON MULTIFACTOR BIOMETRIC AUTHENTICATION

Tran Cong Hung[1], Nguyen Thanh Tri[1,2] and Ho Nhut Minh[3]

[1]Post & Telecommunications Institute of Technology, Vietnam
[2] Binh Duong Department of Information and Communications, Vietnam
[3] Saigon University, Vietnam

ABSTRACT

This paper is demonstrating to create a system of multifactor authentication based on biometric verification. Our system use iris for the first factor and fingerprint for the second factor. Once an attacker attempts to attack the system, there must have two factors. If one of them is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Furthermore, this system will be implemented to enhance security for accessing control login government system.

KEYWORDS

Multifactor authentication (MFA), biometric, iris recognition, fingerprint recognition

1. INTRODUCTION

1.1. Authentication

Authentication is a method by which a system verifies and validates the identity of a user of the system who wishes to access it. Authentication [1] ensures and confirms a user's identity through a code such as a password and verifies genuineness of a document or signature, to make it effective or valid. It is the measure employed to ensure that the entity requesting access to a system is what or who it claims to be, and to counter any inappropriate or unauthorized access.
Authorization is the method of giving individuals access to system objects like information, application programs etc. based on their identity.

1.1.1. Password and PIN based authentication

Using password (a secret word or string of characters that is used for user authentication) or Personal Identification Number (PIN which is a secret numeric password and is typically used in ATMs) to login is the most common knowledge-based authentication method. It is mandatory for the user to provide knowledge of a secret in order to authenticate the process [2] [3].

DOI: 10.5121/ijcnc.2016.8605

1.1.2. SMS based authentication

SMS is used as a delivery channel for a one-time password (OTP) generated by an information system. There are two types of one-time passwords, a challenge-response password which responds with a challenge value after receiving a user identifier and a password list which makes use of lists of passwords which are sequentially used by the person wanting to access a system. User receives a password through the message in the cell phone, and enters the password to complete the authentication. This SMS-based authentication method is used in the login process of Internet banking system to authenticate the process [2] [3].

1.1.3. Symmetric-key authentication

In symmetric key authentication, user shares a secret, unique key with an authentication server. The user may be asked to send a randomly generated message (the challenge) encrypted by the secret key to the authentication server. If the server can found the match for received encrypted message (the response) using its shared secret key, the user is authenticated and server authorizes user's access to the system [2] [3].

1.1.4. Public-key authentication

In Public-key cryptography a pair of private key and public key is used. A private key is kept secretly by the user, while the corresponding public key is commonly embedded in a certificate digitally signed by a certification authority. The certificate is made available to others for sharing the public key among different users. The private key is used to encrypt the messages send between the communicating machines and both encryption and verification of signature is accomplished with the public key [2] [3].

1.1.5. Biometric authentication

Biometrics is a method by which a person's authentication information is generated by digitizing measurements (encoded value) of a physiological or behavioural characteristic. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware device. The device scans the physical characteristic, extracts critical information, and then stores the result. Biometric authentication verifies user's claimed identity by comparing an encoded value with a stored value of the concerned biometric characteristic [2] [3].

1.1.6. Digital Signatures

A digital signature is a digest calculated from a signed document (typically a one-way hash function) which is then signed (encrypted with private key). The client verifies the digest signature by decrypting it with the server's public key and compares it to the digest value calculated from the message received. The signature can also be used by the server to verify data the client is sending. Digital signature is used to assure that the downloaded data is genuine and not malicious or invalid information [2] [3].

1.2. Multi-factor Authentication

Multi-factor authentication (MFA) is an approach to authentication which requires the production of two or more of the three following independent authentication factors:

- Knowledge factor
- Possession factor
- Inherence factor

After submission, each factor must be validated by the other party for authentication to occur. Multifactor authentication (MFA) [1] is a security system that requires more than one form of authentication to validate the authenticity of a transaction. Multifactor authentication requires two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification).

Previously, MFA systems typically based upon two-factor authentication. Because customers are more and more using mobile devices for banking and shopping, however, physical and logical security concerns have converged. This, in turn, has formed more interest in three-factor authentication.

1.2.1. Knowledge factor ("something only the user knows")

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate like password (a secret word or string of characters that is used for user authentication), PIN (A personal identification number (PIN) is a secret numeric password and is typically used in ATMs) and Pattern (Pattern is a regular or stochastic sequence or array of sets of information as e.g. in a single dimensional barcode or in a two dimensional matrix code or in a finger print like set in any n-dimensional stack in any physical representation).

