Journal of Advances in Computer Research
Quarterly pISSN: 2345-606x eISSN: 2345-6078
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 9, No. 4, November 2018), Pages: 1-17
www.jacr.iausari.ac.ir

Biometric Authentication of Fingerprint for Banking Users, Using Stream Cipher Algorithm

Ali AliBabaee[✉1], Ali Broumandnia[2]
1) Department of Computer Engineering, E-Campus, Islamic Azad University, Tehran, Iran
2) Department of Computer Engineering, South Tehran Branch, Islamic Azad University, Iran
a.babaee@iausr.ac.ir; broumandnia@gmail.com

Received: 2018/02/14; Accepted: 2018/03/31

Abstract

Providing banking services, especially online banking and electronic payment systems, has always been associated with high concerns about security risks. Counterfeiting and theft, identity theft, and even, in some cases, the deception of employees of financial institutions and banks, are among offences and atrocities swindlers may conduct. As it is very difficult to identify people with changes in appearance or fake identity documents, a solution has to be considered to resolve the problem. User authentication is usually done based on two or more factors. However, the development of various mail wares and social engineering attacks, undermine user trust, so users' authentication will be highly vulnerable. In this paper, customer authentication for their transactions in electronic banking has been discussed, and a more appropriate way of using biometric fingerprint data, as well as encrypting those data in a different way, has been suggested. Using fingerprint biometrics increases the security of online payment systems. Biometrics is used in a database in the banking system. The fingerprint biometrics is more reliable and easier to use than other biometrics and can be obtained from anyone with an easy access. In this thesis, according to needs analysis, validation is performed not only by the user (or personal machine) but also by the bank itself, according to the standards of the banking system. More precisely, a new protocol, known as Stream Cipher, is developed to generate a one-time password from biometric data, to ensure that security and privacy are maintained. In the suggested system, Ciphering and deciphering user information by issuer bank provides security. First, the user sends his fingerprint to the online store and using the Minimum Mapping method and Minutiae sends the image extracted by Stream Encryption Protocol compared to the database, and in case verified, the acquirer bank sends verification to the store and the money is transferred. The results of the research indicate its proper function compared to other authentication methods (non-biometric). The protocol security analysis also demonstrates the benefits of enhancing security by employing the accelerated encryption methods in the proposed method. The results of the research show The Errors rate (EER, FRR and SFAR) is very low and can be ignored. This method is highly resistant to all kinds of electronic banking attacks, such as phishing and password theft.

Keywords: *Electronic Payment, Biometric fingerprint, Stream Cipher, Online Banking Security, Authentication*

1. Introduction

Since several years ago, people have been using multiple payment systems such as E-Wallets, credit cards, mobile payment systems, etc. for their transactions. Developing tools such as social networks, the increase in Internet users, and the numerous types of devices has multiplied their vulnerability. Abuse and fraud in e-commerce systems, is now becoming a big challenge. These risks [1] will reduce customers and lead into the Banks' loss [2] [40] [30].

In order to control the access in different banking fields, biometrics can be used as a secure password. The fingerprint biometric is more practical and very affordable, because it can be easily installed and used in any environment. It is also very easy to manage and use by any vendor. In fact, fingerprint-based systems are very user friendly [18] [19].

On the other hand, biometric data contains sensitive and important information and can always be attacked and abused; since this data is often exchanged in the same format through the networks, this framework needs special protection and security. The best secure option is encrypting these data in exchange environments. In this paper, alongside with customer authentication for the transactions in online banking, a suitable solution is proposed by using biometric fingerprint data and their encryption in a different method [20] [21].

Results confirmed the conclusion reported in previous works [35] [36] [40], based on simulated spoofing attacks is not always representative. findings may be exploited both to help system designers and researchers to better evaluate the without the need of actually fabricating spoofed traits. Performance drop of systems under spoofing attacks.

Another consequence is that score rules explicitly designed to deal with spoofing attacks, can be even weaker than standard fusion rules, In particular, based on experimental evidences like the ones obtained in this work, more realistic hypothesis on the distribution of the fake traits can be derived, instead of the worst case assumption [37] [38].

We will begin with biometric authentication method, and then we will try to provide a more accurate system by using a new security protocol for bank payments.

2. Biometric Authentication Methods

With the increasing application of authentication in today's world, the importance of authentication methods has also increased. For years, human identity authentication has been considered vital and various methods have been presented, such as ***ID*** cards, passport and so on, which are not very reliable due to forging, loss and other problems. Today, biometric authentication is used to eliminate the defects of old methods. Biometrics, means automatic detection of individuals based on their specific behavioral and biological characteristics such as face, fingerprint, iris, voice, etc., which are not easily forged and therefore, are more efficient and can replace traditional authentication methods and increase security, reduce violations and accelerate daily applications. In general, biometrics are known as the safest passwords. Biometric tools are trying to identify individuals by capturing and storing data and converting them into an appropriate algorithm, Biometric systems have many uses [23] [51] [10] [44].

2.1 Biometric Features

Human biometric features are usually evaluated by the following parameters:

- ✓ ***Universality***: Each individual possesses the feature.
- ✓ ***Uniqueness***: The number of different samples that can be distinguished.
- ✓ ***Permanence***: A measure for the longevity of a feature (over time).
- ✓ ***Collectability***: Ease of use for evaluating different samples.
- ✓ ***Performance***: Accuracy, speed and sustainability of the method.
- ✓ ***Acceptability***: The level of technology acceptance.
- ✓ ***Circumvention***: Ease of alternative use.
- ✓ ***Identity Authentication***: Sending an individual's feature to database, for examining it in order to authenticate the individual; the system's response is necessarily positive or negative.
- ✓ ***Identification***: Extracting individual's biometric feature and searching the database, if there is any.
- ✓ ***Distinctive***: There should not be any two same individuals.

2.2 Logical Parts of a Biometric System

The biometric system is logically divided into two parts:

1. Enrollment: Collecting the individual's biometric feature and saving it in the system. In this phase, the feature is being read and located as separate patterns in the database, after the extraction.

2. Identification: The task of this part is to identify and authenticate individuals when entering or accessing the system. In this phase, after reading the biometric feature, the method extracts the feature and compares it with the patterns inside the database, and finally grants or denies the access to the system.

