January 22-24 2019

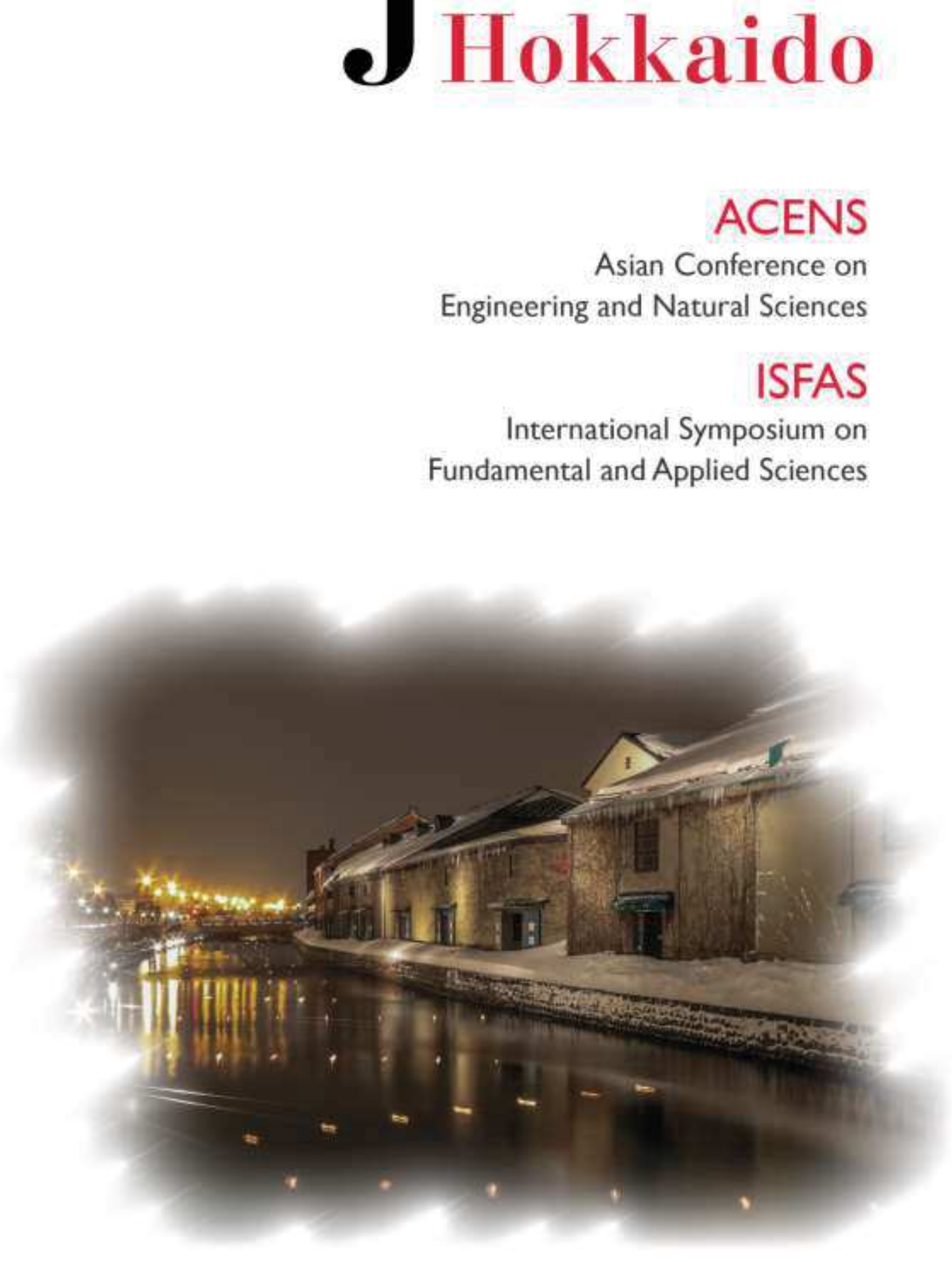
Japan Hokkaido

ACENS

Asian Conference on
Engineering and Natural Sciences

ISFAS

International Symposium on
Fundamental and Applied Sciences



ACENS-0295
Design and Implementation of Banking Authentication Process Using Fuzzy Vault

