An Authentication Protocol for Secure Processing of ATM Systems by Fusion of Biometric and Crypt-Steganography Techniques

P.Anitha[1], M.Grace[2]

1 Department of Computer Science, Soka Ikeda College of Arts and Science for women,Chennai-99,India

2 Department of Computer Science, Soka Ikeda College of Arts and Science for women,Chennai-99,India

***Abstract*:** *Biometric authentication mechanisms are receiving a lot of public attention. Biometrics based authentication is a potential candidate to replace password-based authentication. This paper aims at developing a novel authentication protocol by fusion of Biometric and Steganography techniques for secure processing of ATM Systems. Visual Steganography provides a very powerful technique by which one secret can be distributed in two or more shares. During the enrollment phase in the bank terminal, the user has to enroll his/her fingerprint and finger vein and these enrolled biometric images are required to undergo certain processing and the resultant images are encrypted using RSA algorithm with a secret key and by using the visual steganographic technique, the encrypted secret key is shared between the two images. In the verification procedure, new finger vein and fingerprint images are obtained in the ATM terminals and after processing of the acquired biometric images, it will be decrypted by RSA algorithm using the same secret key and those are verified with the images stored in the bank's database. If matches with the database, then the user can carry out the money transactions and every user has three trials to access the ATM systems and if exceeds, the system will automatically logout the transaction. Since ATMs are now a normal part of daily life, the application of multimodal biometric techniques in every ATM Center's in our country, leads to reduce the stealing and forging and it is very useful for all the people.*

Keywords: *Biometric, Crypt-Steganography, RSA, fingerprint, finger vein, ATM systems*

I. INTRODUCTION

A. Biometrics

Biometrics is a technology that uses the unique pattern of physical or behavioral traits of users for authentication or identification. Uni-modal systems use single biometric trait for recognition suffer from several practical problems like noisy data, spoof attacks etc. Therefore multimodal biometric systems come to effect which make use of different biometric traits simultaneously to authenticate a person's identity [1]. Passwords have some drawbacks such as they could be stolen, lost or forgotten. In contrast, biometrics offers an alternative solution to the task of personal identification or authentication. There are various biometric traits for an individual like fingerprint, finger vein, iris, voice, face, ear and so on [2].

Nowadays, with rapid technological development, biometrics has launched a worldwide revolution in law enforcement. The Department of Defense and the FBI started working on the United States' next generation biometric system, named Next Generation Identification (NGI), which is designed to include fingerprint, face, iris, and palm data, and their facial recognition program became fully operational [3]. In order to prevent identity fraud and strengthen border and national security, many countries employ biometric systems to track and manage the flow of passengers across borders [4]. Generally, a typical biometric systems has four modules namely, sensor module, feature extraction module, template database and matching module [5].

B. Visual Steganography

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. In order to improve the security features in data transfers over the internet, many techniques such as Cryptography, Steganography etc., have been developed. Steganography is the art of hiding the existence of the communication message before sending it to the receiver. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another" [6].

Visual Steganography provides a very powerful technique by which one secret can be distributed in two or more shares as shown in Figure 1. When the shares on transparencies are superimposed exactly together, the original secret can be discovered without computer participation [7].

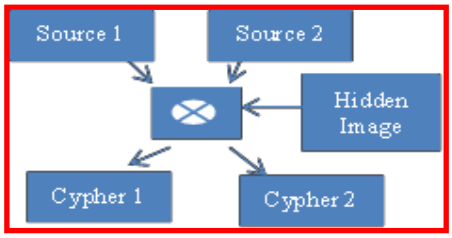

Fig .1. Visual Steganography

C. Cryptography

The word cryptography is derived from two Greek words which mean "Secret Writing". Cryptography is one of the most significant and a popular technique to secure the data from attackers by using two vital processes that is Encryption and Decryption. Encryption is the process of encoding data to prevent it from intruders to read the original data easily. This stage has the ability to convert the original data (Plaintext) into unreadable format known as Cipher text. The next process that has to carry out by the authorized person is Decryption. Decryption is contrary of encryption. It is the process to convert cipher text into plain text without missing any words in the original text. To perform this process cryptography relies on mathematical calculations along with some substitutions and permutations with or without a key [8].