2.3 Biometric Methods Classification

The main biometric methods used to identify individuals, are classified into three main categories:

- ✓ **Chemical Biometrics**: ***DNA***[1], blood sugar, body scent, blood pattern, etc.
- ✓ **Behavioral Biometrics**: walking, pressing the keys (typing rhythm), voice, signature, etc.
- ✓ **Physical Biometrics**: fingerprint, iris pattern, thermal or physical pattern of the face, retina veins pattern, hand geometry, palm pattern, ears, nose, lips movement, eyes movements, nails, etc.

Here, we describe the fingerprint biometrics in particular:

2.3.1 Fingerprint

The lines of the finger tips are called Friction Ridges. The fingerprints of individuals contain patterns that are unaltered during the life of the individual, unless they are severely burned. This has made fingerprint-based identification, one of the most common biometrics [17] .

[1] ***D****eoxy* ***R****ibonucleic* ***A****cid*

2.3.2 Reasons of universality and advantages of fingerprint identification

The most important reasons for the universality of fingerprint identification includes:

- ✓ The success of this method in various applications (judicial, governmental, commercial, etc.), which nowadays is even used in cell phones.
- ✓ The criminals' fingerprints are left behind in the crime scene.
- ✓ The existence of a complete database of fingerprints (so far, more than 70million different fingerprints are available in ***FBI***[1] database, by 2000).
- ✓ The existence of cheap and small fingerprint capturing devices.
- ✓ Each individual has a unique fingerprint.
- ✓ Fingerprint is resistant to aging.
- ✓ Its technology has reached the maturity.
- ✓ Very comfortable to use.
- ✓ Low ***EER***[2]
- ✓ Affordability
- ✓ Popularity

2.3.3 Obtaining a fingerprint image

Based on the type of fingerprint capturing, the devices are divided into two types: live scan and offline scan. In offline models (paper and ink), fingerprints are obtained by dipping fingers into the ink and pressing them on paper and taking photos or scanning the paper. Due to poor quality of the images and of course, technological advancements, this method is gradually reaching to extinction.

The live scan ***CCD***[3] method, operates by digitizing the fingerprint that touches the sensors. In all techniques, the finger surface is in contact with a specific part of the device and the image is taken.

2.3.4 Fingerprint Scanners

Digital Scanners are categorized based on Resolution, Pixel, Sensor Area, Precision, etc. Live Digital Scanners are divided into five categories:

Optical, Capacitive (Semi Conductor), Thermal, Pressure Based, and Ultrasound. Sweep Sensors are widely used in laptops, smart phones, tablets and other commercial devices, due to their small size and low prices. These scanners perform by sweeping the finger on their surfaces. Capacitive scanners are the most cost effective scanners and are used in most notebooks.

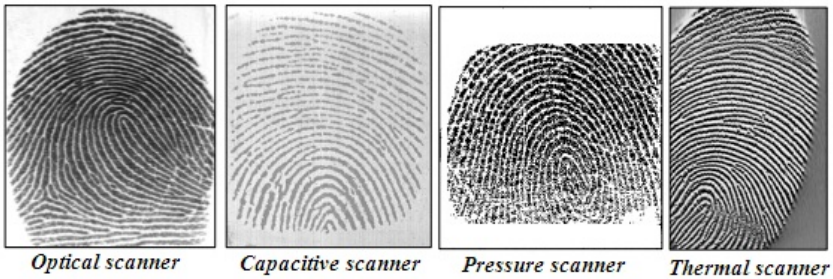

Figure 1: Examples of fingerprint captured by different scanners

[1] ***F**ederal **B**ureau of **I**nvestigation (**FBI**)*
[2] ***E**qual **E**rror **R**ate (**EER**)*
[3] ***C**harge **C**oupled **D**evices (**CCD**)*

2.3.5 Fingerprint Features Classification

Fingerprint pattern has a variety of features at different levels that are generally divided into three categories:

- **Universal Features**

Since most fingerprint databases are often very big, it's very slow and inefficient to check the matching of a particular fingerprint with all patterns through the database. The most important and common patterns, such as circular, spiral and arched, are shown in Figure 2. By using them, there is no need to compare the fingerprint with all the data, and we can easily refer to the data set of a particular class.

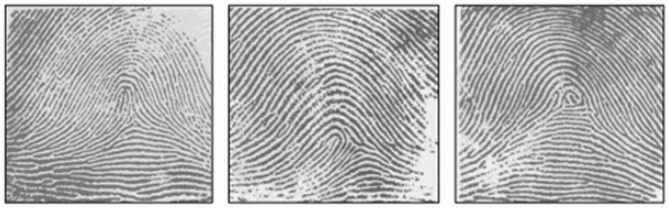

Figure 2: Fingerprint patterns [50]

On a fingerprint, Core is the highest point in the innermost bump, and Delta, is a trifid point that three ridges pass besides it. These points are shown in Figure 3.

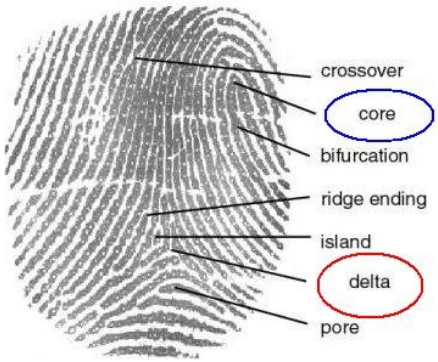

Figure 3: Location of Core and Delta points on the fingerprint [50]

- **Local features**

There are about 150 local features on this surface which are extracted based on local information from the ridges patterns. The most important features are junction points and final points, called Mapping Minuteae.

- **Third level**

It refers to the internal details of the ridges, such as width and curvature, which are not applied due to the need of high-resolution fingerprints.

2.3.6 Registration and Identification Operations

Figure 4, shows a general schema of a fingerprint Identification system.

