© 2015 IJSRST | Volume 1 | Issue 2 | Print ISSN: 2395 - 6011 | Online ISSN: 2395 - 602X
Themed Section: Engineering and Technology

Face Recognition as a Biometric Security for Secondary Password for ATM Users. A Comprehensive Review

Lusekelo Kibona
Department of Computer Science
Ruaha Catholic University (RUCU)
Iringa, Tanzania

ABSTRACT

Authentication is an important aspect in system control in computer based communication. Automatic Teller Machines (ATMs) are widely used in our daily lives due to their convenience, wide-spread availability and time-independent operation. In this paper, the author tried to review some mechanisms used in dealing with security threat posed to ATM users and found that there are potential threats associated with using card based security system so there is a need to add up another secondary security after the primary stage has been passed and that secondary stage is facial recognition security system as explained in an algorithm developed in this paper. The recommendations for future biometric system has been suggested like smell from mouth breathing be considered as the future secondary security system even though it has got its challenges.
Keywords: ATM, ATM cards, Face recognition, Biometric security, banking systems.

I. INTRODUCTION

Biometrics refers to automatic identification of a person based on his or her physiological or behavioral characteristics. It provides a better solution for the increased security requirements of our information society than traditional identification methods such as passwords and PINs [1].

ATM as a cash dispenser which is designed to enable customers enjoy banking service without coming into contact with Bank Tellers (Cashiers). The ATM, therefore, performs the traditional functions of bank cashiers and other counter staff. It is electronically operated and as such response to a request by a customer is done instantly [2]. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip that contains a unique card number and some security information, such as an expiration date. Security is provided by the customer entering a personal identification number (PIN) [3].

Due to limitation on banking hours, it is therefore difficult for people to get access to their money when needed. ATM, represents customers' satisfaction and cost savings device. Customers become their own teller when they use ATM.

Automatic Teller Machines (ATMs) are widely used in our daily lives due to their convenience, wide-spread availability and time-independent operation. Automatic retraction of forgotten card or cash by ATMs is a problem with serious consequences (lost time and money), typically caused by user inattention/negligence [4].

Authentication is an important aspect in system control in computer based communication. Human face recognition is an important biometric verification and has widely used in many applications such as video monitoring system, human computer interaction, door control system and network security.

Face recognition technology is gradually evolving to universal Biometric solutions, since it requires virtually zero efforts from the user end while compared with other biometric options [5].

Using credit or debit cards to withdraw cash from an ATM may become a thing of the past with the introduction of facial recognition technology. The ATM comes with a camera that sends details of a customer's facial dimensions to a database for verification. Once the image is verified, the customer either enters a PIN or answers a personal security question. A thief could not use a photograph to trick the machine because the machine uses length, width and depth to recognize the image [6].

To use an ATM with facial recognition system, all you need is walk to the atm. its digital camera is on 24hours a day, and its computer will automatically initiate a face recognition procedure, whenever the computer detects a human face in camera obtains a picture of your face, the computer compares the image of your face to the images of registered customers in its database .If your face (as seen by the ATMs camera) matches the picture of the in the data base you are automatically recognized by the machine [7].

Figure 1: Images showing the ATM with embedded camera and customers doing transactions[8].

The smart ATM removes the need to carry cards every time one wishes to access the bank account. The idea behind the machine's development is to make banking friendly. Its use could also reduce the now common incidents where carjackers force their victims to empty their accounts at gunpoint, often taking the card and the personal identification number (PIN). The camera uses the system of biometrics to recognize the account holder — those used in computer science are the distance between the eyes and the proportion of the nose to the mouth and the location of the cheekbones. Once the image is found to be authentic, the customer is then prompted to enter their PIN or asked a personal question such as "What's your pet's name?" The correct PIN or answer would then allow the person to use the ATM in the normal way. Your twin brother or sister would pass the face test but fail at the PIN or question stage. It also impossible to use a life-size photograph of the account holder as the machine uses three dimensions, length, width and depth, to recognize the image [9].

Background and Literature Survey

Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. By using biometrics a person could be identified based on "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows" (password, PIN) [10].

The existing ATM model uses a card and a PIN which gives rise to increase in attacks in the form of stolen cards, or due to statically assigned PINs, duplicity of cards and various other threats [11].