These days, there are a number of algorithms have been available to encrypt and decrypt sensitive data which are typically divided into three types. Frist one is symmetric cryptography that is the same key is used for encryption and decryption data. Second one is Asymmetric cryptographic. These types of cryptography rely on two different keys for encryption and decryption. Finally, cryptographic hash functions using no key. The symmetric key is much more effective and faster than asymmetric. RSA algorithm is one of the most important algorithms to provide much more complexity and comparing the performance between the popular encryption algorithms to encrypt and decrypt data [9], [10].

II. Proposed Work

This paper consists of four modules such as Image acquisition and pre-processing of Finger vein, Image acquisition and pre-processing of Fingerprint, Enrollment phase at banking terminals and Verification phase at ATM terminals.

A. Image Acquisition and Pre- processing of Finger vein

The individuality of finger vein compared to other existing biometrics are, it isn't sensitive for environment conditions such as wet, dirt and it's a fraud-proof biometric, remains constant throughout the life, non-contact acquisitions etc. Finger vein authentication is a method that specifies an individual using the vein pattern inside one's fingers. Since de-oxy haemoglobin in the blood absorbs near-infrared lights, the vein patterns appear as a series of dark lines as shown in the Figure 2.

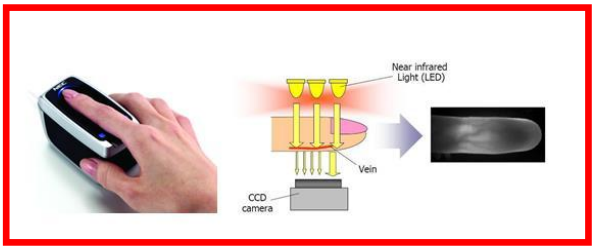

Fig 2. Image acquisition of Finger vein

After the finger vein raw image captured, it is required to preprocess the raw image. This involves image ROI detection, image enhancement and feature extraction. After the raw image captured, it is required to be preprocessed before feature extraction. The unwanted regions have been removed by choosing the interested area in the image called region of interest (ROI) as shown in Figure 3 (b) & (c) and can be done by extracting the centroid and then selecting an area around them [11].

Edge detection is an image processing technique for finding the boundaries of objects within images. Canny edge detection method is the best optimal algorithm among the edge detection algorithms [12]. It works by detecting discontinuities in brightness as shown in Figure 3 (d) and its fundamental criteria are low error rate and good localization [13].

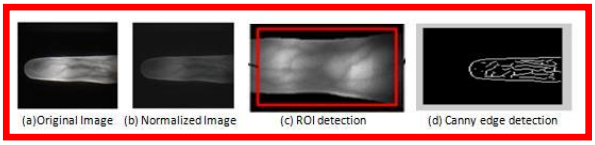

Fig 3. Processing of Finger vein

B. Image Acquisition and Pre- processing of Fingerprint

One of the most commercially available biometric technologies is fingerprint recognition, devices for laptop access are now widely available, users no longer need to type passwords instead, and only a touch provides instant access [14]. The fingerprint image contains minutiae points, core points, ridges and valleys, local features such as bifurcation, termination, bridge, hook etc. and global features such as core and delta and four types of patterns such as whorl, right loop, left loop and arch. The fingerprint images are captured by the sensor device as shown below in Figure 4.

Fig 4. Image acquisition of Fingerprint

In this paper, the image enhancement is done using intensity adjustment method based on the threshold and the threshold value decides how much intensity should be adjusted or not. Binarization process converts a grey level image into the binary image to improve the contrast between the ridges and valleys in a fingerprint image which leads to the extraction of minutiae. The Kernel PCA (Principal Component Analysis) is used for reducing dimensions of the fingerprint images rather than PCA. The Kernel PCA represents nonlinear mappings in a higher dimensional feature space and produced the better result with less error when compared to PCA [15]. A Gabor filter is used for edge detection and is applied to extract feature vectors which are used for the matching process as shown in Figure 5.

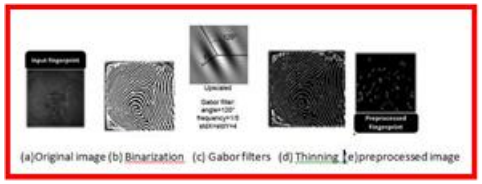

Fig 5. Processing of Fingerprint

C. Enrollment Phase at Banking Terminal

Enrollment and verification of authorized personnel are the important functions of the recognition systems. The recognition systems enroll authorized personnel based on the data provided by the biometric sensors and store the data for future verification or matching.