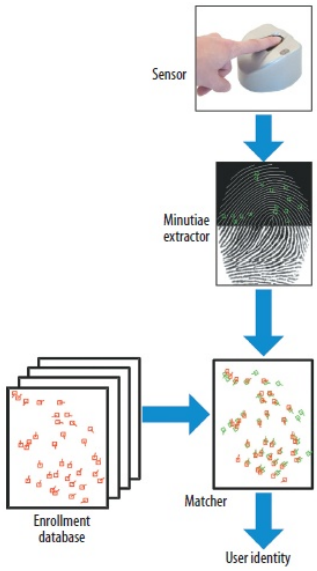

Figure 4: Fingerprint identification levels [46]

At registration phase, the fingerprint is scanned by the sensor and turns into a digital image by reading the features. At identification phase, the user touches the sensor again, and a new image is created from the fingerprint. The Minuteae points of this image are extracted and compared with the samples in the database. The features have three levels:

- ✓ ***First Level*** (left Figure 5): Capturing large scale details such as the shape of the friction ridges, the main pattern of lines and single points.
- ✓ ***Second Level***: The Two branches and Edge End edges.
- ✓ ***Third Level***: Includes all the dimensional characteristics of the fingerprint, such as the thickness of the lines, the shape and the marks of wounds and cuts.

From the obtained features of the first level, we can divide fingerprints into arched, circular or spiral patterns, as previously described.

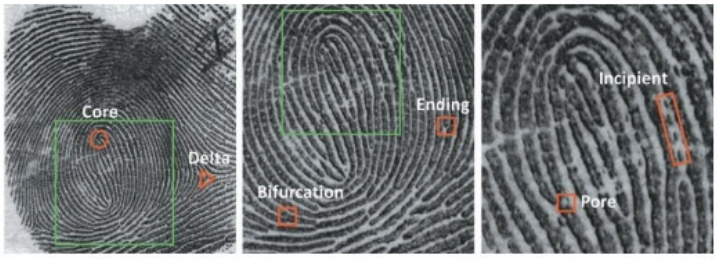

Figure 5: Sample of a Minuteae Extraction Algorithm [46]

3. Encryption

Despite the importance of biometric data, their encryption is vital. The knowledge of investigating and knowing of the principles and methods of secure transferring or storing information is called encryption. Encryption is the use of mathematical techniques to secure information [47] [41].

In principle, encryption is the knowledge of changing the message text or information by a key and a password algorithm, so that only the individual who knows the key and the algorithm, is able to extract the main information from the encrypted information [41] .

3.1 Encryption Algorithm

Any mathematical algorithm or function used in the encryption protocol due to having the required encryption features. The term "Encryption Algorithm" is a comprehensive concept and it is not necessary for each algorithm to be used directly for encryption, but only the application for encryption is considered. Despite the numerous encryption algorithms, only a small number of them are normalized.

3.1.1 Public Key Encryption

The public key is available for all individuals associated with the owner. In fact, the key used for encryption, is different with the key for decryption.

3.1.2 Private Key Encryption

The private key is available only for the owner (only the sender) and the encryption security depends on the confidentiality of the key. Private Key ciphers are divided into two types of Block and Stream ciphers, according to the type of operation, design, implementation, and applications. Their operation is based on a mutually beneficial interaction between two parties, as they agree on the private key by an initial communication, so that a third party does not know the key. The cipher is implemented by combining both keys. To decrypt an encrypted message, the computer must also use the public key provided by the sender, along with its own private key [3].

4. Stream Cipher Encryption

This type of encryption which is used in this article, is an important class of encryption algorithms, which uniquely, encrypts the characters (binary digits) of a message at a time, by using a cipher transfer at different times. In contrast, Block Cipher Encryption, tends to encrypt character groups of a message, by using a fixed encryption message altogether, at the same time. Stream Cipher Encryption is usually faster in terms of hardware than block cipher encryption, and the complexity of its hardware circuits is low.

In this paper standard stream cipher ***RC4***[1] is used in Biocode extraction and authentication as show in figure 7.

5. Application Background

In ***MOC***[2] Biometric Identity Application surveys, safe banking services can be accessed from biometric data on ***E_ID Card*** (new generation of electronic chip cards) issued by the State Registry Organization, which contains individual identity and biometric information and allows the issuance of biometric identity certificates, digital signatures, etc. to authenticate individuals in the country. Of course, this application has its specific problems; in this case, some researchers have investigated these problems,

[1] ***R**ivest **C**ipher ε (**RC4**)- Invented by **R**onald **L.R**ivest*
[2] ***M**atch **O**n **C**ard (**MOC**)*

using ***DEMATEL***[1] technique, and analyzed them by statistical discussion in terms of cross-sectional and structured complication. Some have also used the ***UID***[2] method [52].

5.1 Flawless Payment System Based on Fingerprint Biometrics

In this research, using a biometric stored in the database, simplifies the person's identification. It uses a Unique Identifier database at the bank's center; the individual's fingerprint is matched at the store, and the online cash payment system operates using the fingerprint biometrics in the database as a secure online password [4].

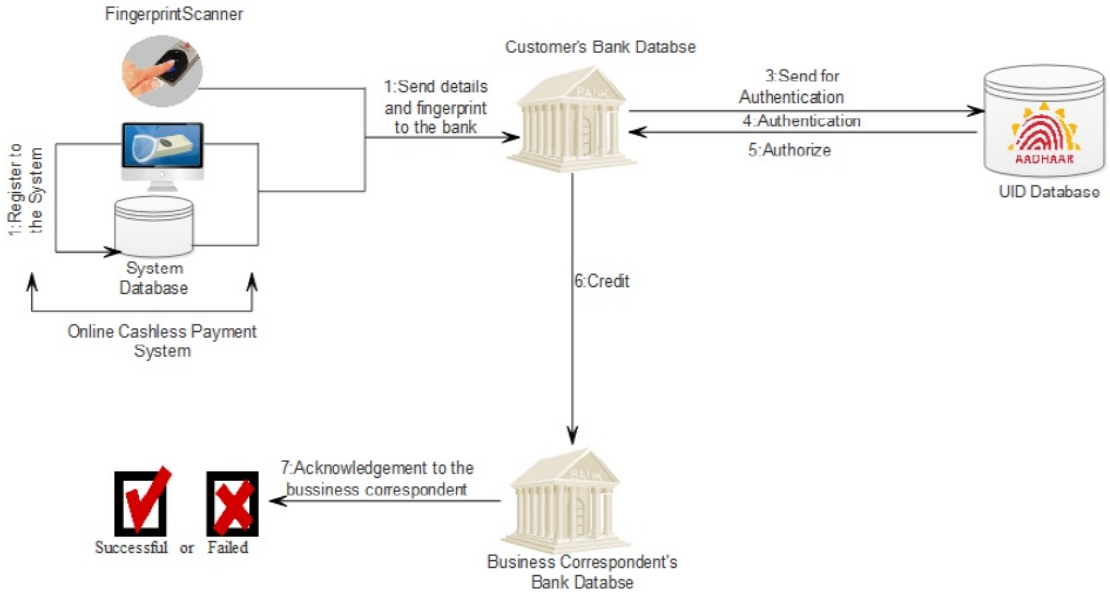

Figure 6: The architecture of the proposed online payment system [4]

This system is written by very weak software and can easily be penetrated and hacked; the system is at a very basic stage and does perform well in extended applications that require speed and precision in the network.