1.2.2. Possession factor *("something only the user has")*

Possession factors have been commonly used for authentication from many years, in the form of a key to a lock. The basic principle is that the key holds a secret which is common between the lock and the key, and the similar principle is used for possession factor authentication in computer systems. A number of types of pocket-sized authentication token are available which display a changing passcode on an LCD or e-ink display, which must be typed in at an authentication screen, thus avoiding the need for an electronic connection. This can be done one in the forms such as sequence-based token, time-based token, and the token may have a small keypad on which a challenge can be entered. The challenge can take one of following tokens:

- Connected tokens: The connected type tokens are available in the form of Magnetic stripe cards, Smartcards, Wireless RFID-based tokens, USB tokens and Audio Port tokens.
- Soft tokens (computer-simulated software-based tokens): The functionality of any disconnected token can be emulated as a soft token on a PC or Smartphone using deployed software, where that device itself becomes the possession factor.
- One-time pads: A one-time pad is a password used only once. Schemes based on a one time pad have been described but are rarely deployed due to the need to supply a new password or pad for each authentication.
- Mobile phones: A new category of TFA tools transforms the PC user's mobile phone into a token device using SMS messaging, an interactive telephone call, or via downloadable application to a Smartphone.
- SMS one time password: SMS one time password uses information sent to the user in an SMS as part of the login process.

1.2.3. Inherence factor *("something only the user is")*

Biometric authentication satisfies the regulatory definition of true multi-factor authentication. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to open the credential vault. For many biometric identifiers, the actual biometric information is rendered into string or mathematic information. The device scans the physical characteristic, extracts critical information, and then stores the result as a string of data. Comparison is therefore made between two data strings, and if there is sufficient commonality a pass is achieved.

This paper is organized as follows: section 1 Introduction, section 2 present Biometric Authentication, section 3 Biometric Modalities, section 4 Proposal System and hardware design and section 5 is Conclusions.

2. BIOMETRIC AUTHENTICATION

Biometric technologies are defined as, “automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic”. The term automated methods refers to three basic methods in concern with biometric devices: A mechanism to scan and capture a digital or analog image of a living personal characteristic; Compression, processing and comparison of the image to a database of stored images; and Interface with applications systems. [1]

2.1. Advantages of Biometrics

Biometric traits cannot be lost or forgotten.
Biometric traits are difficult to copy, share and distribute.
They require the person being authenticated to be present at the time and point of authentication.

2.2. Biometric Features

Uniqueness: An identical trait won’t appear in two people.
Universality: Occur in as many people as possible.
Performance: Don’t change over time.
Measurability: Measurable with simple technical instruments.
User friendliness: Are easy and comfortable to measure. [4] [5] [6] [7]

2.3. Physiological vs. Behavioral

When referring to a biometric technology, it is important to distinguish between physiological and behavioral human characteristic.

A physiological characteristic is relatively a stable human physical characteristic, such as a fingerprint, iris pattern, or blood vessel pattern on the back of the eye. This type of measurement is unchanging and unalterable without significant duress. Alternatively, a behavioral characteristic is a reflection of an individual’s psychological makeup, although physical traits, such as size and gender, have a major influence. Some of the examples of behavioral traits used to identify individuals include: Keystroke dynamics, and speech identification and/or verification.

Today, we have the technology and processing power to employ advanced, cost-effective, and much more accurate biometric identification systems. There are two different ways to resolve a person‟s identity: verification and identification. Verification (am I whom I claim to be?) involves confirming or denying a person's claimed identity. In identification, one has to establish a person‟s identity (who am I?). Each approach has its own complexities and could probably be solved best by a specific biometric system, including the following [4] [5]:

2.3.1. Physical Biometrics

Fingerprint: Analyzing fingertip patterns.
Facial recognition/face location: Measuring facialcharacteristics.
Hand geometry: Measuring the shape of the hand.
Iris scan: Analyzing features of colored ring of the eye.
Retinal scan: Analyzing blood vessels in the eye.
Vascular patterns: Analyzing vein patterns.
DNA: Analyzing genetic makeup. [4] [5] [6] [7]

2.3.2. Behavioral Biometrics

Speaker/voice recognition: Analyzing vocal behavior
Signature/handwriting: Analyzing signature dynamics
Keystroke/patterning: Measuring the time spacing of typed words. [4] [5] [6] [7]

3. BIOMETRIC MODALITIES

3.1. Fingerprint Recognition

A fingerprint is made up of ridges and furrows. Uniqueness is determined by ridges, furrows, the minutiae points. Fingerprint is one of oldest and most popular recognition technique. Every individual possesses unique finger patterns, even twins has different patterns of rings and furrows. Fingerprint matching techniques are of three types [8] [9]:

- Minutiae-based techniques: In these minutiae points are finding and then mapped to their relative position on finger. There are some difficulties like if image is of low quality it is difficult to find minutiae points correctly also it considers local position of ridges and furrows not global [8].
- Correlation- based method: It uses richer gray scale information. It overcome problems of above method, it can work with bad quality data. But it has some of its own problems like localization of points.
- Pattern based (image based) matching: Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a stored template and a candidate fingerprint.

Advantages:

- It is the most developed method till now.
- Relatively inexpensive.
- Even twins have unique fingerprint patterns so highly secure.
- Small template size so matching is also fast.