In this paper, during the enrollment phase, at the bank terminal, the user needs to register with the system by specifying their basic personal information such as name, email id, aadhaar number and his/her fingerprint and finger vein images. These enrolled biometric images undergo certain processing steps and then stored in the bank's database and it is necessary to keep the database in a secure manner. A cryptographic algorithm can be used to secure the database [16]. Here the AES algorithm is used along with a secret key to encrypt these biometric images. The aadhaar number can be used as the secret key. The encrypted fingerprint and finger vein images are stored in the bank's database for future verification. The enrollment phase is depicted in the Figure 6.

D. Verification Phase at the ATM terminals

In the verification or authentication phase, the user has to insert his/her ATM cards and to enter the PIN number. After entering the PIN numbers, the user's has to enroll his/her fingerprint and finger vein images by using high-resolution scanner at the ATM terminals. These enrolled images undergo certain processing and after the feature extraction, these images are verified with the images in the bank's database.

If the biometric images matches with the bank's database, the result shows the user is authorized person and then the user can carry out the money transaction else it will display as unauthorized person and the user can't carry out the money transactions which was shown in the Figure 7. Every user has three trials to access the ATM systems and if exceeds, the system will automatically logout the transaction.

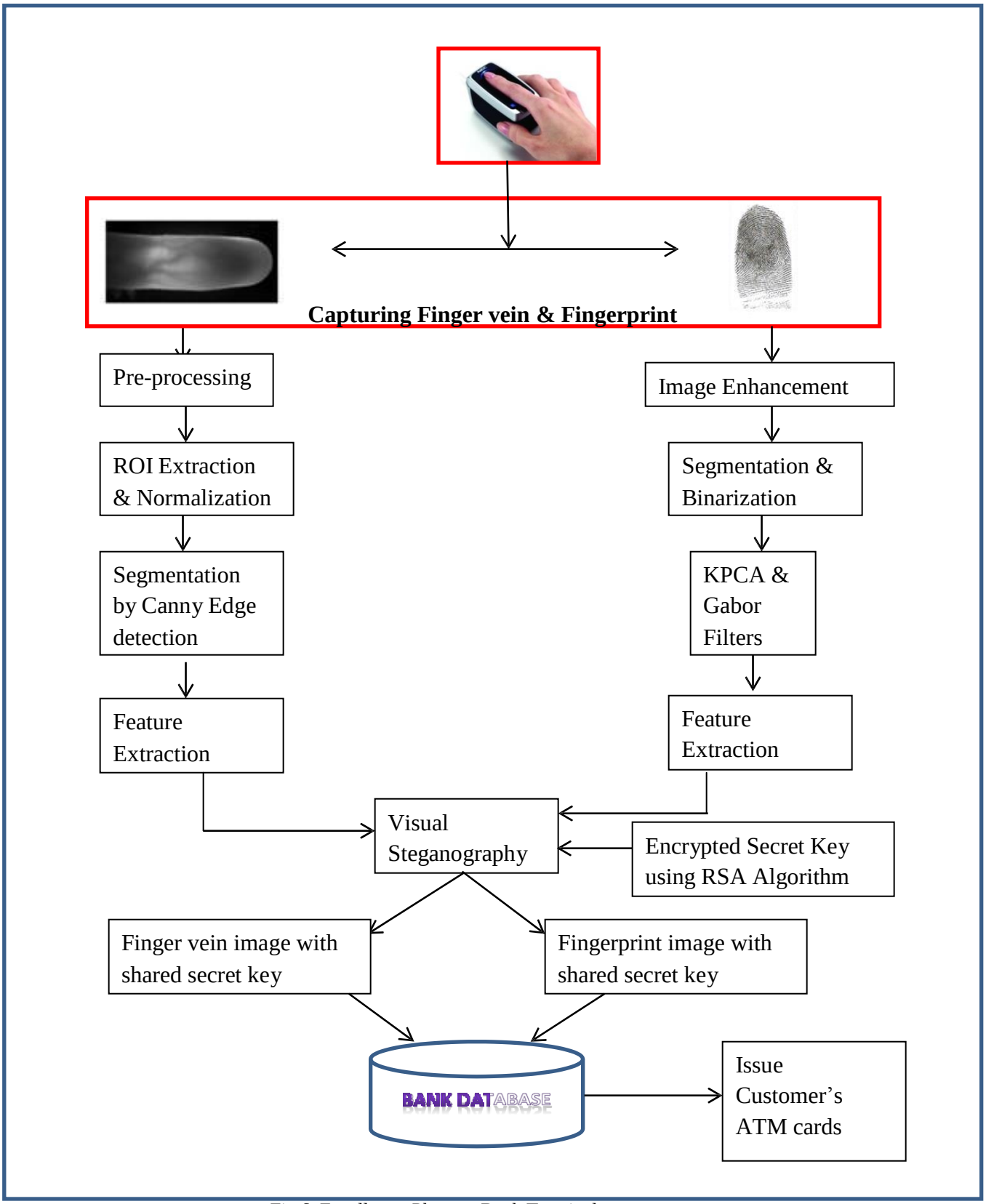

Fig 6. Enrollment Phase at Bank Terminal

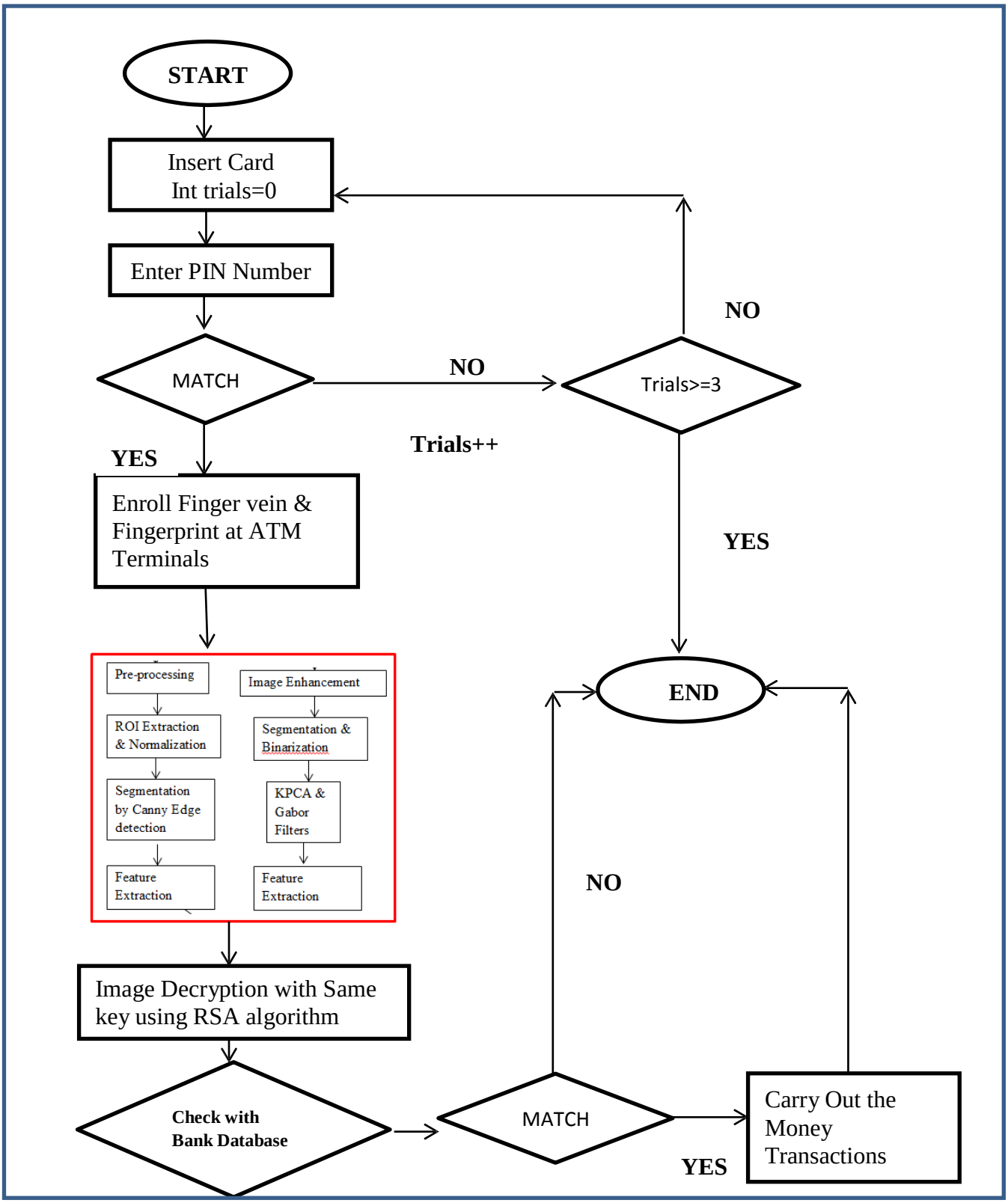

Fig 7. Verification Phase at ATM Terminal

III. Result and Discussion

The software used for the project is Matrix Laboratory (MATLAB). We are not using the finger vein scanner in this project because the scanner cost is too high so we are using a pre-data set to find authorized and unauthorized vein and fingerprint patterns (ie) we constructed a finger vein and fingerprint database for evaluation which contains images form 25 subjects. Here the finger vein and fingerprint images are collected and after some processing steps, that extracted images are encrypted with RSA algorithm using the customer's Aadhaar number as the secret key and the final encrypted images were stored in the bank's database. For verification process, the finger vein and fingerprint images are collected again and further processing were made and the processed images are again decrypted with the same RSA algorithm with the same key. Finally the obtained images are verified with the images in the bank database. If matches the customer can carry out the money transactions. If the user tries above three trials, the system will automatically log out the transactions. The processed images of finger vein and fingerprint are shown below in the Figure 8.

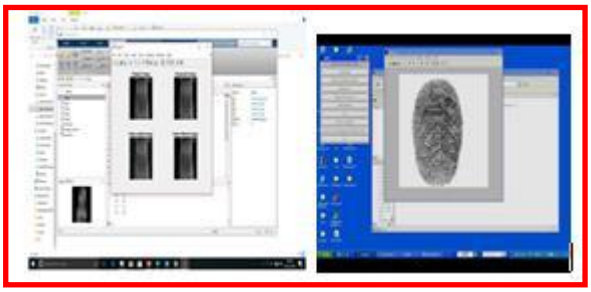

Fig 8. Finger vein and Fingerprint processing