5.2 Electronic Payment Biometric Validation System

This research is designed to develop a commercial protocol for electronic transactions to improve the security of credit card purchases. The biometric mechanism performs as a digital interface to enhance online transaction security with smart phones and to increase customer's trust in remote transaction security.

First, the model converts the data into barcodes by pixel manipulation, and then converts the barcodes into byte arrays. Finally, encryption is performed, using the ***RSA***[3] algorithm.

This system is designed exclusively for mobile transactions and is not functional in a store where the buyer does not have a cell phone [5].

This method may include the risk of exposing account information or even duplicating fingerprint, if the cell phone is stolen.

---

*1 **D**ecision **M**aking **T**rial **A**nd **E**valuation (**DEMATEL**)*

*2 **U**nique **ID**entifier*

*3 **R**ivest **S**hamir **A**dleman (**RSA**)*

6. Proposed Method

Each of the previous works attempted to secure the banking system by using different methods and combining them with a different biometric system in different ways, and despite their advantages, each of them had a disadvantage. Here, with some investigations, some of the existing deficiencies have been resolved and a safer system in proposed, based on fingerprint authentication and Stream Cipher Encryption.

6.1 Proposed Biometric Authentication Method Steps

The proposed authentication protocol uses biometric data that should be read through capturing by a fingerprint reader device and must be protected by a protective algorithm.

The proposed protocol is very precise due to using the fingerprint feature, and can be used for any other biometric method. In fact, this method combines a password-based authentication method with a fingerprint biometric method. Basically, this is a two-factor approach. This method includes the following steps:

6.1.1 Proposed BioCode Extraction Protocol

The proposed BioCode Extraction Protocol includes three parts:

6.1.1.1 Extracting Fingerprint Code

First, the fingerprint of the user or customer is received through the receiver device sensor. After the image processing, a feature vector called the Fingerprint Code is extracted [22].

To store fingerprint information in a database, a Biohashing algorithm is used to analyze the biometrics [7].

The biocode extraction steps are shown in figure 7.