As per [11], The face recognition feature inhibits access of account through stolen or fake cards. The card itself is not enough to access account as it requires the person as well for the transaction to proceed. Eigen face based method is used for the face recognition. However, the drawback of using Eigen face based method is that it can sometimes be spoofed by the means of fake masks or photos of an account holder.

[12], pointed out that the lack of cooperation among banks in the fight to stem the incidence of ATM related frauds now plaguing the industry. He expressed that the silence among banks on ATM frauds makes it difficult

for banks to share vital information that will help curb the menace.

According to [13], the current upsurge and nefarious activities of Automated Teller Machine (ATM) fraudster is threatening electronic payment system in the nation's banking sector with uses threatening massive dumping of the cards if the unwholesome act is not checked.
As per [14] the ATM services are highly profitable for banks, and banks aggressively market the use of ATM cards. ATMs that are off bank premises are usually more profitable for banks because they attract a higher volume of non-bank customers, who must pay service fees. Unfortunately, customers using off premise ATMs are more vulnerable to robbery. ATM robberies estimates are derived from periodic surveys of banks conducted by banking associations. According to those surveys, there was an estimated one ATM crime (including robbery) per 3.5 million transactions.

In his white paper [15], pointed that, there are different techniques of ATM frauds, which are:

Card Theft: In an effort to obtain actual cards, criminals have used a variety of card trapping devices comprised of slim mechanical devices, often encased in a plastic transparent film, inserted into the card reader throat. Hooks are attached to the probes preventing the card from being returned to the consumer at the end of the transaction. When the ATM terminal user shows concern due to the captured card, the criminal, usually in close proximity of the ATM, will offer support, suggesting the user enter the PIN again, so that he or she is able to view the entry and remember the PIN. After the consumer leaves the area, believing their card to have been captured by the ATM, the criminal will then use a probe (fishing device) to extract the card. Having viewed the customers PIN and now having the card in hand, the criminal can easily withdraw money from the unsuspecting user's account.

Skimming Devices: Another method of accessing a consumer's account information is to skim the information off of the card. Skimming is the most frequently used method of illegally obtaining card track data. "Skimmers" are devices used by criminals to capture the data stored in the magnetic strip of the card. Reading and deciphering the information on the magnetic stripes of the card can be accomplished through the application of small card readers in close proximity to, or on top of, the actual card reader input slot, so it is able to read and record the information stored on the magnetic track of the card. The device is then removed, allowing the downloading of the recorded data.

PIN Fraud: This can take the following forms:
Shoulder Surfing: Shoulder Surfing is the act of direct observation, watching what number that person taps onto the keypad. The criminal usually positions himself in close but not direct proximity to the ATM to covertly watch as the ATM user enters their PIN. Sometimes miniature video cameras that are easily obtained might be installed discretely on the fascia or somewhere close to the PIN Pad, to record the PIN entry information.

Utilizing a Fake PIN Pad Overlay: A fake PIN pad is placed over the original keypad. This overlay captures the PIN data and stores the information into its memory. The fake PIN pad is then removed, and recorded PINs are downloaded. Fake PIN pads can be almost identical in appearance and size as the original. An additional type of overlay that is more difficult to detect is a 'thin' overlay that is transparent to the consumer. This method used in conjunction with card data theft provides the criminal with the information needed to access an unsuspecting consumer's account. PIN Interception: After the PIN is entered, the information is captured in electronic format through an electronic data recorder. Capturing the PIN can be done either inside the terminal, or as the PIN is transmitted to the host computer for the online PIN check. In order to capture the PIN internally, the criminal would require access to the communication cable of the PIN pad inside the terminal, which can more easily be done, at off-premise locations.

The moment the card is accessible, PIN is guessed or obtained through other means such as social engineering, shoulder surfing or outright collection under duress. Recently, Biometric ATMs are introduced to be used along with card. This will definitely impact on the amount frauds if fully implemented. Further development has produced biometric authentication in Japan where customers face is used as a means of authentication [16, 17].

According to [7], biometrics as means of identifying and authenticating account owners at the Automated Teller

Machines gives the needed and much anticipated solution to the problem of illegal transactions.

In his research titled "A Third Generation Automated Teller Machine Using Universal Subscriber Module with Iris Recognition" [18], pointed out that in real time ATM cards are being used as a form of identification and authentication. But there is a highest possibility for the ATM cards to be theft or lost and even if the card is bent or heated, it becomes useless to access the ATM machine. With the increase of automated teller machine (ATM) frauds, new authentication mechanisms are developed to overcome security problems. One inherent problem with ATM cards is the possibility of loss or theft and it should be carried for each and every transaction, which we forget to do in many cases.