After encryption the images of Finger vein and Fingerprint will be shown below in Figure 9 and stored in the bank's database,

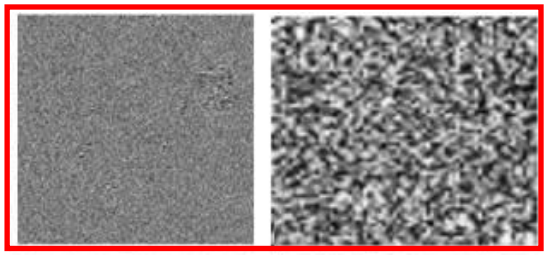

Fig 9. Encrypted image of Finger vein and Fingerprint images

For verification process, collect the finger vein and fingerprint images again in the ATM terminals and after some processing, those images are undergone decryption process and the images are shown in the Figure 10.

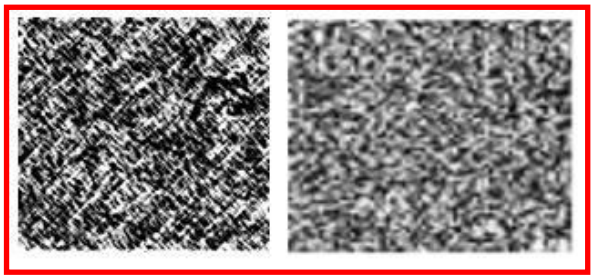

Fig 10. Decrypted image of Finger vein and Fingerprint images

Then those images are check with the bank database and if matches, it will produce the result as authenticated else not, which was shown in the Figure 11

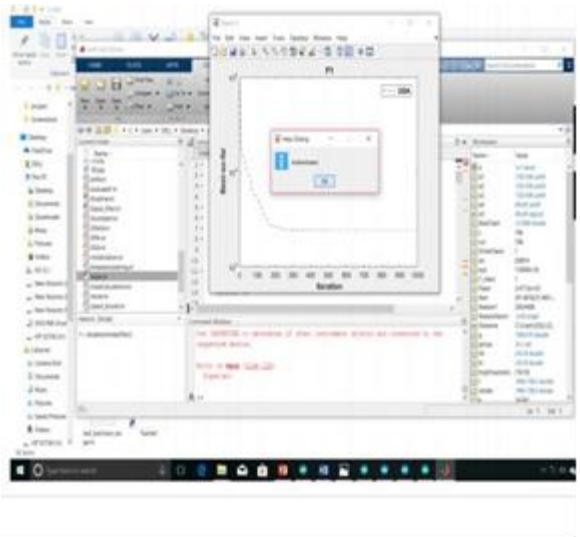

Fig 11. Authenticated

IV. Conclusion

PIN and Password are most common way of accessing ATMs for financial transaction but they can be forged and thus are subjected to attack such as phishing, spoofing etc. In order to overcome such attacks higher security is required. Biometric system is very useful as it employs biological features of an individual such as finger vein and fingerprint etc. In this paper, cryptography and multimodal biometric techniques are fused together for person authentication to ameliorate the security level in ATM systems. Since ATMs are now a normal part of daily life, the application of multimodal biometric techniques in every ATM Center's in our country, leads to reduce the stealing and forging and it is very useful for all the people

.

