International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

RESEARCHERID
THOMSON REUTERS

[Rohith *et al.*, 10(1): January, 2021]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

FACE RECOGNITION TECHNIQUE FOR ATM SECURITY

Rohith. R[*1] & Harshitha R[2]

[*1]Lecturer, ECE Department, Vidyavardhaka Polytechnic, Mysore,
[2]Assistant Professor, ECE Department, GMIT, Mandya

DOI: https://doi.org/10.29121/ijesrt.v10.i1.2021.6

ABSTRACT

In the recent decades the people are depending more on ATM machines for getting instant cash in anytime and anywhere. In related to these ATM machines are installing in every part of the country. As the ATM machines are growing, providing security level for ATM machines is the challenging factor. In the present days, ATM systems uses access card and PIN for identity verification. The technology advancement has bought different biometric identification technique like finger print, facial recognition and retina scanning. But still the security level is not compromising to customers. This model proposes a concept of providing two level security system in order to reduce the frauds like hacking of ATM cards, PIN stolen, Phishing attack etc., In this model Crypto-biometric system is adopted where biometric and cryptography are combined to achieve high security. Between face features and pairs of random vectors given by user, the two dimensional quantization of distance vectors process is used [1]. The cryptographic key generated is of 128 bits it is difficult for hacking. The merging of face features and random vectors are done by using MATLAB.

KEYWORDS: ATM, Biometric, Cryptography, Face recognition, PCA, Xilinx.

1. INTRODUCTION

Nowadays science and technology is growing more and more, the future innovations are being develop with high security. But however the hackers are also being increasing to distract this security level. Automated Teller Machine (ATM) is implanting in every part of the cities and also in rural areas due to speedy development in banking technology. This will creating positive impact and also negative impact on people. The existing ATM machine can be access by using a card and Personal Identification Number (PIN) given to customer. This will be act as one way authentication for banking security. By providing these level of feature for banking Hacking is possible from phishing attack, stolen cards, due to temporary assigned PIN or by duplicate cards and various other techniques. Hence single level of security is not sufficient for existing ATM model.

To overcome this problem, a hybrid model is designed which consists of Biometric authentication technology. It is method of positive identification of a subjects related to humans such as biometric signatures, this cannot be lost, forgotten, stolen or sharing with others. Biometric techniques are based on human subjects like finger print, face recognition, voice, iris, skin etc., [6] Cryptography is the method of generating written codes which keeps information secret. In Cryptography, unreadable format is generated from given data where it cannot be decode by unauthorized user. This converted data is allowed to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

2. INTRODUCTION ABOUT AUTHENTICATION

Biometric is an authentication systems used to verify or identify human identity by using physical, measurable and physiological or by behavioral characteristics like finger print, iris, face, skin, voice, signature, retina, DNA, hand geometry etc.,

- Fingerprint – It depends on unique patterns present in the tip of the finger.
- Iris – This biometric is related to features of colored rings of tissue present in the pupil of human eye.
- Face – This biometric is of facial recognition features which can be obtained by capturing from high resolution cameras.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

- Signature – This biometric analyze the way of signature style. Signing features such as velocity, speed and pressure are as important as the finished signature's static shape.
- Hand Geometry – This biometric involves scanning and measuring the shape of the hand.
- Retina - A retina-based biometric involves analyzing the layer of blood vessels developed at the back of the human eye.
- Voice – This biometric involves voice recognition process, where it performs voice to print authentication i.e. voice is converted to text.

Face Recognition System (FRS)

FRS is tool that physically identifies a human face by digital image of the face or video of face outline captured from a video camera. FRS technique involves the process by comparing captured facial features with the stored facial features database.

There are three types of FRS technique

- **2-D technique**- In 2-D technique, 2 dimensional features of the people's face can be seen, this is shown in Figure 1. Features can be extracted by considering distance between two eyes, width of the eyes, dimension of nose, width of the jaw like, cheek dimensions etc.,

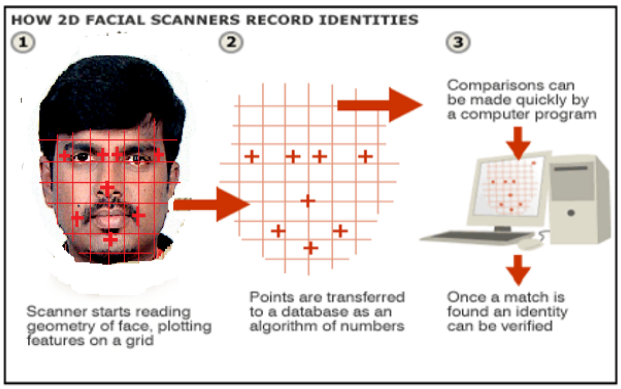

Figure 1: 2-D FRS technique

- **3-D technique**- The accuracy of face recognition can be improve further by using 3D image which is shown in Figure 2. This technique has better viewing in facial appearance like eye sockets, nose, chin, indifferent angle.