Narroup Rakngam[a,], Chaiyaporn Khemapatapan[b]
Department of Computer and Telecommunication Engineering, Faculty of Engineering,
Dhurakij Pundit University, Thailand
E-mail: thailandhsn@hotmail.com [a], chaiyaporn@dpu.ac.th [b]

Abstract

Today, online financial transactions via mobile phone become one of the most convenient channels in human lifestyle. However, one thing that comes up with it is the attacks on the banking system to steal our money in various ways. This research focuses on the design and development a new methodology for authenticating user in an online banking transaction via a mobile phone in order to enhance more security and to ease user for making a financial transaction. Multiple-Factor Authentication ("MFA") is a way for users to identify themselves to a service provider using at least two authentication methods. Traditionally, MFA can be done by authenticating 2 separated factors in cascade process manner. So we designed a combination of two-factor authentication such as OTP/Picture password or OTP/fingerprint by using fuzzy vault.

The experimental results show that the security of the login system which is applied with the proposed method using Fuzzy Vault is more secure than the security of the OTP system and suitable for position-based digital signature. It provides more easier registration, simple sign process and acceptable transaction verification.

Keywords: Fuzzy Vault, Multiple-Factor Authentication, authentication, fingerprint

1. Background

Technology plays a role in all aspects of our life including Banking & Financial Services. Mobile banking is one of the innovations that make life to be more comfortable. We do not have to queue for cash at ATMs or to go to bank office for doing a finance business. These are absolutely possible through mobile banking application at the touch on a smartphone. Table 1 shows the user of mobile banking in Thailand. The number of mobile banking in Q2 2018 increased by 33% and the increase in the number is causing many banks to invest in the development online services including effective internal control and security systems to provide customers with confidence in online banking transactions such as the authentication process. However, the convenience and speed adopted from mobile banking may be offset by the risk of data theft or stealing money from an online account.

Table 1: Description of the samples

	Q3/2017	Q4/2017	Q1/2018	Q2/2018
Number of Customer	28,442,453	31,634,571	34,503,696	37,973,421
Number of transaction (Thousand)	333,741	426,436	482,632	575,376
Transaction Value (Billion Baht)	2,368	2,874	3,203	3,641
				Ref: Bank of Thailand

Therefore, the purpose of this research is to make the process of an Internet and mobile banking systems to be more secure and reliable. Moreover, reducing the risk of customer data leakage or identity theft is also obtained.

Two-Factor Authentications (TFA)

TFA [1] or Two-Factor Authentication is a process for verifying identity using two factors as shown in Figure 1. It refers to 3 types of authentication

1) Something You Know, such as User ID and Password.
2) Something You Have, such as cards, approvals, etc., and
3) Something You Are Like, Finger, etc.

TFA is kind of traditional authentication used in many banking applications. The process is separated into 2 steps. Factors used in each step for authentication are also processed separately. Users have to verify theirs factors both steps. However, it can be noted that the factors of both steps are independent to each other. The examples of TFA can be found from [2], [3] and [4]. These examples followed to the TFA proposals but they have weaknesses such as device type unsuitable, hard to use, etc. Apache Milagro [5] [6] proposed Multi-Factor Authentication which provides a drop-in replacement for password-based authentication that is applicable to an online service. Multi-Factor Authentication (MFA) is a way for users to identify themselves to bank services using at least two authentication methods.