According to [19], for face recognition, there are two types of comparisons. The first is verification, this is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The next one is identification this is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches. Face recognition technology analyzes the unique shape, pattern and positioning of the facial features. Face recognition is very complex technology and is largely software based.

Eum et al [20] in their research, viewed that biometrics has been extensively utilized to lessen the ATM-related crimes. One of the most widely used methods is to capture the facial images of the users for follow-up criminal investigations. However, this method is vulnerable to attacks made by the criminals with heavy facial occlusions. In today's scenario of banking operations, user identity protection, password protection is no longer safe to guard your personal information, in his paper [21], they tried to explain different types of vulnerabilities and loose points which are attempted at the time of financial operations and generates fraud transactions due to fake entries and fake cards which makes the ATM vulnerable.
According to [22], the use of ATM has newline grown rapidly in popularity because of its low banks transactions costs and customers newline convenience which has made it a basic element of today s financial service offering. However, newline the ATM which is meant to serve the customers better is now becoming a frightening for some newline customers because of fraud perpetuated in their accounts through ATM withdrawals. This newline unpleasant experience by customers is one of the challenges of the ATM through all over the newline world. As the ATM works without any human teller interactions It is designed with so many newline security features so that a costumer can perform banking financial transactions without any newline problem with secure transactions but remain there are some vulnerabilities are there which newline make the transaction unsuccessful and unauthorized transactions can be made using ATM .

Furthermore, [23] discussed that, attacks on Automated Teller Machines (ATMs) have become a major problem for ATM-vendors and banks. The most widely used attack method is the so-called skimming. During some of these skimming attacks fake keypad overlays are placed on top of the original ATM keypad. In their paper they proposed a method for the detection of fake keypads. To use the fake card, criminals also need the correct personal identification number (PIN). Until today, there are two methods in use to acquire the PIN: One uses a small camera to capture the keystrokes of a customer. The other one is based on a fake keypad (-overlay), that passes the keystrokes on to the real keypad, while capturing and storing the pressed keys.

According to [24], crimes related to automated teller machines (ATMs) have increased as a result of the recent popularity in the devices. One of the most practical approaches for preventing such crimes is the installation of cameras in ATMs to capture the facial images of users for follow-up criminal investigations. However, this approach is vulnerable in cases where a criminal's face is occluded. Therefore, this paper proposes a system which assesses the recognizability of facial images of ATM users to determine whether their faces are severely occluded.

As per [25], the most significant impact of ATM technology is the customer's ability to withdraw money outside banking hours. But this feat achieved by ATM technology is not without challenges. ATM technology is prone to fraud, and this has made many people shun its use. As suggested by [26], biometric authentication has a great potential to improve the security, reduce cost, and enhance the customer convenience of payment systems. Despite these benefits, biometric authentication

has not yet been adopted by large-scale point-of-sale and automated teller machine systems. [27] discussed that newly-emerging trend in facial recognition software uses a 3D model, which claims to provide more accuracy. Capturing a real-time 3-D image of a person's facial surface, 3D facial recognition uses distinctive features of the face -- where rigid tissue and bone is most apparent, such as the curves of the eye socket, nose and chin -- to identify the subject. These areas are all unique and don't change over time.

[28], defined the face that can identify is normal face. It is necessary for the person who wears these obstacles to prevent the use of ATM. As control the access of ATM, we can reduce the crime and increase the detection ratio of the normal face. According to [29], a Biometric Identification system is one in which the user's "body "becomes the password/PIN. Biometric characteristics of an individual are unique and therefore can be used to authenticate a user's access to ATM centers.

As per [30], the use of Biometric ATM's based on iris recognition technology has gone a long way in improving customer service by providing a safe and paperless banking environment. A biometric system provides automatic recognition of an individual based on some sort of unique feature or characteristic possessed by the individual. Biometrics gained lot of attention over recent years as a way to identify individuals. According to [31], in recent years the algorithm that the fingerprint recognition continuously updated has offered new verification means for us, the original password authentication method combined with the bio-metric identification technology verify the clients identity better and achieve the purpose that use of ATM machine improve the safety effectively.

It is very important that the face is at proper distance from camera or system, at proper angle and lighting is appropriate, otherwise distance from camera will reduce facial size and thus resolution of image. Facial-scan technology has unique advantage, over all other biometrics in the area of surveilling large groups and the ability to use pre-existing static image [32].