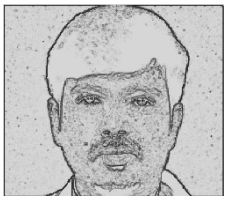

Figure 2: 3-D Image

- **Surface texture analysis**- It is more complex in face recognition technique. It takes the patch of the Skin from face and broke them into smaller blocks as shown in Figure 3. From these blocks using wavelet transform algorithm features are extracted. [4]

Figure 3: Surface texture analysis image

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

3. METHODOLGY

This design is introduced to increase the security level of existing ATM model. It uses Crypto-biometric technique where cryptography and biometric are combined to obtained high security. Face recognition is used as biometric and 16 digit alphanumeric code word is used as PIN for cryptography. This 16 digit PIN is set by account holder not by bank person or computer generated PIN. By this the security level is increased more so that the PIN cannot cracked by second person. Xilinx ISE design suite is an embedded software used to view the encoded and decoded bits then it can be interface to the ATM vault. We use a MATLAB tool to generate the miniature features of the face. The face recognition process consists of three stages as shown in Figure 4,

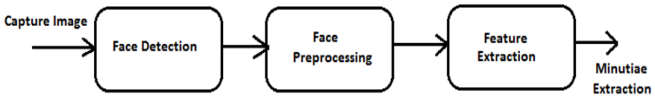

Figure 4: Face recognition process

Face Detection – The main function of the face detection is to localization of the face in the image capture by using high resolution webcam or camera as shown in Figure 5.

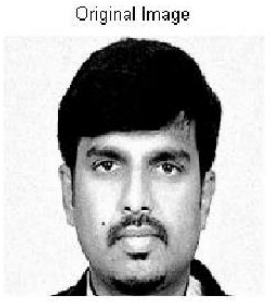

Figure 5: Image captured from camera

Face Preprocessing - The face preprocessing involves the step that to normalize the coarse face detection, so that a strong feature extraction can be achieved. Face preprocessing includes,

- **Binarization-** In Binarization process the grey scale image is converted into binary image because the binary image is easy to process. For this conversion it involves Recursive Otsu method [7]. This algorithm performs comparison of pixel value with the threshold value. If the pixel value is more than threshold value it converted into white pixels and if it is less than or equal to threshold value it converted into black pixels as shown in Figure 6.

Figure 6: a) Original Image b) Image after Binarization

- **Central line thinning** – Once binary image is obtained, the next process is to thin the image it is performed by using central line thinning algorithm. There are 23 templates defined for thinning algorithm. By considering any one of these templates the algorithm decides which pixels to be kept same and which pixel to be converted to white pixels and result obtained is a thinned image.
- Dilation involves the process of smoothing the given images. Holes and edges in the images are filled to get smooth image in dilation process.
- Thinning of dilated image it is done by using central line thinning image algorithm
- After thinning next process is removing unwanted portions from image which is not necessary for further

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

processing, if portions are exist it may cause invalid minutiae detection. Generally 20 to 25 pixels are present in these portions.

Feature Extraction- The final stage of the FRS technique is Feature extraction. Here it extract the photometrical and geometrical interpersonal discriminating features of the face as shown in the Figure 7. It involves the algorithms for minutiae feature extraction are Principal Component Analysis (PCA) or Linear Discriminate Analysis (LDA) [3]

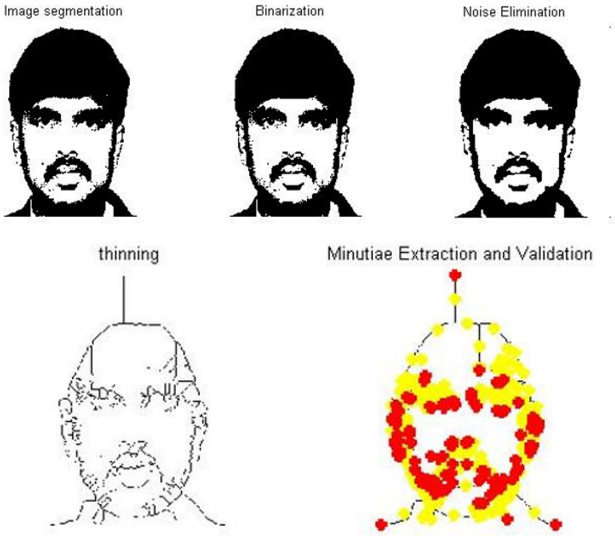

Figure 7: Different stages for Face preprocessing

After the template face miniature feature is extracted, it is merged with the 16 digit secret, it is done by Encoding stage

