International Journal of Engineering & Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-3444

International Journal of Engineering and Technology Volume 2 No. 11, November, 2012

Development of Crypto-Biometric E-Banking System

A.O. Afolabi, Adigun A.A
Department of Computer Science and Engineering,
Ladoke Akintola University of Technology, Ogbomoso. Nigeria

ABSTRACT

The Internet has played a key role in changing how we interact with other people and how we do business today. As a result of the Internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The challenges that oppose electronic banking are the concerns of security and privacy of information. It is not enough for an e-banking system to just provide information to their customers but to provide it to the right customers and at the right time.

This project focuses on developing a secured e-banking system using encryption and face recognition as the two levels of security mechanism since the username and password security mechanism are easily breached by mere guess work. This E-banking system was designed using MATLAB as well as face recognition and encryption.

Keywords: *Biometrics, Encryption, E-banking*

1. INTRODUCTION

Electronic banking, also known as electronic funds transfer (EFT), is simply the use of electronic means to transfer funds directly from one account to another, rather than by cheque or cash. Many banks and other organizations are eager to use this channel to deliver their services because of its relatively lower delivery cost, higher sales and potential for offering greater convenience for customers.

This project is going to focus on providing a better means of security and this is biometric technology using facial recognition security mechanism, therefore the project is about creating an e-banking system whose security mechanism will be facial recognition.

Biometrics technology has been proposed to strengthen authentication mechanism in general by matching a stored biometric template to a live biometric template.

Cryptography provides the necessary tools for accomplishing secure and authenticated transactions. It not only protects the data from theft or alteration, but also can be used for user authentication.

2. REVIEW OF RELATED WORKS

E-banking is the provision of information about a bank and its services via a home page on the World Wide Web (WWW). Electronic delivery of services means a customer conducting his transactions from a remote location (e.g. home) rather that visiting a local branch. In the mid eighties, online banking arrived.

In its early form 'online banking services' requiring a computer, modem and software provided by the financial services vendors. Generally, these services failed to get widespread acceptance due to high call costs and unfriendly system interfaces, and were discontinued by most providers.

Overall, e-banking seems to serve as a complementary means of interacting with customers rather than a substitute for other channels such as physical branches. Despite the large investment in the Internet as a distribution channel, the branch network remains an important channel for retail banking products (Hernando & Neito, 2007).

Biometrics technologies are defined as automated methods of identifying or authenticating the identity of a living person based on unique physiological or behavioral characteristics (smart card alliance, 2005). Physiological biometrics is a physical measurement such as the verification of a fingerprint, hand eye of face. Behavioral biometrics takes a measurement of how an action takes place, such as a signature (Bolle, 2004). In order for a measurement to qualify as a biometrics, the certain requirements must be met (Parbhakar and Jain, 2003).

Automated face recognition is a relatively new concept. Developed in the 1960s, the first semi-automated system for face recognition required the administrator to locate features (such as eyes, ears, nose, and mouth) on the photographs before it calculated distances and ratios to a common reference point, which were then compared to reference data. In the 1970s, Goldstein, Harmon, and Lesk

used 21 specific subjective markers such as hair color and lip thickness to automate the recognition. In 1988, Kirby and Sirovich applied principle component analysis, a standard linear algebra technique to the face recognition problem. This was considered somewhat of a milestone as it showed that less than one hundred values were required to accurately code a suitably aligned and normalized face image.

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into ciphertext, which will in turn (usually) be decrypted into usable plaintext.