Problems:

- Systems can be cheated by having artificial finger like finger made up of wax.
- Cuts, scars can produce obstacle for recognition.

Applications:

- Verification of driver-license authenticity and license validity check.
- Law Enforcement Forensics.
- Border Control/Visa Issuance.

3.2. Face Recognition

Face recognition is based on both the shape and location of the eyes, eyebrows, nose, lips and chin. It is non intrusive method and very popular also. Facial recognition is carried out in two ways [10] [11]:

- Facial metric: In this location and shape of facial attributes (e.g. distances between pupils or from nose to lip or chin) are measured.
- Eigen faces: Analyzing the overall face image as “a weighted combination of a number of canonical faces”.

Another emerging technique is to use face recognition combining with other visual details of skin. This technique is called as skin texture analysis. The unique lines, patterns, and spots apparent in a person„s skin is located. According to tests with this addition, performance in recognizing faces can increase 20 to 25 percent.

Advantages:

- Totally non intrusive.
- Easy to store templates.
- Socially accepted.

Problems:

- Facial traits vary over time.
- Uniqueness is not maintained ex. in case of twins.
- Not proper recognition if person has different expressions like slight smiling can affect recognition.
- Highly dependent on lightning.

Applications:

- General identity verification.
- Surveillance.
- Access Control.

3.3. Iris recognition

The iris is the elastic, pigmented, connective tissue that controls the pupil. The iris is formed in early life in a process called morphogenesis. Once fully formed, the texture is stable throughout life. It is the most correct biometric recognition system so it is called as king of biometrics. The iris of the eye has a unique pattern, from eye to eye and person to person. Eye color is the color of iris. Iris recognition uses camera technology with subtle infrared illumination to acquire images of the detail-rich, intricate structures of the iris. [12] [13] [14] [15]

Advantages:

- Highly accurate.1 chances in 1078 that iris pattern of two individual matches.
- Highly scalable as iris structure remains same throughout lifetime.
- Small template size so fast matching.

Problems:

- Iris scanners are relatively expensive.
- Scanners can be fooled by high quality image.
- Require cooperation from user.

Applications:

- All of the UAE's land, air and sea ports of entry are equipped with systems.
- Google uses iris scanners to control access to their datacenters.

3.4. Retina Scan

The blood vessels at the back of the eye have a unique pattern, from eye to eye and person to person. A light source is needed because retina is not visible. The infrared energy is absorbed faster by blood vessels in the retina than by the surrounding tissue. Based on this pattern of blood vessels can be easily recognized. It is required that a person remove its glasses, focus on a specific point for about 10-15 seconds. A coupler is used to read the blood vessel patterns. A coherent light source is also required for illumination. [16] [17] [18]

Advantages:

- Retinal scan cannot be forged.
- Error rate is 1 out of 10,000,000 (almost 0%).
- Highly reliable.

Problems:

- Reveals some medical conditions (e.g. hypertension), which causes privacy issues.
- It is intrusive so not user friendly.
- Measurement accuracy can be affected by a disease such as cataracts.

Applications:

- Utilized by several government agencies including the FBI, CIA, and NASA.
- Used for medical diagnostic applications.

4. PROPOSAL SYSTEM AND HARDWARE DESIGN

Base on the analyst in section 3, we decided using fingerprint and iris recognition for multifactor authentication system. We used iris recognition for identifying and fingerprint recognition for verifying.