Encoding

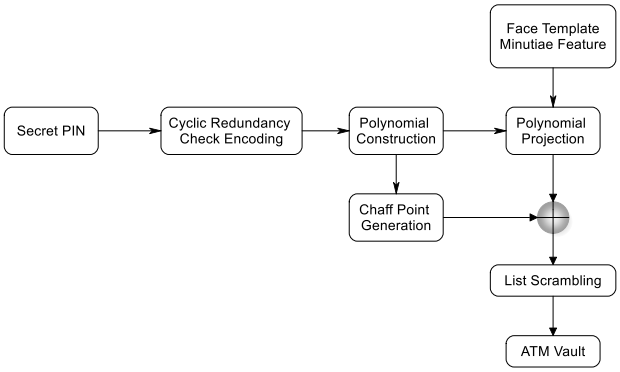

Figure 8: Encoding Stage

The encoding stage involves capturing face image of the user and it is converted into biometric feature. And also 16 digit PIN is set by the user is converted into randomly generated 128 bit. A 128-bit is the cryptographic key that needs to be secured and it is combined with the biometric feature. In order to recover the key from the ATM vault, cryptographic key is encoded using method called cyclic redundancy check [CRC]. The CRC-16 polynomial, $G_{crc} = a^{16}+a^{15}+a^{2}+1$ is used for CRC generation. This CRC-16 is appended to 128-bit random bit to generate 144 bit (Kcrc) code which is used for construction of ATM vault security[2].

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

An polynomial degree of 8, $P(x) = C_8 x^8 + C_7 x^7 + ... + C_1 x^1 + C_0$ is selected for binding with 144 bit (Kcrc)code and biometric feature b_i, i=0,1,2,3…M. The 144 bit polynomial can be divided into nine non overlapping 16 bit segments and every polynomial bit is mapped to coefficients C_0-C_8. Note that, this mapping method should be same for encoding and decoding operation. Because these are again mapped back to decode the secret CRC data which is identified as decoded co-efficient data (Ci).

By using each binary minutiae x_i, the polynomial P(x) is calculated, where x_i is an integer number corresponds to binary feature b_i.

Then Genuine set G is generated has a set of data pair $[x_i, P(x_i)]$ where, I =1,2…M.
By using this Chaff points set C is generated
i.e, $C=\{(a_j, b_j), j=1,2….Nc\}$ where Nc >>M and $a_j \neq x_i$

These pair should not fall on polynomial i.e $b_j \neq f(a_j)$.
The final vault set is constructed by taking the union of two set (GUC) and it is passed through the list of scrambler which randomize the list, that are used as chaff points V = (v_i, w_i) where, i= 1,2,….M+Nc. This scrambler list is stored in ATM vault. The stage each operation is shown in Figure 8.

Decoding
The decoding stage involves the process of accessing ATM using biometric features. When the user wants to access ATM his/her face image is captured by the same pixel camera used at encoding stage and generates the biometric feature bi*, by using this feature it search matches with ATM final vault V.

Windowing process is applied to overcome the error occur due to noisy biometric feature. The captured biometric image bi* is preprocessed to obtain 2D image plane by dividing into two 8 bit sets related to x and y direction. ATM scramble points stored in the vault falls on the ±w window in the image plane are treated as valid candidate points. A set S is formed by considering all valid candidate points which are identified and falls on the ±w window. The number of pairs in set S is denoted by K, for the reconstruction of a polynomial of degree D, total number of (K,D+1) combinations are identified for D+1 points.

