IMPROVING SECURITY LEVEL OF ATM BANKING SYSTEMS USING BIOMETRIC KEY BINDING CRYPTOGRAPHIC TECHNIQUE

[1]NWABUEZE, C. A., [2]EKENGWU, B. O. and [3]MUOGHALU, C. N.
Department of Electrical/ Electronic Engineering, Chukwuemeka Odumegwu Ojukwu University, Uli.
[1]canwabueze@yahoo.com, [2]bekengwu@yahoo.com, [3]cnmuoghalu@yahoo.com

ABSTRACT
With rapid growth in the use of automated teller machines (ATMs), there is need to develop secure, robust and reliable schemes to securely/correctly authenticate users. The conventional ATM authentication schemes available are mostly cryptographic based and this gives room to lots of vulnerabilities. This paper presents an improvement on the conventional cryptographic security scheme currently used in ATMs by proposing the application of Biometric Key Binding (BKB) technique which fuses biometric security with cryptographic protocols on biometric template generated from input test images. The application of BKB not only protects the information of the user's biometric features, but also securely releases cryptographic key that is bound with biometric trait in a monolithic framework. The ease and protection provided by the proposed technique promotes improved security for widespread use of cryptographic systems. This technique provides high output entropy keys and also conceals original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is open to an attacker.

Keywords: *Biometrics, Encryption, Cryptography, Verification.*

1. INTRODUCTION
Personal identification is to associate a particular individual with an identity. This is critical to identification of an individual and occurs millions of times every day by hundreds of thousands of organizations in financial services, health care, electronic commerce, telecommunication, government, etc. With the rapid evolution of information technology, people are becoming more electronically connected. As a result, the ability to achieve highly accurate automatic personal identification is becoming critical. A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed by a legitimate user and not anyone else [1]. Nowadays, crimes at ATMs have risen exponentially. In Nigeria today, ATM identification is done with the use of Personal Identification Number (PIN) which is confidential. In such cases there is the possibility of hacking passwords and personal information and sometimes it is difficult to remember the PIN number [2]. The security of customer account is not guaranteed. As the Automated Teller Machines (ATM) technology is advancing, fraudsters are devising different skills to beat the security of ATM operations. Various forms of fraud are perpetuated, ranging from: ATM card theft, skimming, pin theft, card reader techniques, pin pad techniques, forced withdrawals and lots more. Managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences. In the absence of robust authentication schemes, these systems are vulnerable to the wiles of impostors.

Recognizing a person using passwords is not sufficient for reliable identity determination because they can be easily shared, or stolen. A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person

possesses. Advantages of using biometrics characteristics are reliability, convenience, universality and so on. History has proven that human beings can remember only short password, most of the users even tend to choose password that can be easily guessed using dictionary or brute force search. This limitation has triggered the utilization of biometrics to produce strong cryptographic key [3].

Biometric encryption is a Class of emerging "untraceable biometric" technologies that seek to irreversibly transform the biometric data provided by the user and it is a process that securely binds a PIN or a cryptographic key to a biometric features, so that neither the key nor the biometric can be retrieved from the stored template. The key is re-created only if the correct live biometric sample is presented on verification.

In this paper, an embedded crypto-biometric authentication protocol is proposed. The fingerprint image acquired from the user is encrypted in the ATM terminal for authentication. The encrypted image is then transmitted over the secured channel to the central banking terminal. In the banking terminal the fingerprint image is decrypted. The decrypted image is compared with the fingerprint templates. The authentication is valid if the minutiae matching are successful [4].

2.0 RELATES WORK

Duvey *et al.* [5], proposed a system which provides security to the ATM transactions that uses the Dyne-pass (Dynamic Password) in which the user accesses his account using debit card through ATM machine with the help of PIN. Then ATM machine reads this card and check the PIN with bank server through dedicated network. Bank server now connects to SMS center with a password called the Dyne Password (Dynamic Password). Then using mobile phone network SMS center send the password to Base Transceiver System (BTS). BTS then sends it to the users' cell phone. Finally, the users get the dynamic password and enter this password to the ATM machine. The ATM machine again confirms this dynamic password with bank server and then responds to banking instructions.