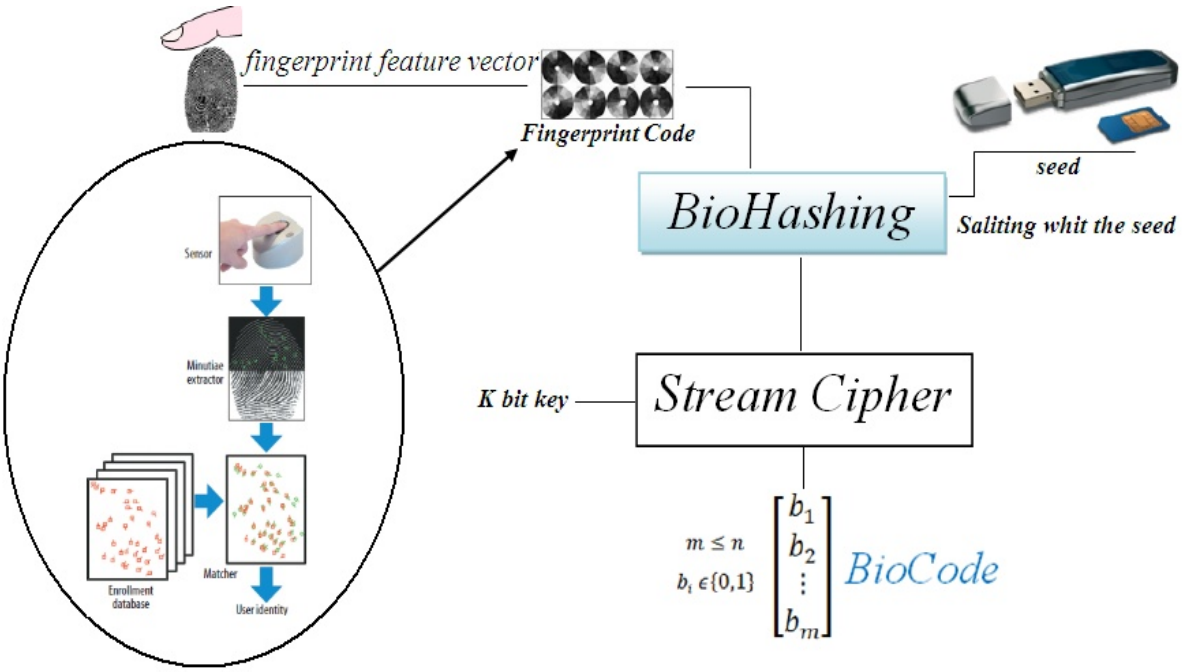

Figure 7: BioCode extraction steps

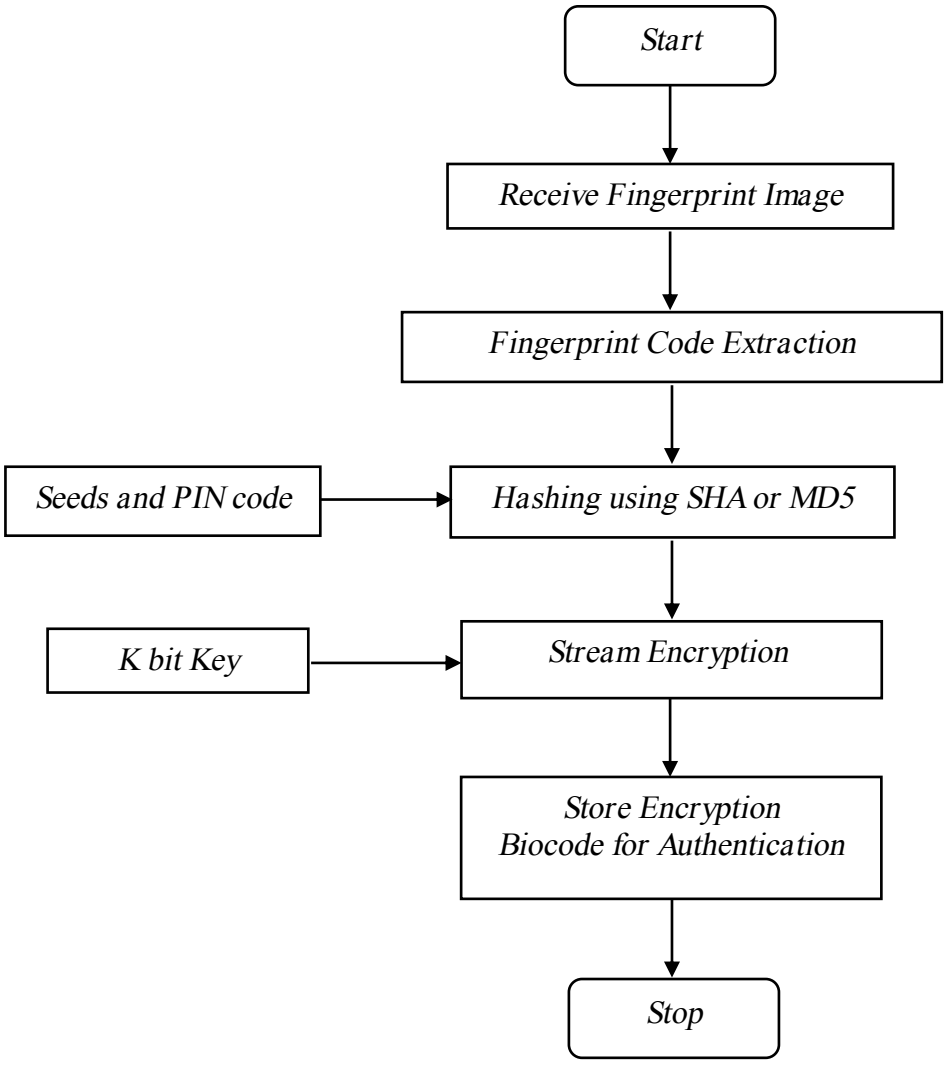

Figure 8: Propused Flochart for Artheatication Sender side

6.1.1.2 Extracting the function by Biohashing Algorithm

The fingerprint code along with the password, passes through a Biohashing Function and the encryption box, which the output of which, will be the BiCode. The Biohashing Function has the following characteristics:

The function is One-Way and irreversible.

Its input length is variable. (Receives messages with any length)

The output length is fixed (mapping from larger space to smaller) so that is:

Resistant to Collision (It is difficult to find different messages that are written with the same string).

This thread is called extract or abstract of the Digest message.

In general, there is no key!

6.1.1.3 Biohashing

The Biohashing Function will be hashing inputs features with standard methods. Standard hashing box can include ***SHA***[1] *or* ***MD5***[1].

[1] ***S****ecure* ***H****ashed* ***A****lgorithm* ***(SHA)***

The 128 or 256 bit key is shared between the receiver and the bank. The password can also be directly available for the customer or embedded in a lock. The BioCode is used in the registration and authentication process of a customer or user.