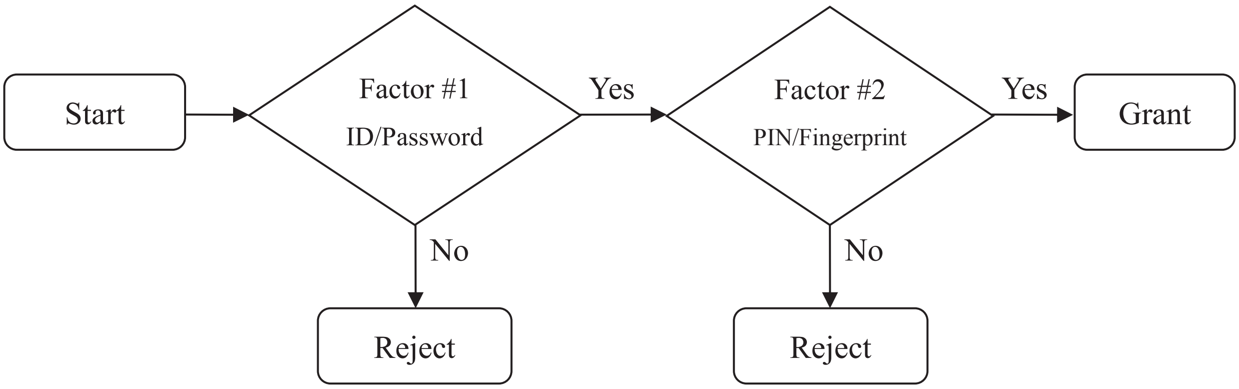


Figure 1: A traditional two-factor authentication

One Time Password (OTP)

OTP [7] or one-time passwords is one way to solve a password problem. The idea is that the password that is used to login changes all the time. Users have to provide a validated communication channel such as email or SMS over mobile phone system. Therefore, each time of making an important transaction, OTP will be generated by bank and sent to the user via the validated channel in order to authenticate.

2. Proposed Method

So, this work offers a conceptual design process. Use a picture password or fingerprint to encrypt the secret in the customer verification process. Design concept for the enrolling process using picture password/fingerprint to open an account and process encryption/decryption by using a key that is registered with the user's bank in the first step.

Process Open New Account

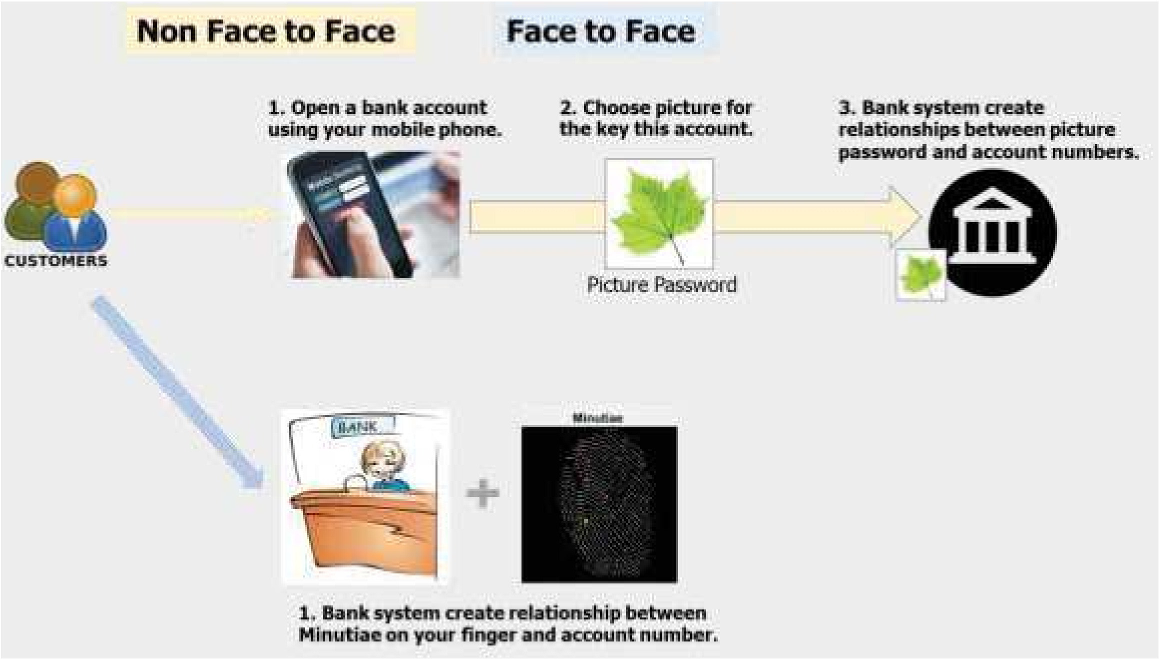

Non Face to Face
Face to Face
1. Open a bank account using your mobile phone.
2. Choose picture for the key this account.
3. Bank system create relationships between picture password and account numbers.
CUSTOMERS
Picture Password
BANK
Minutiae
1. Bank system create relationship between Minutiae on your finger and account number.

Figure 2: Enroll process for open an account

Concepts for designing an account opening process the system is divided into 2 parts as shown in Figure 2.

1) Account opening (Non-Face to Face) to control the process of opening an account user will select the picture to make the account key.