4.1. Flow Charts Of System

4.1.1. Enroll Flow Charts

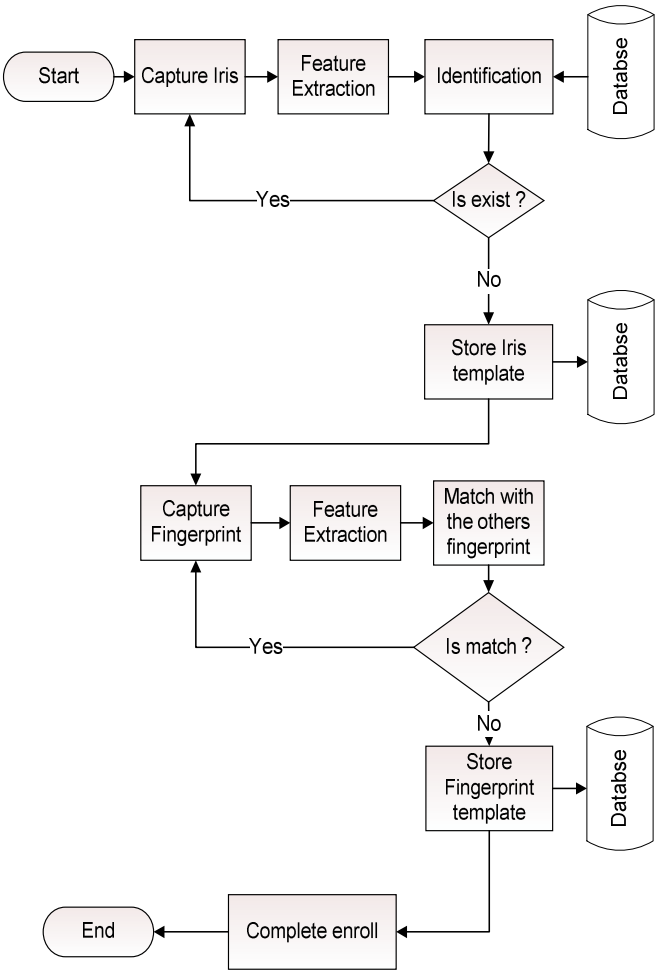

Figure 1. The enrolling flow charts

4.1.2. Authentication Flow Charts

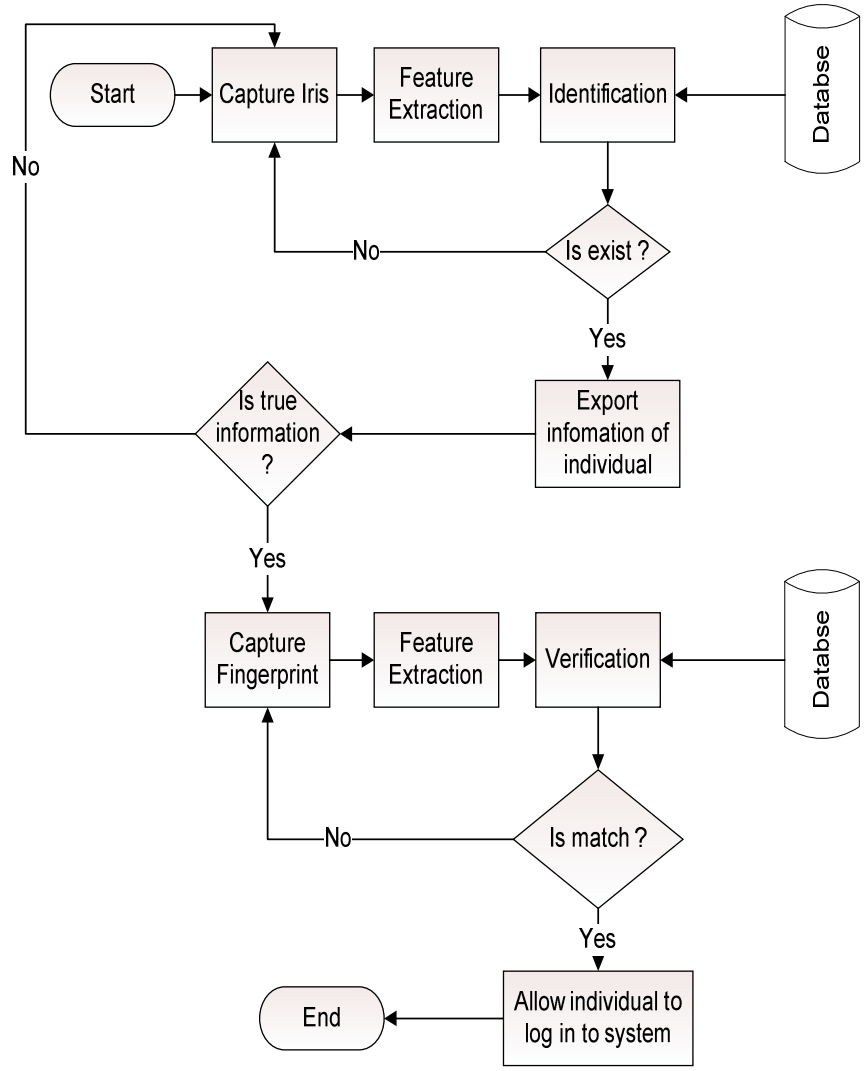

Figure 2. The authentication flow charts

4.2. Hardward Design

The proposed system includes: Iris Sensor and fingerprint sensor. These sensors connect with client computers by COM and USB port, which connect with servers base on LAN network as figure 3. If clients want to use applications at server, they must capture their iris and fingerprint and to send them to servers, servers will implement identification (Iris recognition) and verification (Fingerprint recognition).

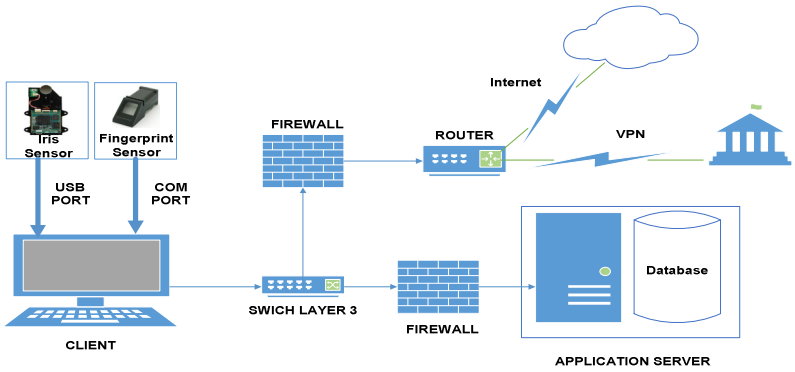

Figure 3. Architecture of multifactor authentication in Binh Duong Department of Information and Communications

