Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.6, No.11, 2016

Various Biometric Techniques Suitable for Securing Banking System

Omogbhemhe, M. I.[1] Momodu, I.B.A.[2]
1.Department of Mathematical and Physical Sciences, College of Basic and Applied Sciences, Samuel Adegboyega University, Ogwa Edo State Nigeria
2.Department of Computer Science, Faculty of Natural Sciences, Ambrose Alli University, Ekpoma, Edo State

Abstract
Biometric is becoming an important method for human identification in many fields of human endeavour. Thus, the banking sector is not an exception. The implementation of biometric techniques in banking systems, will help to provide strong security by allowing customers to use it to validate any banking transaction before the transaction is been carried out. This technique will help to prevent people entrusted with the system, to commit fraud on the customer's account using the system without the knowledge of the customer. This paper present different biometric measures/techniques that are suitable for this operation. The information provided in the paper will serve as a guide towards implementing such system in the banking sector.
Keywords: Biometric, Techniques, Security, Banking System

1. Introduction

E-banking refers to the use of computer hardware, software and the network system in processing customer request directly from/to the bank central database. Before the information age, transactions in the banking sector were carried out using pen and paper for keeping proper customer's records. But today, many of these operations are been carried out using computers. These computers are used in managing bank customer's information thereby speeding up the rate of attending to customer's request. However, a part from the use of Automatic Teller machine (ATM), the customers are not allowed to either operate the system or view the system operation when making any transaction (e.g. Withdraw). This makes the customer to providing account details (e.g. account name, amount, signature, account number etc.) to the bank staff. Meanwhile one of the major problem information security is facing today is that the people entrusted with the use of the system to carry out daily transactions like withdrawing money from customer's account are abusing the system.

It is worthy to note at this point that the banking sector has some employee (bank staffs) that makes use of this system in attending to customers. These customers give their details to the staff in order to attend to their request. The customers' do not see anything wrong in giving account details to the staff, since it is the only way large transactions can be made by the customer. Similarly due to the kind of system in operation the customer do not have the privileges to access the system used in order to ascertain if the transaction was actually made by the bank staff or not or even to validate the transaction after providing the information to the staff. The system only gives privileges to the staff to perform and validate the operation. This is actually a serious threat to bank information security, because the bank staff or any person can copy the customer account details, forge his/her signature and use it to make personal transaction and the system has no means to detect it. In the same vain, using the banking system to attend to customer's request has a lot of vulnerability to fraud. This is true because the system has no provision for a customer to authenticate or validate a transaction in the system after submitting his/her transaction detail. This shows us that it is not the system that helps to checkmate financial fraud in the banking sector but the staffs of the bank at the point of carrying out withdraws from customer's account. This suppose not to be so and many bank staffs take advantage of this to execute frauds on customer's account.

To further strengthen out point, recently three young Nigerian bankers were sentenced to 91 years in prison for withdrawing 114 million naira from customer's account without the knowledge of the customers [9]. The truth is, if there was a means in the banking system to enable customer's transaction authentication before any transaction is been made, such fraud will never occur. Hence, the need for implementing additional measure that will allow the validation of any transaction by the bank customers mainly during withdraws before the transaction is made cannot be overemphasize. One of such means is the use of human biometrics. This paper is seriously in support on implementing biometric techniques for validating transaction in the banking system.

The introduction of biometric as a means of authenticating any transaction (mainly withdraw) from the banking system will go a long way to checkmating this kind of financial frauds in the banking sector by those entrusted with the system. Biometric is the measure of human physical characteristics or personal trait used for the unique identification of the person. It is a science of authentication by measuring the person physiological or behavioural features [1]. Biometrics measures physiological or behavioural characteristics that allow variable identification and some well-known of these biometric (a good example is the iris) are used for forensic identification today [4].

Meanwhile, implementing biometric techniques as a means of authenticating any banking transaction

(mainly withdraw) shows that the customer performing the transaction must be present at the time of the transaction. This will make it difficult for anybody (either bank staff or any other fraudster) to perform transaction in any customer's account without the knowledge of the customer. The very facts that make this technique interesting in checkmating and eliminating frauds in customer's account is that the account name and signature can be interchange but physical trait cannot be interchange.

This paper explained various biometric techniques/measures that will be suitable in authenticating banking transaction by discussing their various advantages and disadvantages. The reason is for us to be able to choose the best and efficient biometric to adopt in securing the banking system.