The Duvey *et al* also proposed biometric based ATM transaction system which is based on biometric data (fingerprint recognition, iris recognition, face recognition, etc). The proposed system uses biometric data with PIN number and if biometric data of the user is matched with stored biometric data, the user will be allowed to do the transaction or exit from the system.
Sudiro [6], when developing recognition system which is based on biometric feature there are some points which must be considered: universality, distinctiveness, permanence and collectability.

Ravikumar *et al.* [7], proposed the concept of fingerprint recognition PIN combination in ATM to make the ATM and ATM transactions more secure. Using fingerprint, users will be more relieved that their account can't be accessed by others and it will maintain the security level very account has two passwords (that is, PIN Number and fingerprints) of the card holder. The nominee fingerprints, or family member fingerprints are also used in case of emergency when actual card holder is unable to do the transactions.

In Santhi *et al* [8], a comparison is drawn between some existing works and enumerated a very serious shortcoming in most of the existing works as regards the use of biometric based systems. It was discovered that

fingerprint verification was the predominant biometric proposed for ATM authentication schemes and that no alternative was suggested if the biometric system fails.

To protect fingerprint images K. Zebbiche, et. al. [9], presented an efficient technique for use in fingerprint images watermarking. The underlying principle of the technique is embedding the watermark into the ridges area of the fingerprint images which represents the region of interest.

By combining asymmetric digital watermarking and cryptography, as powerful mechanism was proposed by Nick Bartlow, et. al., [10] to store raw biometric data in centralized databases. Jain and Uludag [11], introduced an amplitude modulation-based watermarking method in which they hide a user's biometric data in a variety of images.

3.0 METHODOLOGY

A very sophisticated approach to biometric encryption through biometric key binding based on fingerprints is shown in fig 1; the analytical model for biometric key binding technique is based on the works in Souter et al [12].

Basically this research adopts a secure method for consistently reproducing a digital key using a biometric, such as a fingerprint. The digital key is linked to the biometric only through a secure block of data, known as the protected filter or Bioscrypt.

The key cannot be released from the protected filter other than via the interaction with the correct biometric image. Once generated, the digital key is used in a system as an encryption/decryption key. This work aims at overcoming the need to carry, store, or remember private keys for encryption/decryption, or PIN's for any other application by deriving a digital key from a biometric, during a live verification process.

This biometric encryption model works on the existing algorithm for biometric key binding (BKB) based on the convolution of 2D fingerprints. This algorithm is based on the mechanism of correlation [2]. Many Biometric encryption schemes also store a hashed value of the key so that a correct key is released from the BE system only if the hashed value obtained on verification is exactly the same. Also, good practice would be not to release the key, but rather, another hashed version of it for any application. This hashed version can in turn serve as a cryptographic key. With this architecture, an attacker would not be able to obtain the original key outside the BE system.

The protected filter is generated by capturing at least one biometric image; obtaining transformed image information comprising transforming said at least one biometric image to a transform domain; generating a random phase-only function; obtaining a complex conjugate of the phase component of said transformed image information; multiplying said phase-only function with said complex conjugate to generate a phase-only filter; and storing a protected filter, said protected filter comprising said phase-only filter [12]; secure user verification, comprising the steps of: capturing at least one biometric image; obtaining transformed image information comprising transforming said at least one biometric image to a transform domain; obtaining magnitude information from said transformed image information; retrieving a phase-only filter from storage; applying at least said magnitude information to said phase-only filter to obtain a transitory filter with phase and magnitude information; multiplying said transformed image information with said transitory filter to obtain verification information; comparing said verification information with a retrieved reference pattern and, on obtaining a satisfactory match, providing a user verification signal.