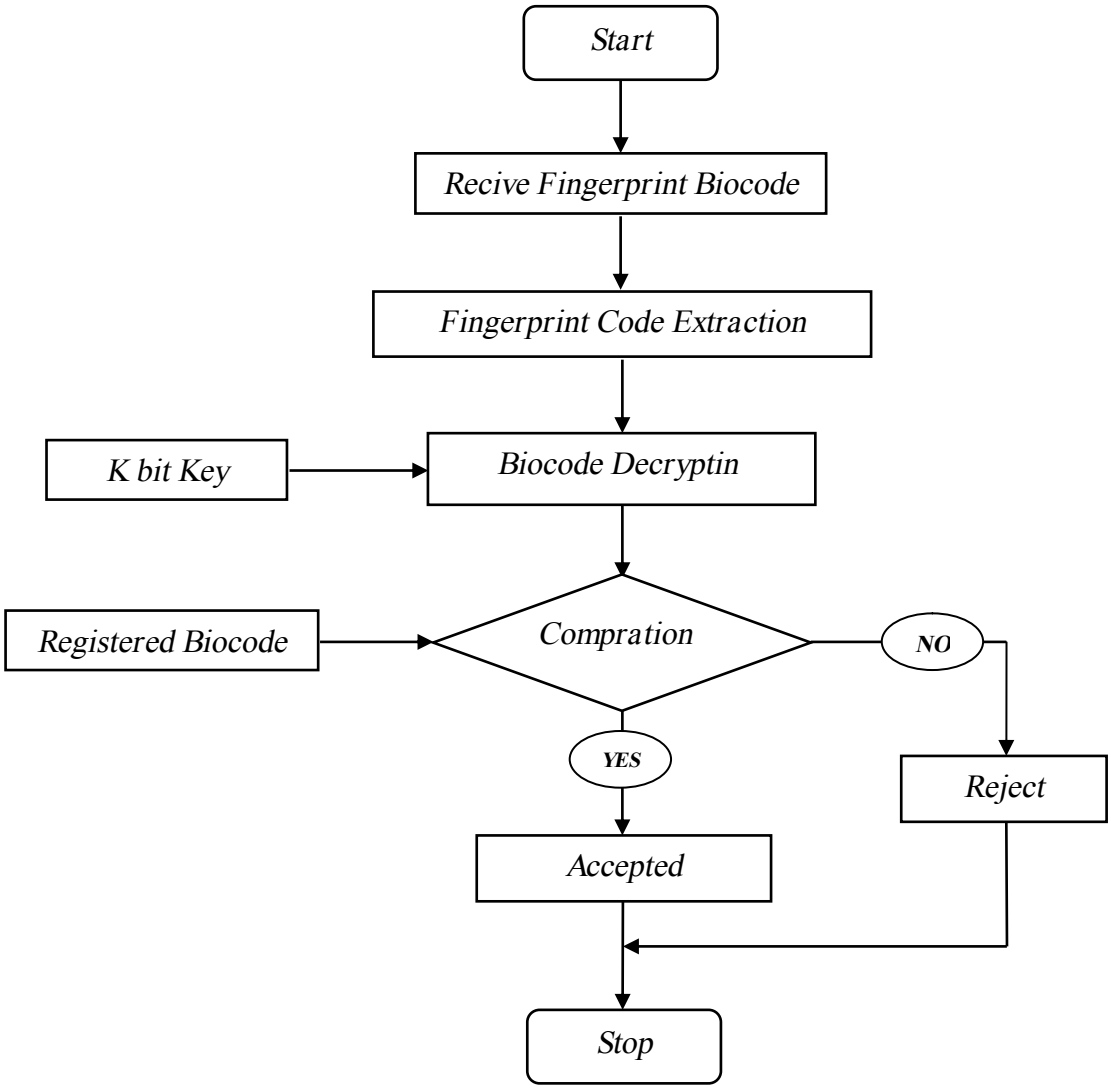

Figure 9: Propused Flochart for Artheatication Recive side

6.1.2 Registration Phase Proposed Protocol

In this fingerprint obtaining method, the presence of a client is required for a single time to provide identity papers at one of the bank's branches. By collecting a reference template that can be called with any name, the process begins. In the proposed method, a biocode called Reference provides a framework from a fingerprint code (a calculated fingerprint feature vector) and a code associated with the serial number of the device that captures the fingerprint. The user's password can be a password or a random number stored on the device, which is protected by biometric verification. When the reference name biocode is calculated, it is sent to the Bank's database through a ***SSL***[2] channel and is stored there for future use cases [8].

[1] ***M**essage **D**igest **5** (**MD5**)*
[2] ***S**ecure **S**ocket **L**ayer* (***SSL***)

6.1.3 Authentication Phase Proposed Protocol

At electronic payment request from the individual, the issuer bank must compare and confirm the fingerprint of the individual with the reference format. So, a challenge is sent to the reference database (the number displayed on the computer or the number sent directly to the fingerprint reader). The reference format should provide the fingerprint and password (not known by the issuer bank).

The captured Biocode, calculates the fingerprint code with biometric data, password and serial number of fingerprint recorder [42].

The biocode registeration challenge is calculated using the biohashing algorithm in the biocode Capture, with the challenge sent by the issuing bank as the password [6] [11].

The issuing bank also uses the biohashing to calculate the received biocode by challenging the algorithm with the reference biocode [14] [15].

Hamming Distance (the number of places where the corresponding symbols are different. In other words, the minimum number of substitutions that changes a string into another, or the number of errors that converts a string into another) is used to compare two biocode challenges, and if the distance is less than the predefined threshold, the reference format is verified [12] [13] [16].

7. Analysis and Evaluation

This section examines the performance and the failures of the fingerprint registration system and the proposed protocol.

7.1 Performance Efficiency

There is not just one measure to evaluate biometric devices, that shows how well a system works. To determine the strength or weakness of these types of systems, several measures must be analyzed [9] [39] [48].

7.1.1 Faults Generated by Fingerprint Registration Systems

Fingerprint system performance is measured based on the ***FPIR***[1] and ***FNIR***[2].

False Positive Identification occurs when the system returns a positive match result for an unregistered fingerprint.

The False Negative Identification occurs when the system reports a negative mismatch result or no match for a registered fingerprint. The relationship between these two factors is calculated from the following equation:

$$\boldsymbol{FPIR = 1 - (1 - FMR)^{N}} \qquad (1)$$

In this equation, ***N*** is the number of users registered in the system. Therefore, the more users registered in the system, the more the rate of ***FMR***[3] should be greatly reduced to maintain the system's optimal performance.

7.1.2 Fingerprint Performance Analysis

In this section, the protocol's performance is analyzed to avoid false rejection.

[1] ***F**alse **P**ositive **I**dentification **R**ate (**FPIR**)*
[2] ***F**alse **N**egative **I**dentification **R**ate (**FNIR**)*
*3 **F**alse **M**atch **R**ate (**FMR**)*

7.1.2.1 Experimental protocol

In this study, three fingerprint databases were used. In the following table, the functions of the best algorithms with their ***EER*** error rates and the ***FRR***[1] rates on this databases are calculated. In this table, ***ZeroFRM*** is the wrong ***FNMR*** mismatch when no falses are accepted. a attack consists of stealing, copying and replicating a biometric trait, to gain unauthorized access, defeating the biometric system security. The feasibility of a spoofing attack is much higher than other types of attacks against biometric systems, as it does not require any knowledge on the system, such as the feature extraction or matching algorithm used. Although liveness detection can be exploited to counteract spoofing rejected by the system. And Besides that In the table 1 of the best algorithms with their ***FRR*** rates and the ***SFAR***[2] rates on this databases are calculated [31] [32] [33].

The ***SFAR*** is the conditional probability that an impostor attempting a spoofing attack is wrongly accepted as a client. For example, if the ***EER*** operating point, defined as the point where the ***FRR*** equals the ***FAR*** [30] [34] [41].

Table 1: Performance of the best algorithm for three databases

DataBase	EER	ZeroFMR	FRR	SFAR
CASIA V3	0.11%	0.18%	1.70%	1.25%
CASIA V4	0.27%	0.65%	1.50%	1.02%
CASIA V5	1.12%	2.25%	2.28%	2.55%

7.1.2.2 Experimental Method

Table 2 presents the datasets of scores used to evaluate the proposal, the number of individuals and also number of nodes and the number of scores also corresponds to the maximum number of edges. while the ***EER*** The threshold is configured to correspond. Among the different evaluation methodologies of the literature, we want to compete with the Zoograph [49]. which is used as the baseline for local evaluation method [41].

Table 2: Description of the datasetsused to evaluatethe proposal.