2) Account opening (Face to Face) For this part, the branch will store the minutiae on your fingerprints and create a relationship with your account.

The above process designs. It is a division of the system for management clarity. In addition, there is an important part of the design for the integrity of the system is the use of registered keys to take advantage. To make the system reliable is acceptable. Figure 3 shows that although the bank has an OTP process to confirm the transaction. It can be attacked by MITM. In this paper, we will find out how to encrypt the OTP before it is sent. Umut Uludag, Sharath Pankanti and Anil K. Jain [8] implement Fuzzy Vault scheme has been seen an application in biometric encryption.

Old Process

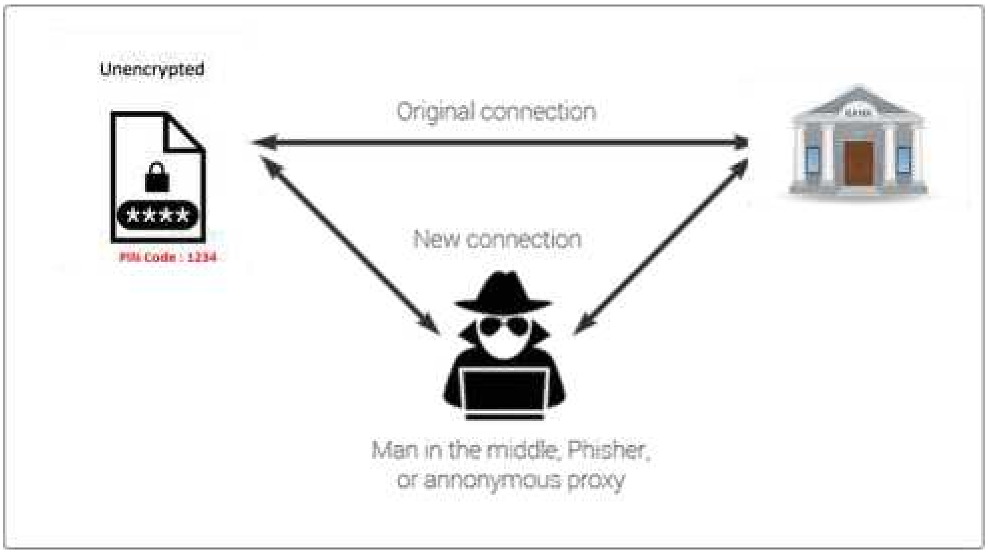


Figure 2: attacks OTP

New Process

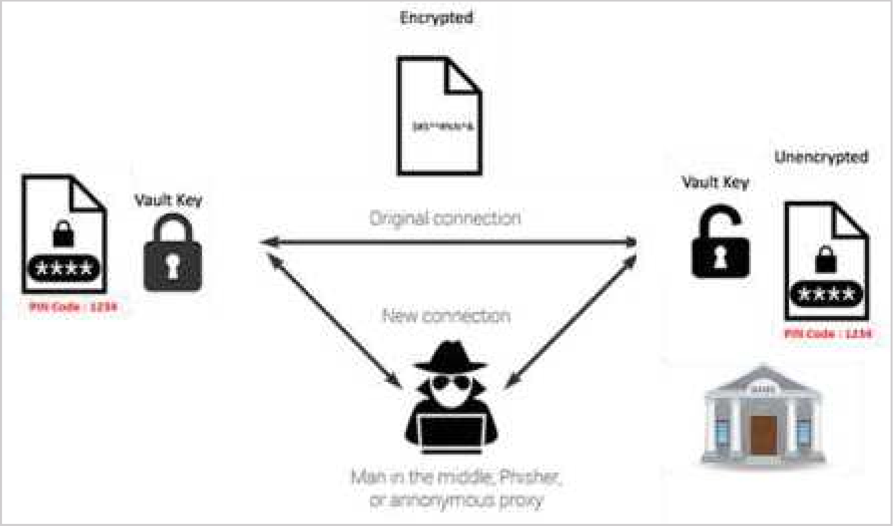


Figure 3: Concepts how to prevent.