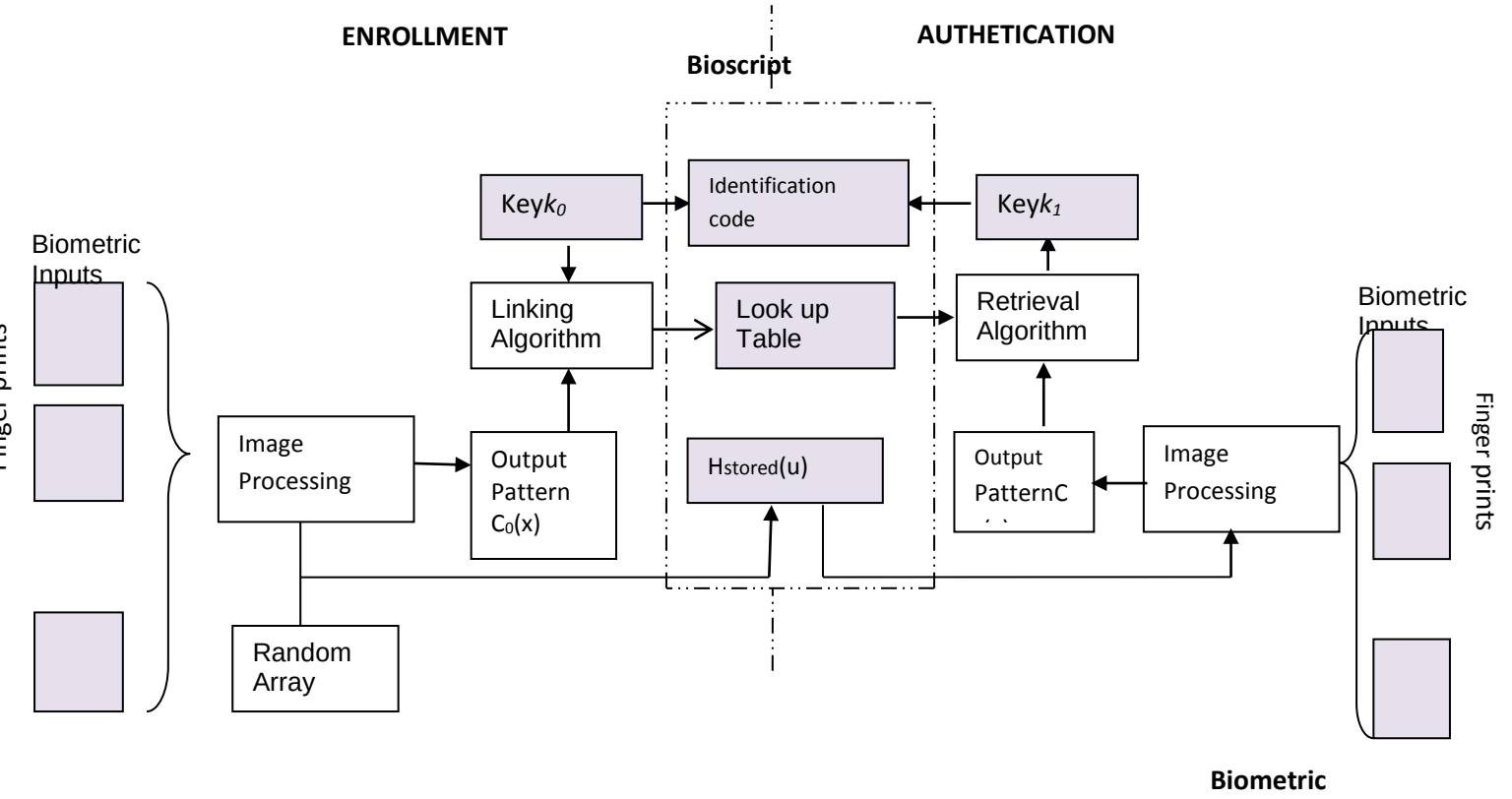

Figure 1: *A model for enrollment and verification in biometrically encrypted system [12]*

Enrollment Algorithm

En-1: processing of image

Combine a series of input fingerprint images from the Action Client (fingerprint training) with a random (phase) array to create two output arrays (product of the two): H_{stored} (u) and $c0$(x).

En-2: Key linking

Link a cryptographic key, k0, to the pattern, $c0$(x), via the link algorithm.

En-3: Identification code creation

Create an identification code, id0, derived from the key, k0.

The objective of the enrollment procedure is to link an arbitrary N-bit key to the user's fingerprint and create the user's Bioscrypt.

Verification/ Authentication Algorithm:

Ve-1: Image Processing

Combine H_{stored} (u), from the Bioscrypt, with a new series of input fingerprint images of the Action Client (also trained) to create an output pattern, $c1$(x).

Ve-2: Key Retrieval

Extract a key, k1, from $c1$(x) using the retrieval algorithm.

Ve-3: Key Validation

Validate k1by creating a new identification code, id1 and comparing it with id0.