DataBase	Type	Modality	Methodology	individuals	Sample/ individuals	scores	EER
AR [24]	Score	Face	SIFT[3] based matching	120	26	360000	10.19%
ENSIB[25]	Score	Face	SIFT based matching	100	40	390000	10.88%
FC94 [26]	Score	Face	SIFT based matching	152	20	438976	0.29%
FVC [27]	Score	Fingerprint	SIFT based matching	100	8	70000	10.27%
veins [28]	Score	Vein	SIFT based matching	24	30	16704	0.0%
OU-ISIR BSS3 [29]	Distance	Gait (accelerometer)	Distance between 2signals	736	variable	10175181	14.88%
CASIAV3 (proposed method)	Score	Fingerprint	SIFT based matching	100	25	---	1.30 %
CASIAV4 (proposed method)	Score	Fingerprint	SIFT based matching	100	25	---	1.85 %
CASIAV5 (proposed method)	Score	Fingerprint	SIFT based matching	100	25	---	2.435%

1 False Rejection Rate (FRR)
2 Spoof False Acceptance Rate (SFAR)
3 Scale Invariant Feature Transform (SIFT)

8. Conclusion

The proposed method is used for application and security in an online payment system, which includes using a biometric authentication mechanism, and is used to confirm the stored format of fingerprints at the time of registration. If the fingerprint is matched with the sample in the database, the payment will be successful, and the customer can execute the transaction and the security will be provided.

This method will be easily effective in ensuring security and confidence in bank payments. The client and the secure electronic payment system can be connected to ***ATM***[1] and any other devices. The application of Stream Cipher encryption algorithm will provide fast implementing, small-size, low complexity and high security for devices with limited resources and includes a simple software implementation.

9. Future Works and Suggestions

Bank payment systems are usually evaluated with their cards and passwords, and the seller's approval in the transaction is ignored. For users, it is difficult to remember passwords. For online banking, this authentication protocol is applicational that can increase electronic payment authentication security. There are many future views for this topic. The best method is to use multiple biometrics instead of passwords; methods such as Face Detection, Iris, Voice, etc. will be appropriate.

References

[1] Y.Espelid, L.H. Netland, A.Klingsheim, and K. Hole. A proof of concept attack against norwegian internet banking systems. Financial Cryptography and Data Security, pages197–201,2008.

[2] S. Murdoch and R. Anderson. Verified by visa and mastercard securecode: or, how not to design authentication. Financial Cryptography and Data Security, pages 336–342, 2010.

[3] Sourabh Chandra, SmitaPaira, SkSafikul Alam, Goutam Sanyal,comparative survey of symmetric and asymmetrickey cryptography 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)978-1-4799-5748-4/14/2014 IEEE.

[4] Manjiri,A. Lavadkar, Pallavi K.Yhorat, Ankita R, Kasliwal, Jaya S, Gadekar, Dr.Prapti Deshmukh.” Fingerprint Biometric Based Online Cashless Payment System” JOSR Journal of Computer engineering (JOSR-JCE), PP 27-32.

[5] Nikhil Khandare, Dr.B.B.Meshram.“Electronic Payment Biometric Validation System” International Journal of Reserch and Applications e-HSSN:2320-8163, Volume1, Issue 5 (Nov-Dec 2013), pp,53-58.

[6] C.Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. on Information Security, 3, 2011.

[7] A.B.J. Teoh, D. Ngo, and A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition, 40, 2004.

[8] S. Murdoch and R. Anderson. Verified by visa and mastercard securecode: or, how not to design authentication. Financial Cryptography and Data Security, pages 336–342, 2010.

[9] G. Antoniou and L. Batten. E-commerce: protecting purchaser privacy to enforce trust. Electronic commerce research, 11(4):421–456, 2011.

*1**A**utomated **T**eller **M**achine (**ATM**)*

[10] M .Mosleh, F. Forootan and N. Hosseinpour, "Presenting a New Text-Independent Speaker Verification System Based on Multi Model GMM", Journal of Advances in Computer Research, Quarterly pISSN: 2345-606x eISSN: 2345-6078, Sari Branch, Islamic Azad University, Sari, I.R.Iran, (Vol. 5, No. 4, November 2014), Pages: 67-78, www.jacr.iausari.ac.ir.

[11] J. Daugman. New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 37(5):1167–1175, October 2007.

[12] A. Juels and M. Sudan. A fuzzy vault scheme. In ISIT, page 408, 2002.

[13] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In ACM Conference on Computer and Communications ecurity, pages 28–36, 1999.

[14] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. Scifi - a system for secure face identification. In IEEE Symposium on Security and Privacy, 2010.

[15] N.K. Ratha, J.H. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication system. IBM Systems J., 37(11):2245–2255, 2001.

[16] C.Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. on Information Security, 3, 2011.

[17] A .Gholami and H. Hassanpour, "Common Spatial Pattern for Human Identification Based on Finger Vein Images in Radon space", Journal of Advances in Computer Research, Quarterly pISSN: 2345-606x eISSN: 2345-6078, Sari Branch, Islamic Azad University, Sari, I.R.Iran, (Vol. 5, No. 4, November 2014), Pages: 31-42, www.jacr.iausari.ac.ir.

[18] Manal Adham, Amir Azodi, Yvo Desmedt, and Ioannis Karaolis. How to attack two-factor authentication internet banking. In Financial Cryptography, 2013.

[19] European Commission. Directive 2000/31/ec of the european parliament and of the council of 8 june 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('directive on electronic commerce'), 2000.

[20] European Commission. Directive 2007/64/ec of the european parliament and of the council of 13 november 2007 on payment services in the internal market amending directives 97/7/ec, 2002/65/ec, 2005/60/ec and 2006/48/ec and repealing directive 97/5/ec, 2007.

[21] Y. Espelid, L.H. Netland, A. Klingsheim, and K. Hole. A proof of concept attack against norwegian internet banking systems. Financial Cryptography and Data Security, pages 197–201, 2008.

[22] B. S. Manjunath and W.Y. Ma. Texture features for browsing and retrieval of image data. IEEE Transactions on Pattern Analysis and Machine Intelligence, 18:37–42, 1996.

[23] M .Rajabi, S. Ghofrani and A. Ayatollahi, "A New IRIS Segmentation Method Based on Sparse Representation", Journal of Advances in Computer Research, Quarterly pISSN: 2345-606x eISSN: 2345-6078, Sari Branch, Islamic Azad University, Sari, I.R.Iran, (Vol. 8, No. 8, February 2017), Pages: 89-105, www.jacr.iausari.ac.ir.

[24] A. Martinez and R. Benavente, "The AR face database," CVC Tech. Report, 1998. [Online]. Available: http://www2.ece.ohiostate. edu/ aleix/ARdatabase.html.

[25] B. Hemery, C. Rosenberger, and H. Laurent, "The ENSIB database : a benchmark for face recognition," in International Symposium on Signal Processing and its Applications, special session "Performance Evaluation and Benchmarking of Image and Video Processing", 2007.