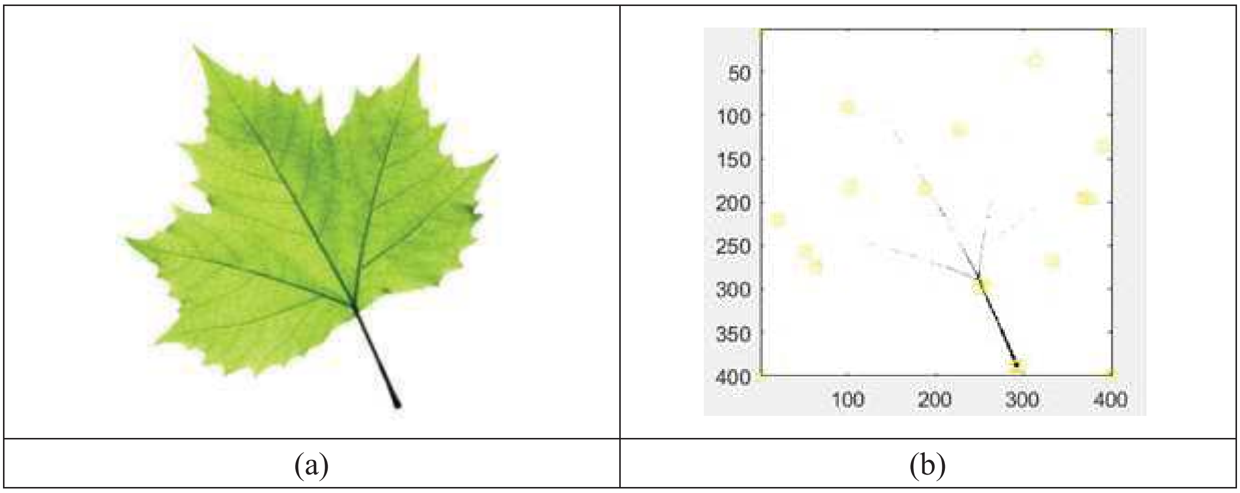
The process presented in this study encodes OTP using picture security/ fingerprint, in Figure 4, that user has verified with the bank since the opening of the account. So, even the victim will be intercepted. However, the hacker cannot view the data. Or even trying to attack Vault, OTP will expire, cannot use anything.

Extract Features Image

Corner detection algorithm [9][10] is an algorithm that helps to identify the corners in an image. Harris corner detector to accurately mark the position of the corner point takes a different corner of a score into the account with reference to the directional corner detection algorithm is the algorithm. Help to identify corners in the image.

Algorithm 1. Harris Corner Detection

```
Require: Input image $I$ parameter $k$,
Ensure: optimal $\alpha$ and $M$
Compute image gradient $I_x$ and $I_y$ for every pixel;
Compute the element in the Harris Matrix $H$
repeat Each pixel
    Define ROI of pixel by Gaussian filter
    Update Harris matrix $H$
    Compute eigenvalues of Harris matrix $H$
    Compute corner score of the pixel
until
Threshold corner score
Mark pixel as corner point for maximum corner score
```

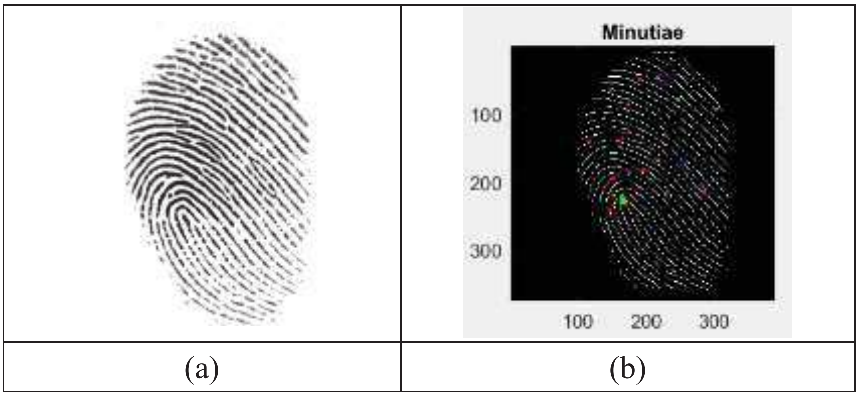


(a) (b)

Figure 4: Original Picture Password (a) Feature image (b)

Extract Features Fingerprint

The features of fingerprints which are ridge endings and ridge bifurcations. Minutiae and pattern are very important minutia in fingerprint analysis since no two fingers show the same. The design of a fuzzy vault using minutiae-based. We follow the approach proposed Rabia Bakhteri and Mohamed Khalil Hani [11].