The objective of the verification procedure is the successful retrieval of the N-bit key for a legitimate user.
A set of biometric images is acquired from the Action Client and combined with *H*stored(u), the lookup table, and id0, from the Bioscrypt, to retrieve and check the validity of an N-bit key. If this key is found to be correct, it will be passed on to the cryptographic system.

A Simple Analogy of Biometric Key Binding

0000 0101 = finger print at enrollment
\+ XOR/bit manipulation
1010 0101 = RNG generated by system
1010 0000 = stored value
\+ = XOR/bit manipulation
0000 0101 = fingerprint at verification
1010 0101 = RNG regenerated

A summary of enrolment and verification of the proposed system is shown in the algorithm below.

Algorithm 1: Enrollment of a costumer.

Input: a set of the legitimate Action Client's fingerprint images, a randomly generated phase-only array, *R*(u), and an N-bit cryptographic key, k0. *R*(u) is generated using a random number generator (RNG).

Output: an identification code id0 derived from key, k0.

Steps:

- Generate random phase-only array
- Generate N-bit cryptographic key.
- Collect a set of fingerprint images T=n, n>6(fingerprint samples).
- Perform Fourier transform the fingerprint image
- generate an output function $c_0(x)$ and filter function$H_{stored}(u)$(product of finger print and random array)
- store $H_{stored}(u)$)as part of Bioscrypt
- link c0(x)with N-bit key k_0 and create a look up table
- use k_0 to encrypt S-bits of $H_{stored}(u)$to form id_0
- *append* $H_{stored}(u)$*to* id_0 *and the look up able*
- *end*

Algorithm2: verification of the customer

Input: a set of the legitimate Action Client's fingerprint images. $H_{stored}(u)$, and an output pattern, $c1(x)$.

Output: an identification code id1derived from an N-bit cryptographic keyk_1 in which id1= id0, then k1= k0, with high probability and k1can be released to the system

Steps:

- Collect a set of fingerprint images T=n, n>6(fingerprint samples).
- Perform Fourier transform the fingerprint image
- Combine the new set of fingerprints with $H_{stored}(u)$and look up table and id0 to check for the validity of N-bit key
- Using $H_{stored}(u)$from Bioscrypt, , c1(x) is evaluated

- $C_1(x)$is used to retrieve N-bit key k_1
- use k_1 to encrypt S-bits of $H_{stored}(u)$to form id_1
- $id_1$is then compared with id_0, if id1= id0, then k1= k0, with high probability and k1can be released to the system
- else display verification failed message
- end

4.0 RESULTS AND NALYSIS

The proposed technique maybe used for implementation and produced unique identifier works more efficiently and uniquely in determining whether the person is authorized or not. The performance of the technique is evaluated in terms of FAR, FRR, AR or accuracy.

Experimental Result of the Existing ATM

The experiments reported in this paper have been conducted on the fingerprint images, DB3_B in FVC2004 each containing fingerprint images of size (128 *128) pixels. The database consists of 11 person each person has 4 images for finger

For each person 4 images have been used in the training phase and 3 images for test phase. Fingerprints are tested individually.

After a set of experiments have been conducted we found these results as shown in table 1.

It has been found that the maximum accuracy happened when using threshold of 4.0.

From the paper, they gave FAR of 15%, FRR of 14%, and accuracy of 14.5%.

Table 1: *Result of the Performance of the Existing System* [2]

Threshold	FAR (%)	FRR (%)	Average error (AR)
1.0	22	9	15.5
2.0	30	7	18.5
3.0	35	19	27
4.0	15	14	14.5
5.0	18	20	19
6.0	23	16	19.5
7.0	5	25	15
8.0	12	20	16
9.0	17	14	15.5
10.0	21	10	15.5
11.0	0	90	45

Experimental Result of New System

The experiments reported in this work have been conducted on the fingerprint images DB1_B in SecuGen Hamster containing fingerprint images of size (128 *128) pixels.

The database consists of 11 persons each person has 4 images for fingerprint capture, processed and stored in different location and each of them were been tested into 100 times. For each person 6 images have been used in the training phase and 4 images for test phase.

It has been found that the maximum average error happened when using threshold of 5.0 and 0.

We have done our experiments on windows 7, processor core i3 and RAM 6 GB to obtain average error and run time of 30 seconds.

They gave discrimination (FAR) of 2, distortion (FRR) of 7, and average error of 4.5%.