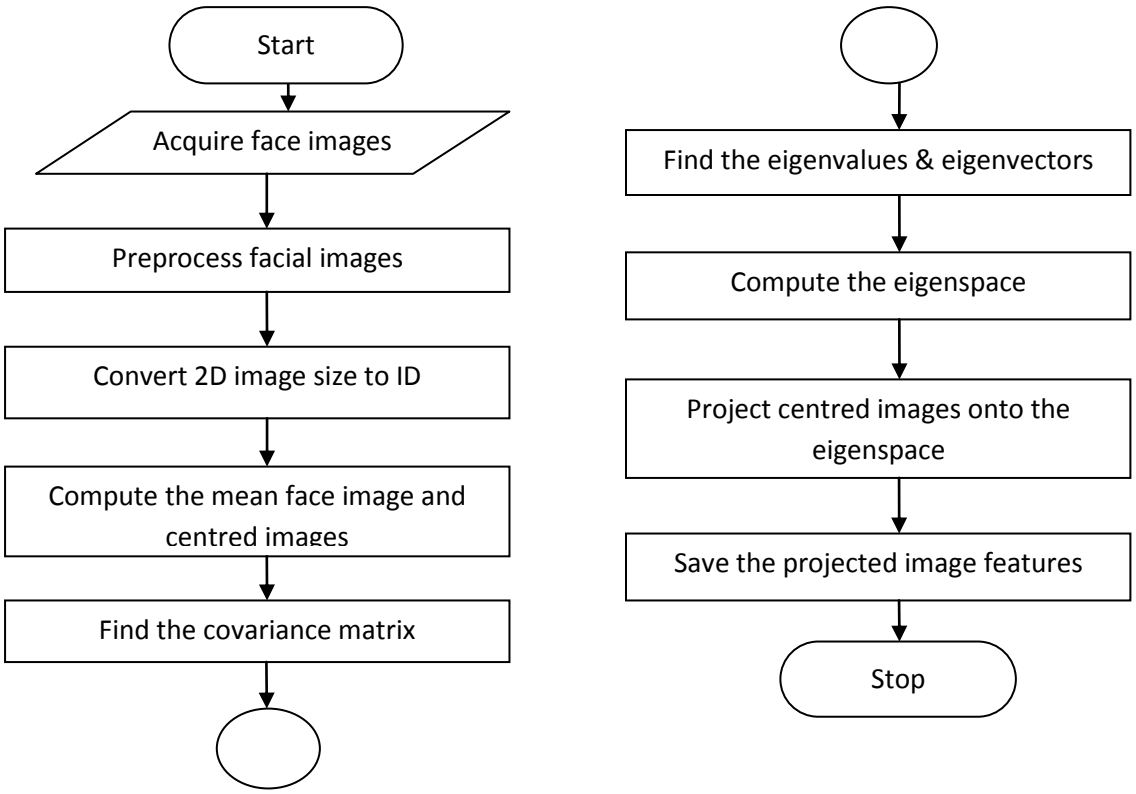
Principal Component Analysis (PCA), commonly referred to as the use of eigenfaces, is the technique pioneered by Kirby and Sirivich in 1988. With PCA, the probe and gallery images must be the same size and must first be normalized to line up the eyes and mouth of the subjects within the images. The PCA approach is then used to reduce the dimension of the data by means of data compression basics and reveals the most effective low dimensional structure of facial patterns. This reduction in dimensions removes information that is not useful and precisely decomposes the face structure into orthogonal (uncorrelated) components known as eigenfaces. Each face image may be represented as a weighted sum (feature vector) of the eigenfaces, which are stored in a 1D array.