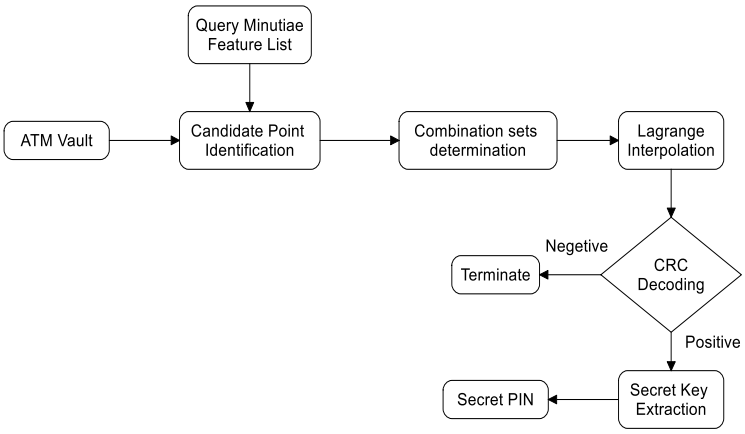

Figure 9: Decoding Stage

For each combination Lagrange Interpolating technique is adopted for recovering polynomial. For a specific set of combination
we have, L = { (v1,w1), (v2,w2), …..(v_{D+1} ,w_{D+1}),
then the polynomial can be constructed as

$$P^*[x] = \frac{(x-v2)(x-v3)\ldots\ldots\ldots(x-vD+1)}{(v1-v2)(v1-v3)\ldots\ldots\ldots(v1-vD+1)} w_1 + \frac{(x-v1)(x-v3)\ldots\ldots\ldots(x-vD+1)}{(v2-v1)(v2-v3)\ldots\ldots\ldots(v2-vD+1)} w_2 + \ldots\ldots\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + \frac{(x-v1)(x-v2)\ldots\ldots\ldots(x-vD)}{(vD+1-v1)(vD+1-v2)\ldots\ldots\ldots(vD+1-vD)} w_{D+1}$$

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

The co-efficients in the generated polynomial are mapped back to the decoded secret CRC code (K*crc). Error in this generated code can be check by dividing the polynomial corresponding to CRC code K*crc by CRC polynomial Gcrc = $a^{16}+a^{15}+a^2+1$. If the remainder obtained is zero, then there is no errors. The cryptographic key K can be taken out by considering the first 128 bits of K*crc.

4. RESULTS AND DISCUSSION

The results obtained from the proposed work and output of the developed system under various condition using Xilinx is discussed in this section. Firstly the face feature is obtained by the reference image using MATLAB tools and it is merging with the 16 bit alphanumeric secret key. To enhance the performance of the project we conducted our experimented on 100 different set of faces on different subject. Some of samples which contains the coefficient values of image and secret key generated for different set of data can be viewed through Xilinx and data are tabulated in the Table 1. The Figure 10 & 11 shows the graphical representation CRC decode data, polynomial values for different set of Images.

TABLE 1 : Coefficent values of different images

Co-efficents /Data Samples	coeff_val	xcrd_dec	xploy_val1	ycrd_dec
	[59116,4630,41251,18825,28108,61664,55858,36184,42604]	[242,184,178,131,189,95,135,211,147]	[416,864,256,224,1696,1984, 736,144,1]	[162903588;355901324;381157044;189855114;366996864;258070034;129652878;242706976;256683898]
	[20102,13107,1929,36314,18155,58916,64314,56733,1670]	[245,135,160,137,175,172,151,121,164]	[1728,859,921,899,1681,1339,41,179,1]	[115265571;87853798;111981350;204639090;224185718;254917922;240882838;198751698;247084330]
	[20102,62259,10153,3546,1771,26148,31546,40349,1670]	[246,57,131,79,97,164,168,230,243]	[1648,1397,89,93,1041,1717,1929,173,1]	[181909852;160077160;111717822;76137020;104926840;135250730;173172478;98879228;200558485]
	[44710,37651,51081,19930,18155,9764,47930,56733,26246]	[170,60,147,165,225,204,175,110,246]	[1792,1272,1969,857,1921,313,1089,217,1]	[62571856;80118226;250605166;220132826;167417695;313989474;203681686;20823876;194929500]
	[44710,21267,59305,52698,1771,42532,15162,40349,26246]	[245,240,88,105,86,90,112,216,99]	[1056,496,1536,176,416,256,1696,236,1]	[253781827;33969206;282434254;275183106;224185260;47705856;186976166;225973870;224780238]
	[28326,45875,18313,3546,50923,42532,64314,56733,26246]	[232,245,222,226,233,231,242,211,218]	[576,1968,224,432,976,1168,1824,232,1]	[342107022;142150691;255061476;326069352;322056111;250943321;148773656;246809969;306494208]
	[28326,29491,26537,36314,34539,9764,31546,40349,26246]	[80,70,103,97,100,104,121,112,149]	[1680,1379,1161,699,1041,1619,1321,139,1]	[15872566;41006076;120834646;163743384;406114 6;220414126;152888306;179917734;193063450]