II. METHODS AND MATERIAL

The methodology adopted by this study was 'Internet Search'. The study consulted different sources on the Internet to establish evidence and facts about the claimed issues. Where possible the websites of the specific resource were visited, for example website of some journals which only put materials in html format rather than pdf or documents. The reviewed literatures are mostly available on the Internet. Another means employed is observations and where possible in some areas algorithm were developed to facilitate the discussion. So generally secondary source of data were mainly used in a large part to come up to conclusion.

III. RESULTS AND DISCUSSION

In the case of Tanzania especially Iringa Municipal, the facial recognition systems as an added security towards securing the transactions done at ATM will be difficult task for most of the users as it will prompt banks to every time recapture the images of the users due to either face fractures due to accidents or human violence which is now taking place in large part of the municipal and that leaves either part to be injured and then makes facial recognition system a difficult task.

The ATM system consists of camera embedded in machine that will recognize the face standing about 0.5m in front of system and perform matches against the facial database. The user usually starts with the ATM card as usual but must also have the PIN correctly remembered for pre verification before the facial scanning starts. The following is an algorithm to be used.

1. Starts
2. The user inserts an ATM card into the ATM slot
3. The user is asked for first time to enter the correct password/PIN for the inserted card
4. The machine verifies if the inserted PIN matches with the stored one in the database and if the inserted PIN is incorrect then the machine will prompt the user to reenter the correct PIN again and if again the entered PIN is incorrect then the machine will withhold the card and report to the bank officer before even going to the next step for facial recognition.
5. If the entered PIN in step 4 above is correct then the machine will prompt the ATM user to face the ATM embedded camera for capturing the image.
6. The machine then compares the captured image at ATM place and the one stored in the database if there is a match between the two, if there is no

match between the two images then the card will be withheld by the ATM and the report will be sent to the bank officer for further action.

7. If there is a match between the two images that is the one captured at ATM and the one stored in the database, then the user will be allowed to carry out the transaction he want to perform.
8. End.

The above algorithm shows that there is double authentication for the user before he/she is allowed to carry out any transactions, the first one is the normal one which we usually use for the carded ATMs but the second one is the tight biometric security system in which the user himself will be identified based on the information stored in the database, if there is a match for both of the security credentials supplied by the customer then the transactions will be freely opened.

In the decision box for matching the face by comparing the captured image and the stored one in the database, the following is done:

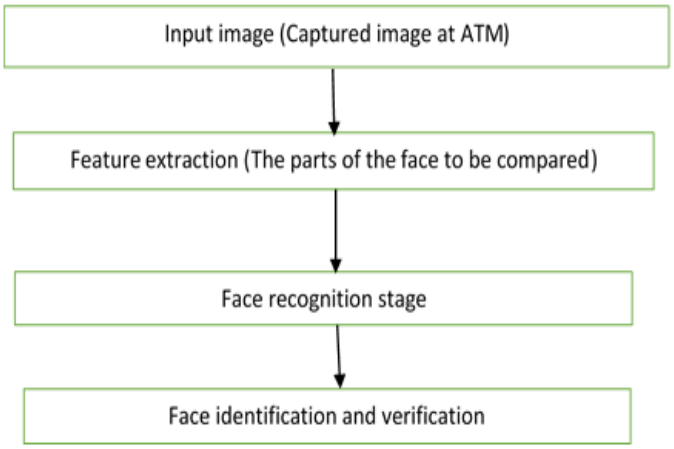

Figure 2: Face detection and verification flow diagram

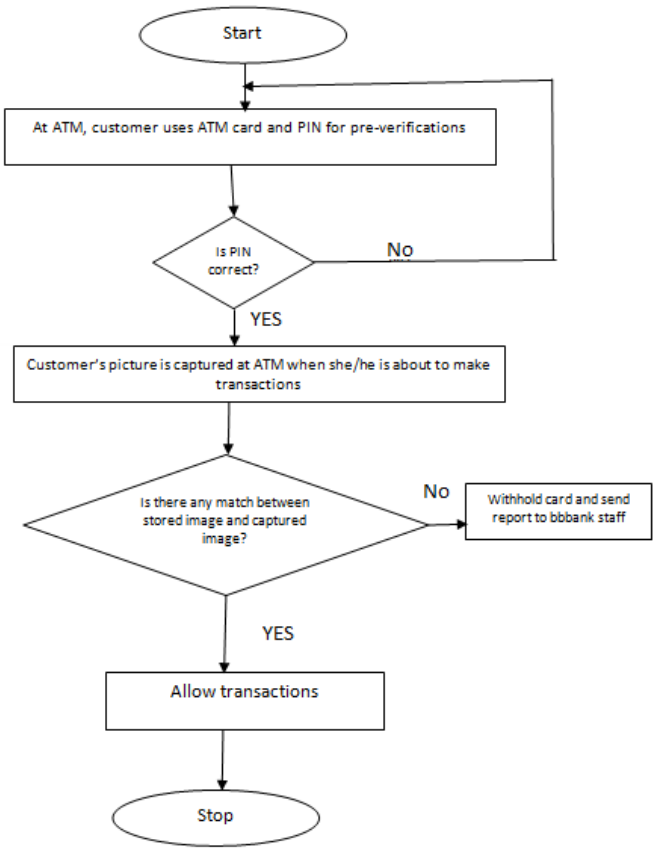

Figure 3: System flow diagram for the transactions made in ATM by the user after authentication.

Advantages of using Double Authentication

There will be great advantage to use double authentication for security purpose as one will be required to have both ATM PIN and his/her facial representations in order to have access to the transaction. This will dramatically reduce some card theft incidences as one may have the password/PIN of the card but will again be required to have facial match with the card owner. And in case there are two identical twins who are closely related to each other still the PIN will decide who us the real owner of the ATM card.

Disadvantages

In case the card owner gets accident or get injured in the face, then he will be prompted to go to the bank where his account details are stored in the database in order to change the image stored to match the current image.

In case customer have forgotten his password for the ATM card, then there will be no option rather than going to the respective bank where he firstly opened his account so as to have PIN reset.

IV. CONCLUSION

According to visited literature review which brings about the secondary data sources and some few primary data sources, it seems that there are potential threat posed to the ATM users either in robbery or in lost cards. The purpose of this study was to visit the literature in ATM security system and to propose one which will be more secure compared to the existing system. It was found that most of the visited literatures suggests that the use of ATM cards be suspended or totally discouraged while imposing new security system which will be more advanced compared to PIN based cards and the suggested system to be imposed is biometric security system either in finger print or facial recognition even though there are some challenges concerning facial recognition as a biometric security because of injuries which can occur to customer himself/herself.

A part from biometric security systems involving only facial, eye, iris and fingerprint, new biometric security can be used which is smell sensing from the mouth as everyone has natural smell from the mouth it will be easier to have unique identification except when one is drunk.

From above explanation, the author thinks that having both ways of logging in, in the ATM will be more safe than having only one way of accessing transactions, that is to say having PIN accesses and facial recognition login credentials creates more security as one have to pass both security barriers before having access to the transactions.

V. FUTURE WORK

In the future research must be conducted on the use of smell from mouth breathing as the second security for one to have access to transactions after passing the first security barrier that is PIN. And more often restrictions must be made on the users as warning before using ATM you are required to have your original smell because at the moment of taking or capturing your biometric information you were not drunk then the same must be applied to the ATM usage but if your information were taken while you were drunk then the same trend must continue when you need to access the ATM, it is a bit challenge.

VI. ACKNOWLEDGMENT

I would like to extend our appreciations to Dr. Silvano Kitinya and Carl Mmuni from Ruaha Catholic University (RUCU) for their support during the preparation of this paper and Ruaha Catholic University management and staff for encouragement they gave me during data collection, analysis and interpretation. Also I would like to thanks our childrens Neema and Nelson Lusekelo Kibona for being there all the time when I needed them

VII. REFERENCES

[1] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 43, pp. 90-98, 2000.

[2] A. Ogunsemor, "Banking services: The emergence and impact of electronic banking," The Nigerian Banker, pp. 2006-1781, 1992.

[3] A. S. Adepoju and M. E. Alhassan, "Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria–A Case Study of Selected Banks in Minna Metropolis," Journal of Internet Banking and Commerce, vol. 15, pp. 1-10, 2010.

[4] E. Derman, Y. K. Gecici, and A. A. Salah, "Short term face recognition for Automatic Teller Machine (ATM) users," in Electronics, Computer and Computation (ICECCO), 2013 International Conference on, 2013, pp. 111-114.