(a) (b)

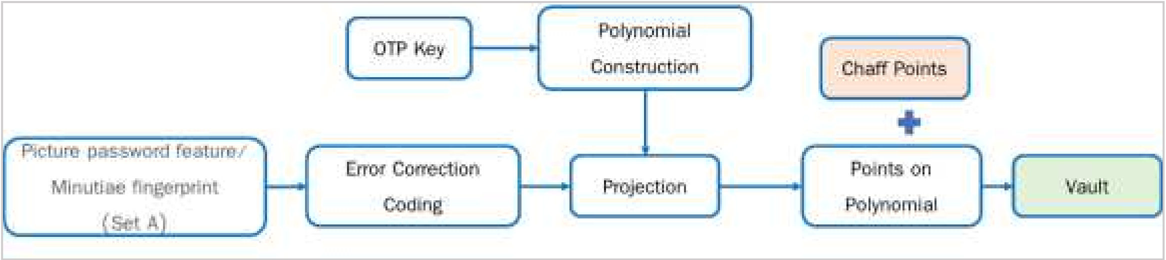
Figure 5: Original Fingerprint (a) Query Minutiae (b)

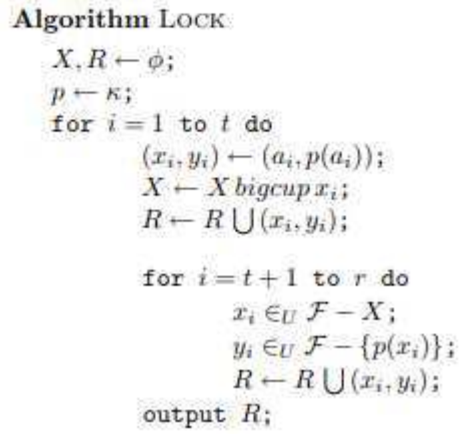
Fuzzy Vault

The fuzzy vault has been proposed by Juels and Sudan [12] in theoretical security analysis for the general fuzzy vault scheme by giving an estimate for the number of candidate polynomials that would fit with a given vault. The security of fuzzy vault scheme is based on the infeasibility of the polynomial reconstruction problem. These schemes deploy a variant of Reed-Solomon decoding and also hides the private user data among a large number of random chaff points. There are two operations in the fuzzy vault (Encoding and Decoding).

Encoding

A fuzzy encrypted process that creates a secure vault fuzzy template. This secret code (OTP Key) is hidden using biometric data/picture feature (Set A). The overall algorithm of fuzzy vault encoding is described below.



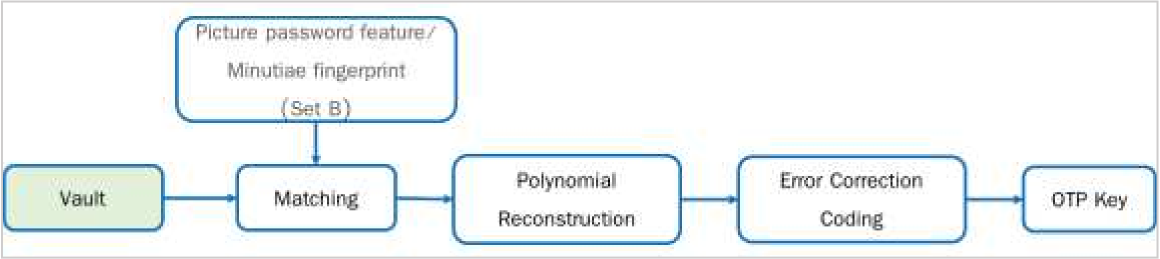


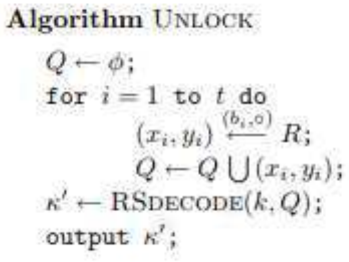
```
Algorithm LOCK
    $X, R \leftarrow \phi$;
    $p \leftarrow \kappa$;
    for $i = 1$ to $t$ do
            $(x_i, y_i) \leftarrow (a_i, p(a_i))$;
            $X \leftarrow X\, bigcup\, x_i$;
            $R \leftarrow R \bigcup (x_i, y_i)$;

            for $i = t + 1$ to $r$ do
                    $x_i \in_U \mathcal{F} - X$;
                    $y_i \in_U \mathcal{F} - \{p(x_i)\}$;
                    $R \leftarrow R \bigcup (x_i, y_i)$;
            output $R$;
```