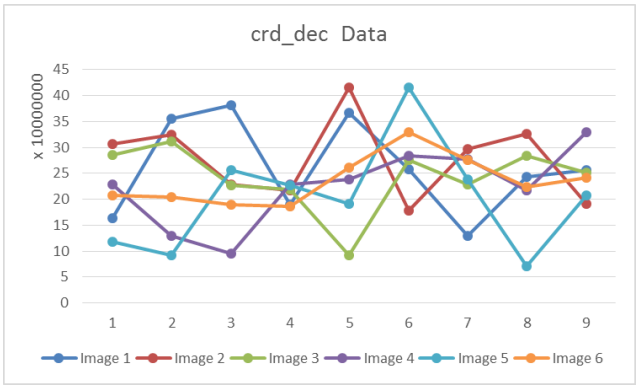

Figure 10: CRC data for different Image

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

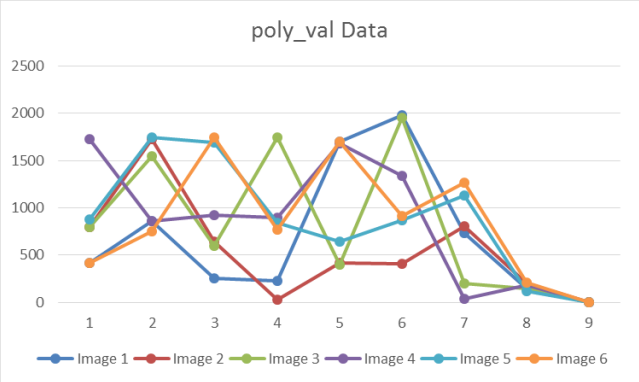

Figure 11: Polynomial variable for different images

5. CONCLUSION

ATM security is improving further by using crypto-biometric technique where cryptography and face biometric are merged. It replaces password based authentication into biometric based authentication. The secret key or PIN will be set by the user not banker or computer. This key is of 16 digit alphanumeric digits will be encrypted into 128 bits, which makes impossible for memorize for hackers. Crypto-biometric process provides two level security for the ATM user so that hacking of PIN can be reduced. By adopting two dimensional technique for face recognition it can implemented on low cost. This technique is more efficient than fingerprint biometric to provide ATM security.

REFERENCES

[1] Y. Wang and K. N. Plataniotis, "Fuzzy Vault for Face Based Cryptographic Key Generation," 2007 Biometrics Symposium, Baltimore, MD, 2007, pp. 1-6, IEEE
[2] Umut Uludag, Sharath Pankanti and Anil K Jain, "Fuzzy vault for Fingerprints" Proc. of Int. Conf. on Audio and Video based BiometricPerson Auth., pp. 310-319, 2005
[3] Mohsin Karovaliya and Saifali Karedia, "Enhanced security for ATM machine with OTP and Facial recognition features", International Conference on Advanced Computing Technologies and Applications, - 1877-0509 © 2015 ICACTA
[4] T.Suganya, T. Nithya and B. Meena Preethi, "Securing Atm By Image Processing – Facial Recognition Authentication", International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882
[5] N. Anusha, A. D. Sai and B. Srikar, "Locker security system using facial recognition and One Time Password (OTP)," 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2017, pp. 812-815,IEEE
[6] S. Kar, S. Hiremath, D. G. Joshi, V. K. Chadda and A. Bajpai, "A Multi-Algorithmic Face Recognition System," 2006 International Conference on Advanced Computing and Communications, Surathkal, 2006, pp. 321-326, IEEE
[7] Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme" Proc. Of IEEE Int. Symp. on Info. Theory,pp. 408,2002
[8] S. Liu and M. Silverman, "A practical guide to biometric security technology," in IT Professional, vol. 3, no. 1, pp. 27-32, Jan.-Feb. 2001, IEEE
[9] Nana Kwane Gyamfi and Kwaku Nuamah Gyambra, "Enhancing the security features of Automated Teller Machine", ISSN 2221-0997
[10] Moses Okechukwu Onyesoluand and Ignatius Majesty Ezeani, "ATM Security Using Fingerprint Biometric Identifer: An Investigation Study", International Journal of Advanced Computer Science and Applications, Vol. 3, No.4, 2012, IJACSA
[11] https://www.latestlaws.com, June7, 2018, Husband cannot use Wife's ATM card, Court agrees with SBI
[12] Avni Mittal, Shubhani and Sarika Tyagi, "Security of ATM Using Digital Image Processing", IJIACS ISSN 2347 – 8616, Vol. 2, No.4, 2014.