[26] U. of Essex, "Faces94 database, face recognition data," 1994.

[27] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "Fvc2002: Second fingerprint verification competition," in International Conference on Pattern Recognition, vol. 3, 2002, pp. 811 – 814. [Online]. Available: http://bias.csr.unibo.it/fvc2002/

[28] P.-O. Ladoux, C. Rosenberger, and B. Dorizzi, "Palm vein verification system based on sift matching," in the 3rd IAPR/IEEE International Conference on Biometrics (ICB'09), 2009, pp. 1290–1298.

[29] N. T. Trung, Y. Makihara, H. Nagahara, Y. Mukaigawa, and Y. Yagi, "Performance evaluation of gait recognition using the largest inertial sensor-based gait database," in Biometrics, 2012 5th IAPR International Conference on, 2012, pp. 360–366.

[30] L .Pourabdi and A. Harounabadi, "Providing a Method to Identify Malicious Users in Electronic Banking System Using Fuzzy Clustering Techniques" Journal of Advances in Computer Research, Quarterly pISSN: 2345-606x eISSN: 2345-6078, Sari Branch, Islamic Azad University, Sari, I.R.Iran, (Vol. 8, No. 2, May 2017), Pages: 67-77, www.jacr.iausari.ac.ir.

[31] X. He, Y. Lu, and P. Shi. A fake iris detection method based on fft and quality assessment. In Chinese Conf. on Pattern Recognition, pp. 316–319, 2008.

[32] B. Geller, J. Almog, P. Margot, and E. Springer. A chronological review of fingerprint forgery. J. of Forensic Science, 44(5):963–968, 1999.

[33] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Z. Li, W. R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo Navarro, M. Castrill´on-Santana, J. Maatta, A. Hadid, and M. Pietikainen. Competition on counter measures to 2-D facial spoofing attacks. In Int'l Joint Conf. on Biometrics (IJCB), In press, 2011.

[34] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers. LivDet2011 - Fingerprint Liveness Detection Competition 2011. In 5th Int'l Conf. on Biometrics (ICB), In press, 2012.

[35] R. N. Rodrigues, L. L. Ling, and V. Govindaraju. Robustness of multimodal biometric fusion methods against spoof attacks. J. of Visual Languages and Computing, 20(3):169–179, 2009.

[36] R. N. Rodrigues, N. Kamat, and V. Govindaraju. Evaluation of biometric spoofing in a multimodal system. In Int'l Conf. Biometrics: Theory Applications and Systems (BTAS), pp. 1–5, 2010.

[37] Z. Akthar, B. Biggio, G. Fumera, and G. L. Marcialis. Robustness of multi-modal biometric systems under realistic spoof attacks against all traits. In IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS), pp. 5–10, 2011.

[38] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli. Evaluation of multimodal biometric score fusion rules under spoof attacks. In 5th Int'l Conf. on Biometrics (ICB). In press, 2012.

[39] B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli. Robustness of multi-modal biometric verification systems under realistic spoofing attacks. In Int'l Joint Conf. on Biometrics (IJCB). In press, 2011.

[40] A. Adler. Vulnerabilities in biometric encryption systems. 5th Int'l Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA), volume 3546 of LNCS - Springer, pp. 1100–1109, 2005.

[41] S.E.T. Secure electronic transaction specification. Book 1: Business Description. Version, 1, 2002.

[42] R.M. Bolle, J.H. Connell, and N.K. Ratha. Biometric perils and patches. Pattern Recognition, 35(12):2727–2738, 2002.

[43] P. Johnson, B. Tan, and S. Schuckers. Multimodal fusion vulnerability to non-zero effort (spoof) imposters. In IEEE Int'l Workshop on Information Forensics and Security (WIFS), pp. 1–5, December 2010.

[44] K .Mirzaei Talarposhti and M. Khaki Jamei, "An Efficient Model for Lip-reading in Persian Language Based on Visual Word and Fast Furrier Transform Combined with Neural Network", Journal of Advances in Computer Research, Quarterly pISSN: 2345-606x eISSN: 2345-6078, Sari Branch, Islamic Azad University, Sari, I.R.Iran, (Vol. 8, No. 2, May 2017), Pages: 103-124, www.jacr.iausari.ac.ir.

[45] http://biometrics.idealtest.org/dbDetailForUser.do?id=7

[46] Anil K. Jain, Jianjiang Feng , Karthik Nandakumar ,"Biometrics Fingerprint Matching",2010, Published by the IEEE Computer Society.

[47] F .Ghanbari Adivi and M. Mehrnia, "Audio Signal Encryption Based on Permutation Relations and Residue Number System", Journal of Advances in Computer Research, Quarterly pISSN: 2345-606x eISSN: 2345-6078, Sari Branch, Islamic Azad University, Sari, I.R.Iran, (Vol. 7, No. 3, August 2016), Pages: 67-76, www.jacr.iausari.ac.ir .

[48] Biometrics Metrics Report, v3.0, Prepared for: U.S. Military Academy (USMA) – West Point, December 2012.

[49] R. Giot, R. Bourqui, and M. El-Abed, "Zoo graph: a new visualisation for biometric system evaluation," in Information Visualisation 2016, 2016, pp. 190–195.

[50] http://www.viewzone.com/fingerprintsx.html and https://www.researchgate.net/figure/Basic-fingerprint-patterns-a-the-arch-is-the-simplest-of-all-the-configurations-b_fig1_11673949.

[51] M .Eliasi, M. Taghi Manzuri, Z. Yaghoubi and A. Eliasi, "Novel Texture Description and Face Identification Methods by Defining Bridle Paths and Using Gabor Phases", Journal of Advances in Computer Research, Quarterly pISSN: 2345-606x eISSN: 2345-6078, Sari Branch, Islamic Azad University, Sari, I.R.Iran, (Vol. 7, No. 3, August 2016), Pages: 67-76, (Vol. 5, No. 3, August 2014), Pages: 35-53, www.jacr.iausari.ac.ir.

[52] M.A. Lavadkar, P.K. Thorat, A.R. Kasliwal, J.S. Gadekar and Dr. P. Deshmukh, "Fingerprint Biometric Based Online Cashless Payment System", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727, PP 27-32, www.iosrjournals.org.