REFERENCES

[1] Hatim A. Aboal samh, *"A Multi Biometric System using combined Vein and Fingerprint Identification"*, International Journal of Circuits, Systems and Signal Processing, pp 29-36, Issue 1, Vol.5, 2011.

[2] Riaz, N.; Riaz, N.; Riaz, A.; Riaz, A.; Khan, S.A.; Khan, S.A. *"Biometric template security: An overview"*, Sensor Rev. 2017, 38, 120–127.

[3] The FBI Now Has the Largest Biometric Database in the World. Will It Lead to More Surveillance? Available online: http://www.ibtimes.com/fbi-now-has-largest-biometric-database-world-will-it- leadmore-surveillance-2345062 (accessed on 27 November 2018).

[4] U.S. Security Officials Will Begin Scanning All 10 Fingerprints of Most Non- Americans Traveling to the United States. Available online: https://travel.state.gov/content/visas/en/news/u-s--security-officialswill-begin-scanning-all-10fingerprints-.html (accessed on 27 November 2018).

[5] Anitha P, Grace M, *"Multimodal Approach on Finger vein and Fingerprint by using Visual Steganography for Efficient Biometric Security"*, International Journal of Computer Sciences & Engineering (IJCSE), E-ISSN:2347-2693, Vol 5,Issue 11,pp.140-145, November 2017.

[6] Neha Chhabra, *"Visual Cryptographic Steganography in Images"*, International Journal of Computer Science and Network Security, pp 126-131, Vol.12, No.4, 2012.

[7] K. Sankareswari, S. Arul Jothi, *"Hybrid Approach for Securing Biometric Templates Using Visual Cryptography"*, International Journal of Advance Research in Computer Science and Management Studies, pp 61-65, Vol.3, Issue 9, 2015.

[8] R.Saranya , S.Prabhu, *"Image Encryption using RSA Algorithm with Biometric Recognition"*, International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 11 Nov. 2016, Page No. 19149-19154.

[9] Shireen Nisha, Mohammed Farik, *" RSA Public Key Cryptography Algorithm – A Review"*, International Journal Of Scientific & Technology Research, Volume 6, Issue 07, pp. 187-191, July 2017.

[10] Joseph Mwema, Michael Kimwele, Stephen Kimani, *"A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates"*, International Journal of Computer Trends and Technology (IJCTT) ISSN: 2231-2803 – Volume 20 Number 1,pp.12-18, 2015.

[11] Humairah Hamid, V.K. Narang, Priti Singh, *"Review on Vein Pattern Based Biometric Systems"*, International Journal of Innovative Research in Science, Engineering and Technology, Vol.6, Issue 5, 2017.

[12] A. L. Kabade, *"Canny edge detection algorithm"*, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), 5(5):1292-1295, 2016

[13] Kayode A. Akintoye, M. Rahim M. Shafry, Abdul Hanan Abdullah, *" A Novel Approach for Finger Vein Pattern Enhancement using Gabor and Canny Edge Detector"*, International Journal of Computer Applications (0975 – 8887), Vol.157, No 2, 2017.

[14] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng and Craig Valli, *"Security and Accuracy of Fingerprint-Based Biometrics: A Review"*, Symmetry, January 2019.

[15] Mohammad Mohsen Ahmadinejad, Elizabeth Sherly, *"A Comparative Study on PCA and KPCA Methods for Face Recognition"*, International Journal of Science and Research (IJSR), ISSN: 2319-7064, Vol. 5, Issue 6, 2016.

[16] Shaik Riyaz Ulhaq, Shaik Imityaz, Selvakumar, L.Gopinath, *"Multimodel Biometric Template Authentication of Fingervein and Signature using Visual Cryptography"*, International Journal of Engineering and Techniques, Vol. 3, Issue 3, 2017.