4.2.1. Iris Sensor

We used IriShield-USB MO 2121 EVM from Iritech Inc [19]. It shows features as follows:

- Capture Distance: (Optimal distance = 5 cm (2 inches), Focal depth = 6 mm (0.2 inch).
- Image Format: ISO Standard 19794-6 (2005 & 2011), (640 x 480 Pixels, 8 bit Grayscale), full support of K1, K2, K3, K7.
- Power: Single USB Bus Powered (DC +5V±5%) (Max power consumption=250mA).
- Illumination: Near infrared LED.
- Connectivity: USB 2.0 (IriShield™ - USB Series), UART/ RS-232 (IriShield™ -UART Series).
- Security: RSA (2048-bit) and AES (256-bit); X509 Certificate, PFX/PKCS#12 Certificate, RSA key pair generated on-board.

4.2.2. Fingerprint Sensor

We used FPM-10 from Adafruit [20]. It shows features as follows:

- Supply voltage: 3.6 - 6.0VDC.
- Operating current: 120mA max.
- Peak current: 150mA max.
- Fingerprint imaging time: <1.0 seconds.
- Window area: 14mm x 18mm.
- Signature file: 256 bytes.
- Template file: 512 bytes.
- Storage capacity: 162 templates.
- Safety ratings (1-5 low to high safety).
- Interface: TTL Serial.

- Baud rate: 9600, 19200, 28800, 38400, 57600 (default is 57600).

Figure 4. The iris and fingerprint sensor

4.3. Software

We designed and analysed the software by C# and SQL Server 2008, design of the interface is as follows:

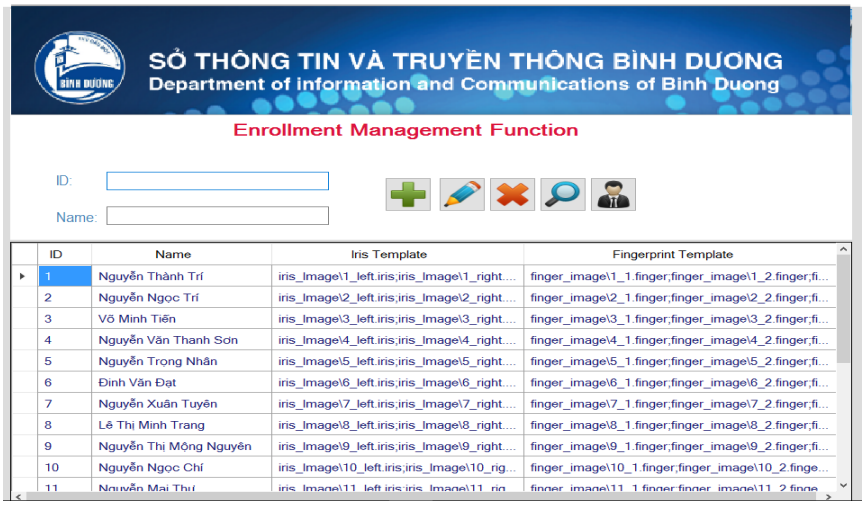

Figure 5. Interface of enroll function

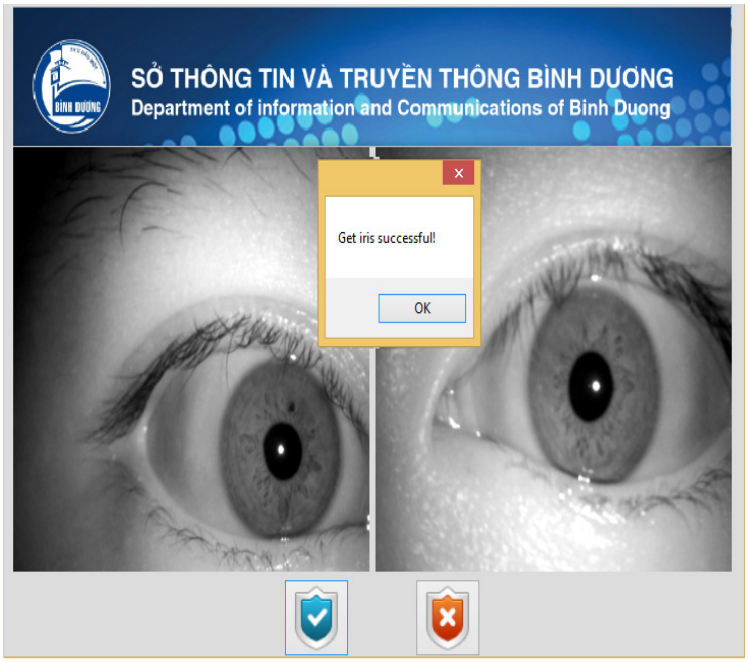

Figure 6. Result of getting iris image successful for enroll function

Figure 7. Result of getting finger image successful for enroll function

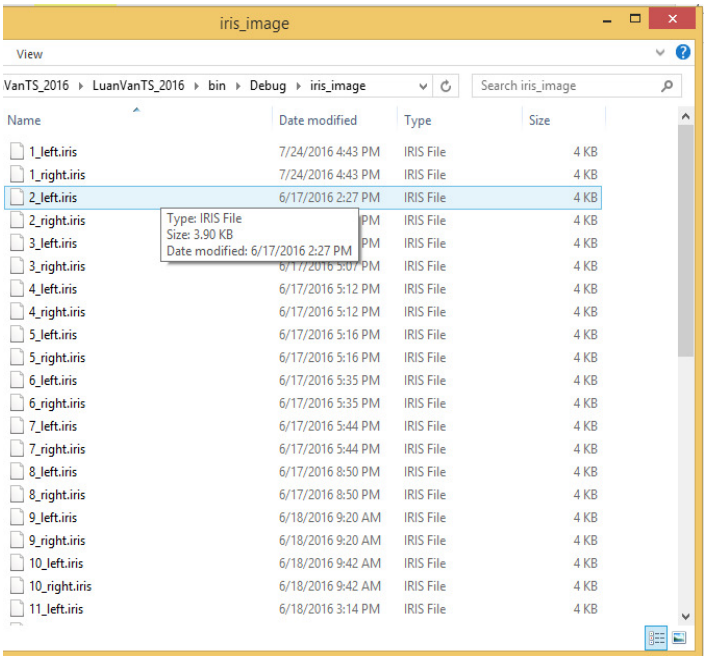

Figure 8. Iris templates is stored on disk drive

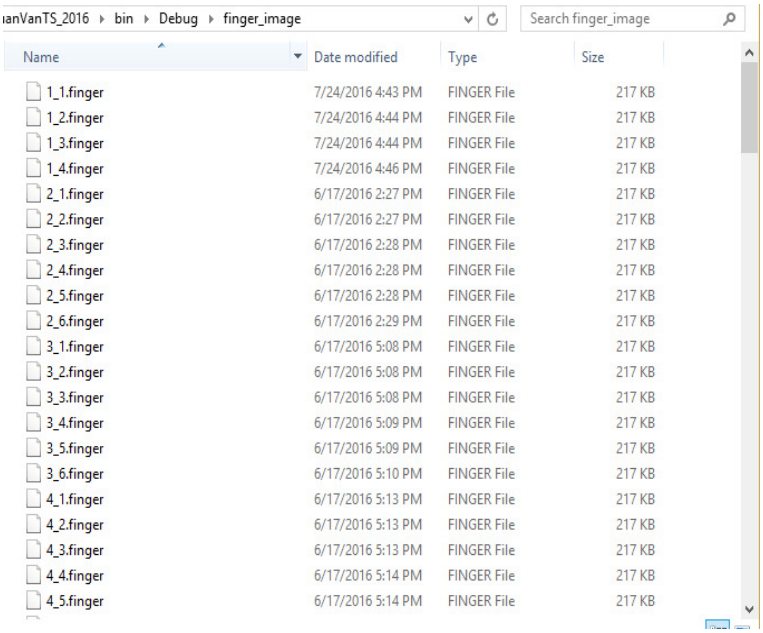

Figure 9. Finger templates is stored on disk drive

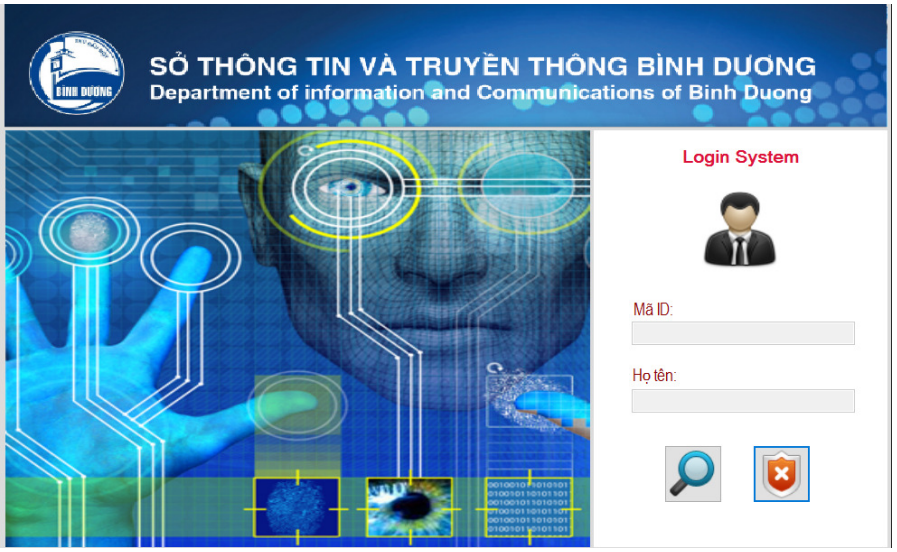

Figure 10. Interface of login function

Figure 11. Result of successful identification with iris recognition and export information of user