3. METHODOLOGY

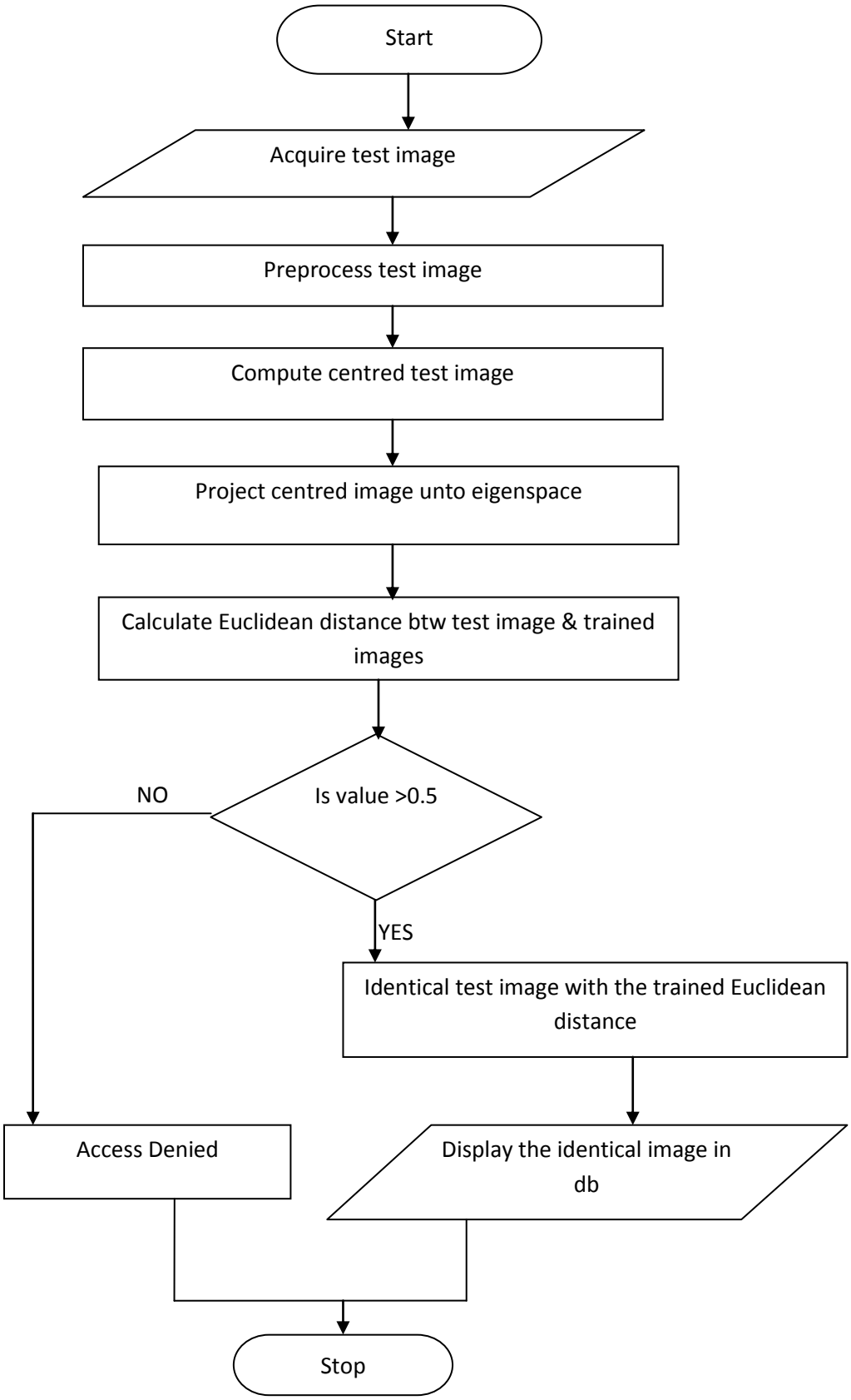
3.1 Image Acquisition Scheme

A database of facial images of individuals (representing a bank's customers) was created. Each individual has 4 images of samples of different facial expressions. The image database was trained using the PCA technique and the features are saved for recognition purposes. The bank registers a new customer by acquiring the customer's facial images of different expressions and then adds the images to the ones in the database after which the database is retained using the PCA and the features saved for future use. MATLAB was used throughout the development of this application.

3.2 PCA Flowchart



PCA Image Training Process



3.3 Data Security Algorithm

The data encryption and decryption algorithm used is the RSA algorithms which are shown in algorithms 1 to 5. To decrypt an information the alphabets and digits (0 to 9)

are represented by their respective numbers as shown in the Table1 3.1

Table 3.1: Alphabets and Digits represented by their representative number

Alphabet	Code	Alphabet	Code	Alphabet	Code
A	0	W	22	s	44
B	1	X	23	t	45
C	2	Y	24	u	46
D	3	Z	25	v	47
E	4	a	26	w	48
F	5	b	27	x	49
G	6	c	28	y	50
H	7	d	29	z	51
I	8	e	30	0	52
J	9	f	31	1	53
K	10	g	32	2	54
L	11	h	33	3	55
M	12	i	34	4	56
N	13	j	35	5	57
O	14	k	36	6	58
P	15	l	37	7	59
Q	16	m	38	8	60
R	17	n	89	9	61
S	18	o	40		
T	19	p	41		
U	20	q	42		
V	21	r	43		

A string of characters is first broken into blocks of 3 and the message representative integer for each block is computed. Each block of 3 characters is represented in base 8. For example, the representation of a string "Lautech 12" is as follows:

Lautech12= Lau tec h12
Lau= $11*8^2 + 26*8^1 + 46*8^{0=}$ 958
tec= $45*8^2 + 30*8^1 + 28*8^{0=}$ 3148
h12= $33*8^2 + 53*8^1 + 54*8^{0=}$ 2590

Then, the integer values 958, 3148 and 2590 are encrypted using the RSA algorithm.