Table 2: Result of the Experimental New System

Threshold	FAR %	FRR %	Average error
1.0	20	6	13
2.0	27	0	13.5
3.0	29	7	18
4.0	15	12	13.5
5.0	2	7	4.5
6.0	19	12	15.5
7.0	4	22	13
8.0	12	19	15.5
9.0	18	10	14
10.0	15	12	13.5
11.0	0	70	35

Comparing the existing and the new system results, it has been found that the existing system gives its best result at threshold 4.0 with the false acceptance rate of 15% and false rejection rate of 14% and also the average error of 14.5% and run time of 90 seconds. While the new system has been found with bioscript technique using threshold of 5.0 which also gave the best results, it has an average error of 4.5%, distortions (FRR) 7% and 22% discrimination (FAR) and run time of 30 seconds showing that new system has less error than the existing system which makes it more secured and reliable for authentication and verification of users.

CONCLUSION

Both key binding cryptographic method and biometrics based identification have their shortcomings, yet biometric encryption system which combines biometrics and cryptography may provide another effective method to protect peoples' sensitive information. This system has been found to surpass traditional cryptographic systems, because, it is impractical for a person to lose his/ her biometrics, and also the biometrics are difficult to falsify or steal thus providing an efficient approach for concealing biometric templates.

The tentative results have portrayed the efficacy of the proposed approach in protecting the template by immutable cryptographic key. The concluding remarks about proposed technique are:

- performance does not rely on specific biometrics;

- Clean separation between impostor and genuine distribution;
- Even if the feature extractor is low, performance is accurate;
- Privacy is granted

REFERENCES

[1] Kumar, R., Singh, U. and Sharma, P. (2012), *Hybrid Biometrics for Enhancing ATM Security*, Army Institute of Technology, Dighi Hills, India.

[2] Ekengwu B.O. (2016), *Enhancing Automated Teller Machines (Atm) Security Using Biometric Key Binding Cryptography Technique*, M.Eng Dissertation submitted in COOU, Uli.

[3] Sharma, D. and Khurana, S. (2012), *Secure Personal Recognition System based on Hashes Keys*, International Journal of Advanced Science and Technology, Vol. 47, pp. 115 -122.

[4] Selvaraju, N. and Sekar, G. (2010), *A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm*, International Journal of Computer Applications, Vol. 3, No.6, pp. 5-9.

[5] Duvey, A.A., Goyal, D., Hemrajani, D. and Naveen, D. (2013), *A Reliable ATM Protocol and Comparative Analysis on Various Parameters with other ATM Protocols*, International Journal of Communications and Computer Technologies, Vol. 1, No. 56, pp. 92-97.

[6] Sudiro, S. A., Voine, M. P., Kusuma, T.B. and Maulana, C. (2007), *Simple Fingerprint Minuitiae Extraction Algorithm Using Crossing Number on Valley Structure*, International Journal of Advanced Science and Technology, Vol. 54, pp. 41-44.

[7] Ravikumar, S., Vaidyanathan, S. and Thamotharan, B. (2013), *A New Business Model for ATM Transactions Security using Fingerprint Recognition*, International Journal of Engineering and Technologies (IJET), Vol.5, No. 3 pp. 2041-2047.

[8] Santhi, B. and Ram, K. K. (2012), *Novel Hybrid Technology in ATM Security using Biometrics in JATTT*, Journal of Theoretical Applied Information Technology Vol. 37 pp. 2 - 9.

[9] Zebbiche, K., Ghouti, L., Khelifi, F. and Bouridane, A. (2006), *Protecting Fingerprint Data using Watermarking*, In Proceedings of the first NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06).

[10] Bartlow, N., Kalka, N., Cukic, B. and Ross, A. (2007), *Protecting Iris Images Through Asymmetric Digital Watermarking*, IEEE Trans. on Information Technology, Vol. 44, pp. 1300-1309.

[11] Jain, A. K. and Uludag, U. (2004), *Hiding Biometric Data*, Proceedings of the IEEE on Info. Tech., Vol. 25, No. 11.

[12] Soutar, C., Roberge, D., Stojanov, S. A., Gilroy, R. and Kumar, B. V. K. (1998), *Biometric Encryption – Enrollment and Verification Procedures*, In Proc. SPIE, Optical Pattern Recognition, I.X., Vol. 3386, pp.24-35.