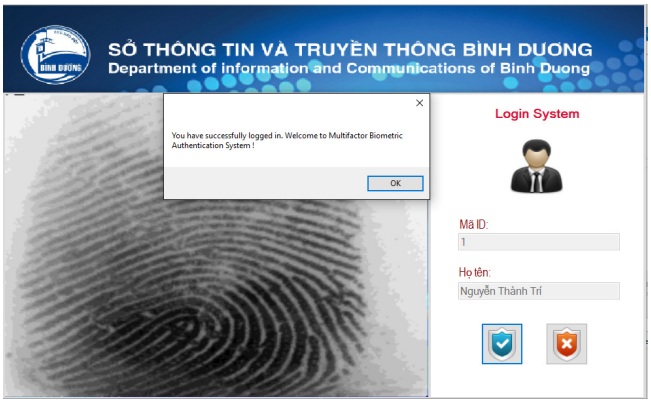

Figure 12. Result of successful verification with fingerprint recognition and allow user to access system

Figure 13. User log in to document management software successful

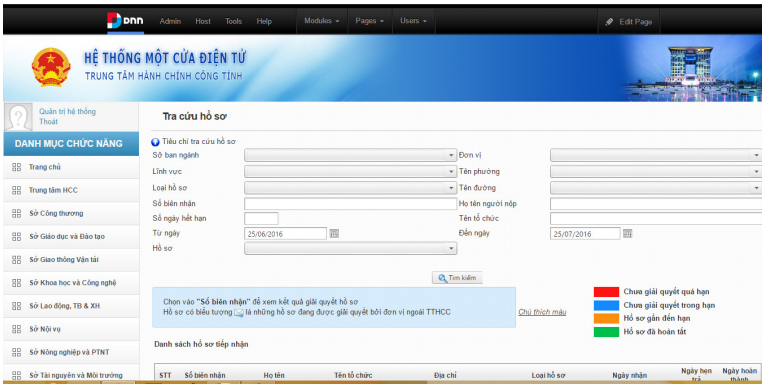

Figure 13. User log in to public service of goverment management successful

4.4. Simulation and Discussion

4.4.1. Database of Simulation

The proposed system was tested using the iris and fingerprint database as shown in Table 1. The database consists of 600 iris and fingerprint image of 50 different individuals. Out of the collected data 600 samples from both iris and fingerprint are used for training the system and rest 360 are used for testing. The system is also tested with 360 samples of unregistered data.

Table 1: Details of number of users

Type of users	Number of templates	
	Training	Testing
Registered	50 (Persons) × 2 (Irises) × 6 (Fingerprints) = 600	30 (Persons) × 2 (Irises) × 6 (Fingerprints) = 360
Unregistered		30 (Persons) × 2 (Irises) × 6 (Fingerprints) = 360
Total	600	720

4.4.2. Result and Discussion

Table 2. Results of accuracy

	Iris	Fingerprint	Iris + Fingerprint
FRR	2.78%	4.17%	1.67%
FAR	1.12%	1.12%	0.00%
Average Error Rate	1.95%	2.65%	0.84%
Accuracy	98.05%	97.36%	99.16%

The two common error rates are False accept rate (FAR) and False Reject Rate (FRR). FAR is defined as "the probability of an impostor being accepted as a genuine individual. That is, in a biometric authentication system, the FAR is computed as the rate of number of people falsely accepted over the total number of enrolled people for a predefined threshold. FRR is defined as "the probability of a genuine individual being rejected as an impostor" [9]. That is, in a biometric authentication system, the FRR is computed as the rate of number of people falsely rejected (genuine people are rejected) over the total number of enrolled people for a predefined threshold. FAR and FRR can be changed by a significant amount depending on the threshold used in the system. If a lower threshold is used in a similarity based biometric matching system, then the FAR will be higher and the FRR will be lower and vice versa. The performance of a biometric system may also be expressed using average error rate which is average of FAR and FRR. A lower average error rate value thus indicates better performance.

Results as shown at table 1, accuracy of our system (99,16 percent) is better performane than iris or fingerprint authentication system in turn are 97.36 and 97.36 percent.
Time of indentification (Iris recognition) is less equal one second and verification (Fingerprint recogniton) user is less equal three seconds.

5. CONCLUSIONS

In this paper, we studied mutltifactor authentication, biometric authentication and comparation of biometric authentication. Base on those biometric authentications, we built a multifactor authentication system using iris and fingerprint biometric. Simulation of our multifactor authentication system is relatively high accurate, therefore it can be used as a control access system, high safety login information systems,etc. In future studies, we are going to continue experience on large database, detection of fake iris and fingerprint, improving processing time of capturing and matching iris and fingerprint template.