Algorithm 1: Encrypting a message

1. Begin
2. Form the encoded message block EB
3. Convert the string EB to an integer m m= string ToInteger(EB)
4. Encrypt with the RSA algorithm s= m^d mod n
5. Convert the resulting signature value, s to block OB OB= IntegerToString(s)
6. Output OB
7. End

Algorithm 2: RSA Key Generation

1. Begin
2. Generate prime numbers, nP between 1 and 20,000

3. Select the primes p & q such that n= pq and Ø= (p-1) (q-1)
4. Select the public exponent e, such that 1< e< Ø and gcd(e, Ø) =1
5. Use the extended Euclidean algorithm to compute the private exponent d such that 1<d<Ø and ed≡ 1(mod Ø)
6. Output n, p, q, d, e
7. End

Algorithm 3: RSA Key Encryption

1. Begin
2. Obtain public key (n,e) and message m
3. Compute the ciphertext c
   $c=m^e \bmod n$
4. Output C

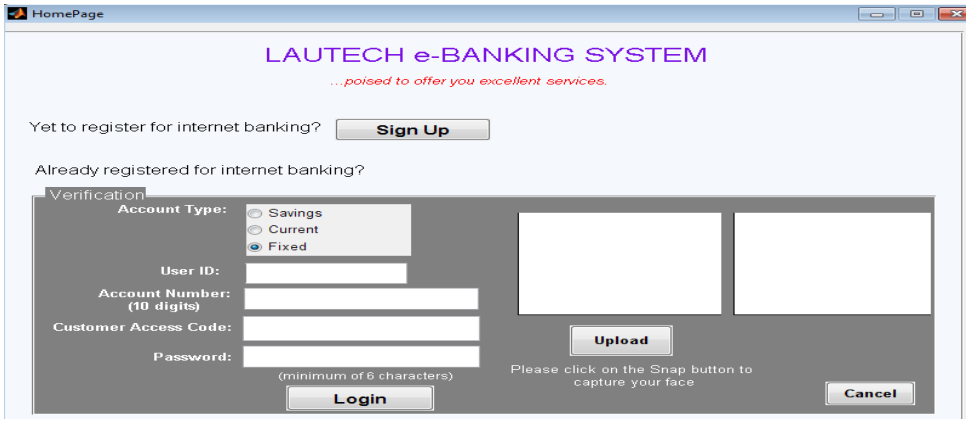
Algorithm 4: RSA Key Decryption

1. Begin
2. Obtain the ciphertext c
3. Use the private exponent d to recover m
   $m=c^d \bmod n$
4. Output the plaintext m
5. End

Algorithm 5: Extended Euclidean algorithm

1. Begin
2. Input two non-negative integers a & b with a≥b
3. If b←0
4. d←a; x←1; y←0;
5. Else Set x_2←1,x_1←0, y_2←0,y_1←1
6. While b>0
7. q ←[a/b] , r←a-qb, x←x_2-qx_1, y←y_2-qy_1
8. a←b, b←r, x_2←x_1, x_1←x, y_2←y_1, y_1←y
9. END
10. d←a, x←x_2, y←y_2
    END