2. Biometric Techniques

There exist many biometric techniques, however, the ones that will be of interest as far as this paper is conscience are fingerprint, iris, Lips, facial and voice recognition. These few ones were discussed because of their popularity and easy adaptability features by the users.

2.1 Facial Recognition

This is the use of facial features to verify an individual from a digital image or video system. It involves evaluating selected facial features from the image captured and compares it with the one in the database to ascertain whether the person is legitimate or not. The advantage of this technique is that they can perform massive identification which other biometric can't perform [8]. The technique doesn't require any direct contact with the person in order to verify his/her identity. However the disadvantages associated with this technique is that it does not work effectively with bad/poor weather. It is a costly technique when compare with the finger print technique.

2.2 Fingerprint

Every human being has some uniqueness in their fingerprint because of the numerous ridges and valley on the surface of the finger. Fingerprint feature extraction and matching approach relies on the fact that the uniqueness of fingerprint can be determined by detecting prominent singular point known as minutiae. It is therefore possible to use this as a means of authenticating transaction in the banking system. The advantage is that they are largely universal. Only 2% of the world population cannot use fingerprint due to skin damage [3], it is very easy to use and the operation requirements are less expensive. Hence, it will be suitable for authenticating banking transaction. However, fingerprint scanner can be cheated with artificial fingerprint [6].

2.3 Iris

This is one of the biometric authentication techniques with very low false acceptance. Once taken, it is compare with the one in the database. It offers one of the secured strategies of authentication and recognition. Everybody has different and independent iris texture, this make it possible to use it as a means of identification. One of the advantage of this technique is the easy recognition of fake iris (e.g. when the person wear colour contact) and it has a very low processing time. One of it disadvantages is that it perform poorly at a distance because of it small nature [7]. Also, iris scanners are expensive [8].

2.4 Voice Recognition

According to [5], voice recognition is a technology through which sound, phrases and word voice by human beings are transformed into electrical signals and these signals are converted into code design. This kind of technology can be used by people with damage skin for identification. It fit everybody and does not require much training to operate it. However this technique may make mistake if there is noise and disturbance. The technology is very expensive to implement.

2.5 Lip identification

Human lip can be used to identify a particular person. It originated from felony and forensic process [7]. Lips form and colour can be used to recognize human identity. One advantage is that lips attributes are usually distinct from every person, thus can serve as a means of identification. Similarly, sizes of lip are small, thus, can easily be process with a computer program. One demerit is that a smile by the person can cause difficulties in identifying the person.

3. Conclusion

Different biometric techniques suitable for securing banking system have been presented with their advantages and disadvantages in this paper. This is to enable us know the best and efficient one that can be used in authenticating transaction in the banking system. Since biometric techniques can be used to validate any transaction in the banking system (software) before full transaction is made, it will be impossible for the system to allow people entrusted with the banking operations (staffs) to commit fraud on customer account information

without the knowledge of the customer. Future research in this area should be able to provide the best biometric technique to use in these banking systems and the possible algorithm to using such technique.

References

[1] Adeoye T.O. (2014). Development of a computerized biometric control examination screening and attendance monitoring system with fee management. World of Computer Science and Information Technology Journal Vol. 4. No 6, 76-81.
[2] Anil K. Jain, Arun Ross and Salil Prabhakar (2004), "An Introduction to Biometric Recognition."
[3] David Weiss (2009), "Fingerprint Biome
[4] Guruprasad K.V and Sandeep P.H (2015). A modified Thinning Algorithm for Minitiae Feature Extraction of Fingerprint Image on FPGA. Proceedings of 19th IRF International Conference. 25th January 2015 Chennai. India.
[5] Jim Baumann, "VoiceRecognition".
[6] Omogbhemhe M.I and Momodu I.B.A (2015), "Biometric Bank Account Verification System in Nigerian: Challenges and Opportunities. International Journal of Computer Science and Information Security (IJCSIS), Vol. 13, No. 6
[7] Penny Khaw ; SANS Security Essentials (GSEC) Practical Assignment Version 1.3," Iris Recognition Technology for Improved Authentication".
[8] Rabia Jarfi and Hamid R. Arabina (2009), "A Survey of Face Recognition Techniques", Journal of Information Processing Systems, Vol.5, No.2, June 2009.
[9]http://naijagists.com/photo-nigerian-bankers-jailed-for-91years-for-withdrawing-n114million-from-customers-accounts/