REFERENCES

[1] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus (August 2013), "Electronic Authentication Guideline", NIST Special Publication 800-63-2.

[2] Prachi Soni, Monali Sahoo (January 2015), "Multi-factor Authentication Security Framework in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5 Issue .

[3] Deepa Panse, P. Haritha (August 2014), "Multi-factor Authentication in Cloud Computing for Data Storage Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4 Issue 8.

[4] Palvi Sharma, Manit kapoor, NaveenDhillon (January 2016), "A Survey paper on Various Techniques for Biometric Authentication System" International Scientific Research Organization Journal, Volume 01 Issue 01.

[5] Gursimarpreet Kaur, Dr.Chander Kant Verma (April 2014), "Comparative Analysis of Biometric Modalities" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4.

[6] Selva Priya G, Anitha P, Vinothini C (2014), "An Introduction to Biometrics: The Power of Security".

[7] P Tripathi (2011), "A Comparative Study of Biometric Technologies with Reference to Human Interface" International Journal of Computer Applications (IJCA), vol. 14, no.5.

[8] Jain, A. K.; Ross, A. & Pankanti, S. (2006), "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics And Security, vol. 1, no. 2, pp 125 – 144.

[9] Mouad .M.H.Ali, Vivek H. Mahale, Pravin Yannawar và A. T. Gaikwad (2016), "Overview of Fingerprint Recognition System" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT).

[10] S. Z. Li and A. K. Jain, Eds (2004), Handbook of Face Recognition. New York: Springer Verlag.

[11] Sandeep Mishra, Anupam Dubey (January 2015), "Face recognition approaches: A survey", International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 6 Issue 1.

[12] John Daugman (2004), "How Iris Recogniton Works", IEEE Transactions On Circuits and System for Video Technokogy, Vol 14, No 1, pp 21-31.

[13] Sanjay R. Ganorkar, Ashok A. Ghatol (2007), "Iris Recognition: An Emerging Biometric Technology", In Proc. of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, , pp.91 – 96.

[14] Manisha, Gurdeep Kaur and Parminder Singh (2014), "Iris Recognition Techniques: A Review", International Journal of Information & Computation Technology ISSN 0974-2239, Volume 4, Number 17

[15] Manisha More, Vishakha Nagrale, Vanita Tonge (2015), "A Survey on Iris Recognition Techniques" International Journal of Novel Research in Computer Science and Software Engineering, Vol. 2, Issue 1, pp: (89-94).

[16] C. Marino, M. G. Penedo,M. Penas, M. J. Carreira, F. Gonzalez (May 2006), "Personal authentication using digital retinal images", Journal of Pattern Analysis and Application, Springer, Volume 9, Issue 1, pp. 21–33.
[17] Ms. Shivani Shikarwar, Ms. Devanshi Rathod, Mrs. Hiteshi Diwanji (April 2014), "Review paper on retina authentication and its security issues", International Journal For Technological Research In Engineering Volume 1, Issue 8.
[18] Md. Amran Siddiqui, S. M. Hasan Sazzad Iqbal, Md. Rounok Salehin (November 2011), "Personal Authentication through Retinal Blood Vessels Intersection Points Matching" , International Journal of Computer Applications (0975 – 8887) Volume 33– No.9.
[19] https://www.adafruit.com/products/751.
[20] http://www.iritech.com/products/hardware/irishield%E2%84%A2-series.

Authors

Tran Cong Hung was born in Vietnam in 1961. He received the B.E in electronic and Telecommunication engineering with first class honors from HOCHIMINH University of technology in Vietnam, 1987. He received the B.E in informatics and computer engineering from HOCHIMINH University of technology in Vietnam, 1995. He received the master of engineering degree in telecommunications engineering course from postgraduate department Hanoi University of technology in Vietnam, 1998. He received Ph.D at Hanoi University of technology in Vietnam, 2004. His main research areas are B – ISDN performance parameters and measuring methods, QoS in high speed networks, MPLS. He is, currently, Associate Professor PhD. of Faculty of Information Technology II, Posts and Telecoms Institute of Technology in HOCHIMINH, Vietnam.

Nguyen Thanh Tri was born in Vietnam in 1990. He received the B.E in informatics and computer engineering from Posts and Telecoms Institute of Technology in HOCHIMINH, Vietnam, 2013. He is currently a MSc. Candidate in Information System from Post & Telecommunications Institute of Technology, Vietnam in 2016. He is working in Binh Duong Department of Information and Communications, Vietnam.

Ho Nhut Minh was born in Vietnam in 1987. He received the B.E in Electronics and Telecommunication engineering from Ho Chi Minh City University of Technology and Education, Vietnam, 2010. He received the M.E degree in Telecommunications Engineering from Post and Telecommunication Institute of Technology in Ho Chi Minh, Vietnam, 2014. He is working as lecturer in Faculty of Electronics - Telecommunication, Saigon University, Vietnam.