4. HOW THE IMPLEMENTATION WORKS

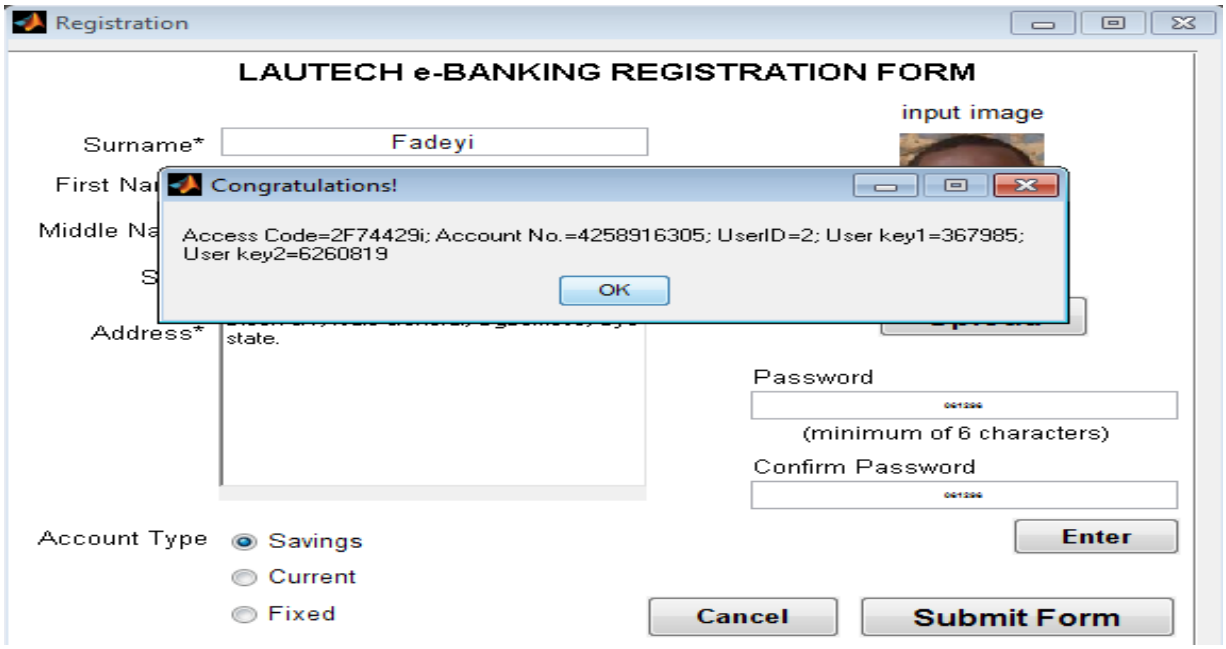


The E-Banking Homepage

Registration Interface

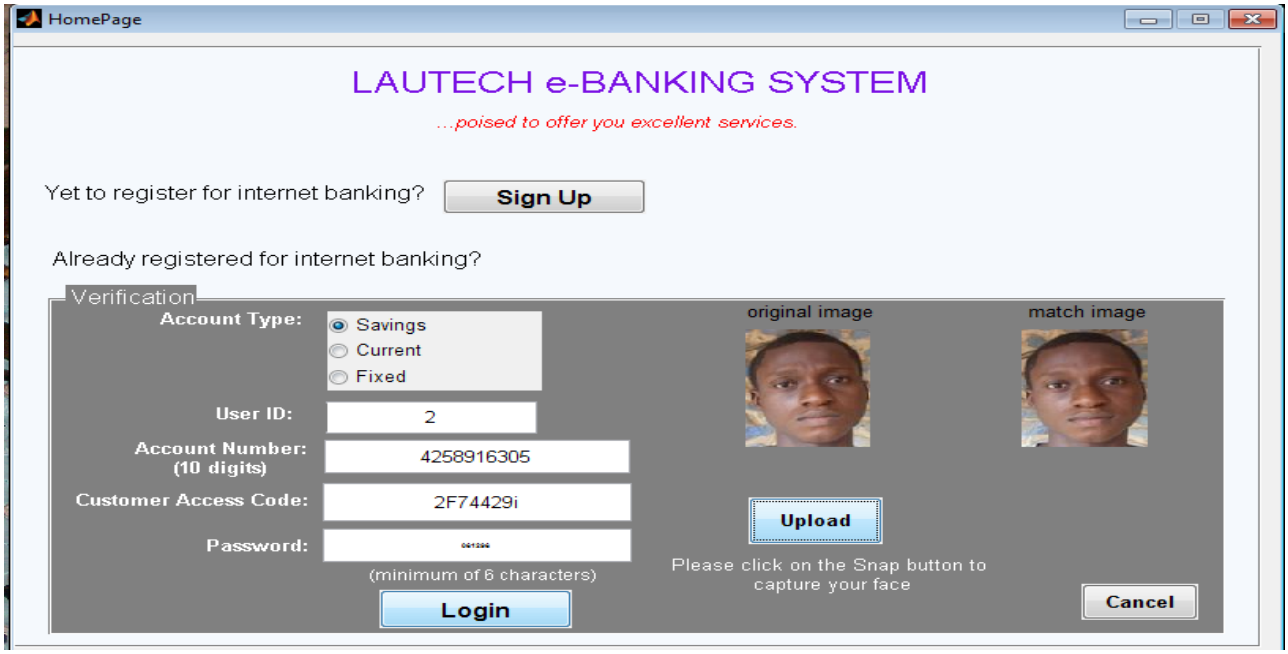
The first encountered interface display the option of what the customer wants to do since the customer can either sign up as a new user for registration or log in as an existing customer.