[5] S. M. Satone and G. Kharate, "Face detection and recognition in color images," IJCSI, p. 467, 2011.

[6] http://www.atmmarketplace.com/news/facial-recognition-coming-to-atms/.

[7] O. E. Aru and I. Gozie, "Facial Verification Technology for Use In Atm Transactions," American Journal of Engineering Research (AJER) e-ISSN, pp. 2320-0847.

[8] https://www.google.co.tz/search?q=face+recognition+systems+for+atm+images.

[9] http://www.nation.co.ke/News/Your%20face%20is%20all%20you%20will%20need%20at%20an%20ATM%20/-/1056/911432/-/3f6h2w/-/.

[10] K. Delac and M. Grgic, "A survey of biometric recognition methods," in Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium, 2004, pp. 184-193.

[11] M. Karovaliya, S. Karedia, S. Oza, and D. Kalbande, "Enhanced Security for ATM Machine with OTP and Facial Recognition Features," Procedia Computer Science, vol. 45, pp. 390-396, 2015.

[12] R. Ihejiahi, "How to fight ATM fraud online," Nigeria Daily News, p. 18, 2009.
[13] O. Odidison, "ATM fraud rises: Nigerians groan in Nigeria," Daily News, pp. 8-10, 2009.
[14] C. E. Anguelov, M. A. Hilgert, and J. M. Hogarth, "US consumers and electronic banking, 1995-2003," Fed. Res. Bull., vol. 90, p. 1, 2004.
[15] I. Diebold, "ATM fraud and security: White Paper," New York, 2002.
[16] S. Das and J. Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System," International Journal of Information and Communication, 2011.
[17] J. O. Adeoti, "Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out," Journal of Social Sciences, vol. 27, pp. 53-58, 2011.
[18] B. S. Raj, "A Third Generation Automated Teller Machine Using Universal Subscriber Module with Iris Recognition," image, vol. 1, 2013.
[19] K. J. Peter, G. Nagarajan, G. G. S. Glory, V. V. S. Devi, S. Arguman, and K. S. Kannan, "Improving ATM security via face recognition," in Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 2011, pp. 373-376.
[20] S. Eum, J. K. Suhr, and J. Kim, "Face recognizability evaluation for atm applications with exceptional occlusion handling," in Computer Vision and Pattern Recognition Workshops (CVPRW), 2011 IEEE Computer Society Conference on, 2011, pp. 82-89.
[21] N. Sharma, "Analysis of different vulnerabilities in auto teller machine transactions," Journal of Global Research in Computer Science, vol. 3, pp. 38-40, 2012.
[22] N. Sharma, "Analysis of vulnerability and security issues over auto teller machine transactions and design of a general security model," 2014.
[23] J.-F. Ehlenbröker, U. Mönks, and V. Lohweg, "Surface Fingerprint Detection."
[24] J. K. Suhr, S. Eum, H. G. Jung, G. Li, G. Kim, and J. Kim, "Recognizability assessment of facial images for automated teller machine applications," Pattern Recognition, vol. 45, pp. 1899-1914, 2012.
[25] G. N. Odachi, "ATM Technology and Banking System in West African Sub-Region: Prospects and Challenges," African Research Review, vol. 5, 2011.
[26] J. Breebaart, I. Buhan, K. de Groot, and E. Kelkboom, "Evaluation of a template protection approach to integrate fingerprint biometrics in a PIN-based payment infrastructure," Electronic Commerce Research and Applications, vol. 10, pp. 605-614, 2011.\
[27] S. Thorat, S. Nayak, and J. P. Dandale, "Facial recognition technology: An analysis with scope in India," arXiv preprint arXiv:1005.4263, 2010.
[28] S. M. Yoon and S.-C. Kee, "Detection of Partially Occluded Face Using Support Vector Machines," in MVA, 2002, pp. 546-549.
[29] S. Pravinthraja and K. Umamaheswari, "Multimodal Biometrics for Improving Automatic Teller Machine Security," Bonfring International Journal of Advances in Image Processing, vol. 1, pp. 19-25, 2011.
[30] K. L. N. Rao, V. Kulkarni, and C. K. Reddy, "Recognition Technique for ATM based on IRIS Technology."
[31] R. Rasu, P. K. Kumar, and M. Chandraman, "Security for ATM Terminal Using Various Recognition Systems," International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, 2012.
[32] E. Spinella, "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning," SANS Institute, San Francisco, CA, vol. 28, 2003.