Decoding

The decoding process for the Fuzzy Vault, as provided below, the minutiae coordinates are extracted from the query information in the bank.





```
Algorithm UNLOCK
    $Q \leftarrow \phi$;
    for $i = 1$ to $t$ do
            $(x_i, y_i) \xleftarrow{(b_i, o)} R$;
            $Q \leftarrow Q \bigcup (x_i, y_i)$;
    $\kappa' \leftarrow$ RSDECODE$(k, Q)$;
    output $\kappa'$;
```

3. Results

The results presented that the fuzzy vault is secure in the sense that it does not leak information about minutiae since it uses one-way hash and fuzzy vault scheme stores only a transformed version of the template, which makes it applicable to various modalities such as fingerprint, feature image. From tables 2 and 3, it can be seen that the time taken to find the minutiae is 4.92 seconds, which takes more time to find the feature image that takes 0.74 seconds. However, the computation time of the proposed system is too long. From both tables, the time taken to generate vault approximately 26 seconds.

Table 2: Fingerprint process / Vault / Decryption Time

Encryption			Decryption
No. of Finger	finding minutiae	vault	
80	4.916365 seconds.	26.81376 seconds.	0.404869 seconds.

Table 3: Image process / Vault / Decryption Time

Encryption			Decryption
No. of Pic.	Feature picture	vault	
100	0.741486 seconds.	26.97481 seconds.	0.384185 seconds.

Conclusion In this paper, we have design and implementation banking authentication process using fuzzy vault it changed the process from the original. The two factors authentication (TFA) factors used in each step for authentication are also processed separately to new process encrypted the factor (OTP) using fingerprint/picture password fuzzy vault, the experimental results show it helps to ensure that financial transactions occur. It's a real customer, but there is a risk if the customer makes more than one transaction and hackers have all transactional information. He can find the original point by comparing points from all received vaults. For future work we will add another process, especially in authentication stage and model calculation in chaff point generator.

4. References

[1] M. Benantar, Access control systems: security identity management and trust models, 2nd ed. Texas: Springer, 2006.

[2] "Aradiom SolidPass", http://www.aradiom.com/SolidPass.

[3] "FileID", http://www.fireid.com/.

[4] M. Hendry, Smart Card Security and Applications, 2nd ed. Washington D.C: Artech House, 2001.

[5] Masahiro Matsui, Hiroaki Ohtsuka, Tetsutaro Kobayashi, Hironobu Okuyama, Akira Nagai, and Go Yamamoto. *Milagro Multi-Factor Authentication*. NTT Technical Review, Vol. 14, No. 12, Dec. 2016

[6] Apache Milagro, Milagro - The Apache Software Foundation, http://milagro.apache.org/

[7] S. Garfinkel, G. Spafford, and A. Schwartz, Practical UNIX and Internet Security, 3rd ed. California: O'Reilly Media, Inc, 2003.

[8] Umut Uludag, Sharath Pankanti and Anil K. Jain "Fuzzy vault for fingerprints ". in Proceedings of Audio- and Video- based Biometric Person Authentication, Rye Town, NY, 2005.

[9] Dey, Nilanjan and; et al. (2012). "A Comparative Study between Moravec and Harris Corner Detection of Noisy Images Using Adaptive Wavelet Thresholding Technique". arXiv preprint. p. 1209.1558.

[10] C. Harris and M.J. Stephens. A combined corner and edge detector. In Alvey Vision Conference, pages 147–152, 1988.

[11] Rabia Bakhteri and Mohamed Khalil Hani. "Biometric Encryption using Fingerprint Fuzzy Vault for FPGA-based Embedded Systems ". in TENCON ,2009.

[12] A. Juels, and M. Sudan, “A fuzzy vault scheme”, Proc. Of IEEE Int. Symp. on Info. Theory, pp. 408, 2002