On clicking on the sign up button, a new window is displayed where a new customer enters the surname, first name, middle name, address, password, select the account type, sex, upload the picture taking by the bank and then clicks on the enter button to submit the password for acceptance before clicking on the submit button. If the password matches a "Password Accepted" window is displayed else a "Password Mismatched" window is displayed.



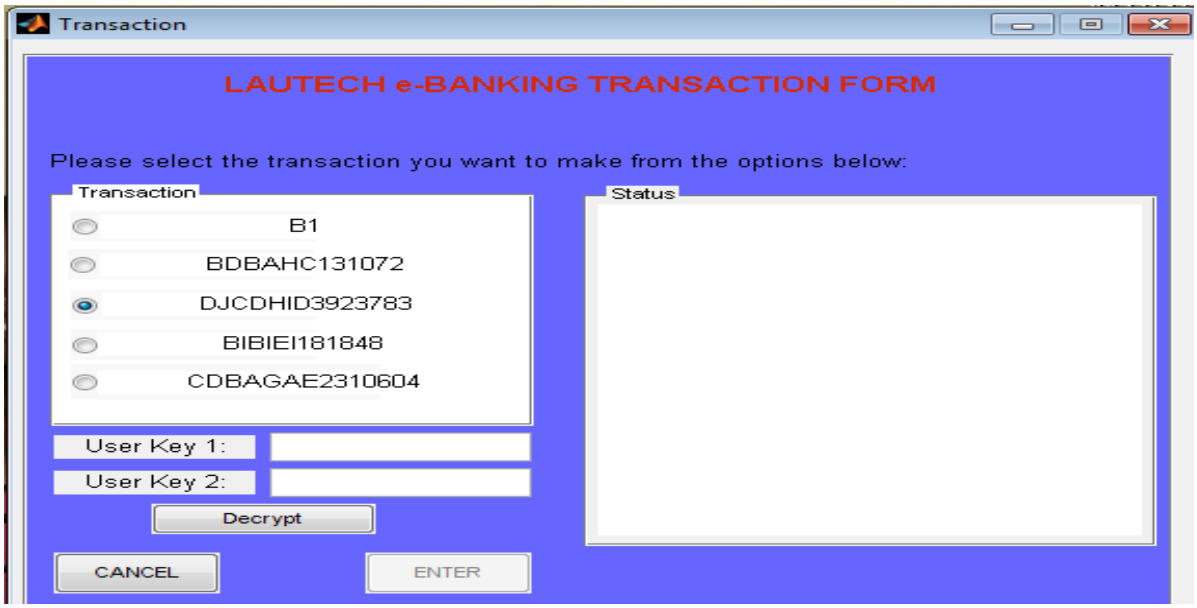
Access Code, Account No., UserID and the Private keys automatically generated

Immediately, the customer has finished supplying his/her details for registration and click on the submit button, the access code, account number, the userID, private keys which is the user key1 and user key2 will be automatically generated else if any of the entered detail is not in the correct format an error message is displayed.



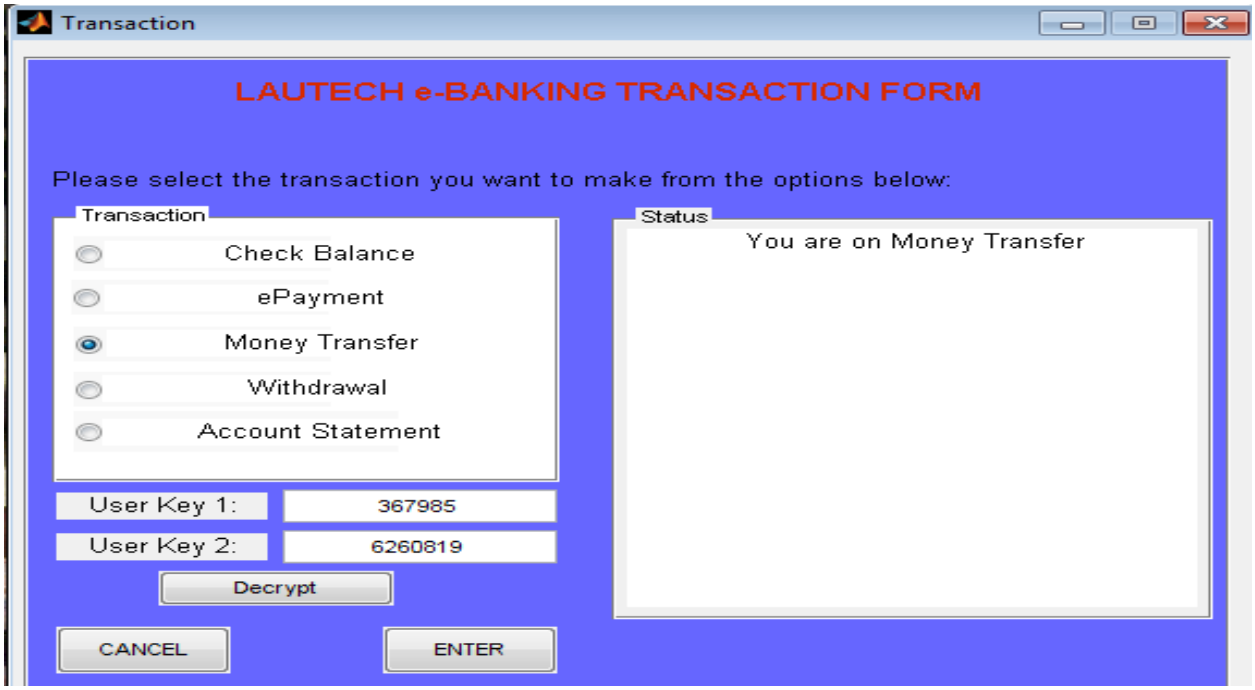
Verification Interface

This is where the customer enters the userID, account number, access code, password, select the type of account, upload the picture for verification on clicking on the login button a new window is displayed for transaction else if the details are not supplied in the correct format an error message is displayed.



The Encrypted Transaction Interface

The transaction details appear in an encrypted format to the customer that is cipher text, so the customer has to supply the private keys which are the user key1 and user key2 which has been generated during the registration phase. The customer has to supply these keys for the information on the transaction interface to be decrypted to the plaintext.



Transaction Interface

On providing the private keys, the customer then clicks on the Decrypt button to see the operations that can the carried out as per their account. The customer select any of the operations such as withdraw, money transfer, e-payment, check balance or check the statement of account.

5. CONCLUSION

The Internet has grown exponentially, with more than 30 million users worldwide currently. The Internet enhances the interaction between two businesses as well as between individuals and businesses. As a result of the growth of the Internet, electronic commerce has emerged and offered tremendous market potential for today's businesses. One industry that benefits from this new communication channel is the banking industry. Electronic banking is offering its customers with a wide range of services: Customers are able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions and effectively eliminate the rigors of traditional banking system and upgrade banking status.

To reduce the potential vulnerabilities regarding to the security, a combination of cryptography and face recognition system seem to be one of the most reliable means of authentication in a banking system environment. In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard.

REFERENCES

[1] A. J. Menezes; P. C. van Oorschot; S. A. Vanstone (1997). Handbook of Applied Cryptography. ISBN 0-8493-8523-7

[2] Donald E. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms, 3rd ed., Addison-Wesley, 1998.

[3] Electronic Banking. Http://www.electrobank.com/ebaeb.htm

[4] How Encryption Works http://www.howstuffworks.com/ encryption.htm

[5] http://www.e-banking.net/index.htm

[6] Journal of Internet Banking and Commerce -- www.Arraydev.com/commerce/jibc

[7] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET Evaluation Methodology for Face-Recognition Algorithms," IEEE Transactions on PAMI, 2000, Vol. 22, No. 10: 1090-1104.

[8] PKCS #1, RSA Cryptography Standard, RSA Laboratories, Version 2.1, June 2002.

[9] Soutar, C., Roberge, D., Stoianov, A., Gilory, R., Kumar, B.V.: Biometric encryption, www.bioscrypt.com.

[10] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain "Biometric Cryptosystems Issues and Challenges"Proceedings of the IEEE 2004.

[11] Understanding Public Key Infrastructure – RSA Security