ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

Development of E-Banking System with Crypto-Biometric Technology

Pallavi.Y[1], Nagraj Kyasa[2]

P.G. Student, Department Of Electronics and Communication, Don Bosco Institute of Technology, Bangalore, Karnataka, India[1]

Assistant Professor, Department Of Electronics and Communication, Don Bosco Institute of Technology, Bangalore, Karnataka, India[2]

ABSTRACT: Internet has played an important role in changing how we interact with other people and how we do business in today's technological world. The resultant of this leads to an emerged of electronic commerce which allow businesses to more effectively interact with their customers and other corporations inside and outside their industries. One of such 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. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One such essential aspect for secure communications is cryptography, and another is biometric. 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 be reached by some mere guess work. This E-banking system is designed using MATLAB with face recognition and encryption.

KEY WORDS: Biometrics, Principal component analysis, Encryption, E-banking.

I.INTRODUCTION

Internet has changed the life of human significantly and it has dominated many fields including e-Commerce, e-Healthcare etc. Internet increases the comfort of human life, on the other hand it also increases the need for security measures too. For example all web browsers and servers take almost every care to make guarantee the safe business through internet. Still they are vulnerable to attacks. 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 for offering greater convenience for customers. E – banking is a result of growing expectations of bank's customers. This system does involve direct interface with the customers. The customers do not have to visit the bank's premises. Electronic-banking offers the convenience of conducting most of your banking transactions at a time that suits to customer. The rapid advancement in electronic distribution channels has produced tremendous changes in the financial industry in recent years, with an increasing rate of change in technology, competition among players and consumer needs. The advances in technology-based systems, especially those related to the internet, are leading to fundamental changes in how companies interact with customers. Internet banking has become the self service delivery channel that allows banks to provide information and offer services to their customers with more convenience via the web services technology. Cryptography is the backbone upon which modern security has been established for authentication. Biometrics technology has been proposed to strengthen authentication mechanism in general by matching a stored biometric template to a live biometric template. However, both system themselves are not attack proof and are vulnerable against several types of attacks. An emerging solution is to integrate the authentication feature of biometrics and the core function of conventional cryptography, called crypto-biometric. More over in today's technology biometric system

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

protection schemes are in high demand. Thus, bio-cryptography inherits the advantages of both and provides a strong means to protect against biometric system attacks.

Thus project is mainly based on two domains cryptography and biometric technology. Cryptography is used for authentication purpose using encryption and decryption technique, where as biometric is also used for authentication purpose using physiological biometric of face recognition. Hence, the improvement of the security of e-Banking is done using these two domains.

I. II. 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, by referring Jiaqin Yang and Kh Tanveer Ahmed "Recent trends and developments in e-banking in an underdeveloped nation – an empirical study ,"[4].

By Hernando & Neito ,"E-Banking Management –Issues, Solution & Strategies "[3] 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.

By referring M. Kirby & L. Sirovich, "Low-Dimentional Procedure for the Characterization of Human Faces"[1], Automated face recognition is a relatively new concept which was 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. Thus, 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.

III. SYSTEM DESIGN

A. *Image Acquisition Scheme*

A database of facial images of individuals, representing a bank's customers is created. Each individual has to give 10 images of samples of different facial expressions. The image database is trained using the Principal Component Analysis (PCA) technique and the obtained features are saved for the recognition purposes. The bank registers a new customer each time by acquiring the customer's facial images of 10 different expressions, in the same way for each and every customer and then adds the images to the ones in the database after which the database is trained using the Principal Component Analysis (PCA) and the features are saved for future use.

B. *PCA Flowchart*

1) PCA Training: Image acquisition scheme is followed by the method of Principal Component Analysis (PCA) technique where the images will be trained by PCA as shown in the flowchart of Fig. 1, where the image of face of different customers of different 10 images are acquired, create an average value over that and compute the mean face image and covariance matrix, identify Eigen values & Eigen vectors with by which eigenspace is calculated, weights are identified and features are saved for recognition purposes.

2) PCA Testing: The trained image by Principal Component Analysis (PCA) process is then matched with the real test image. The real image is when the customer needs to log in to access account sits in front of camera and upload image. This process calculate the eigenspace value of the real test image and calculates the Euclidean distance between both real test image and the trained PCA image, if both gets match i.e. , if the value is greater than threshold value the further process is continued or else it will display the error message saying "Invalid User" and the process is stopped. The process flow is as showed in Fig. 2

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

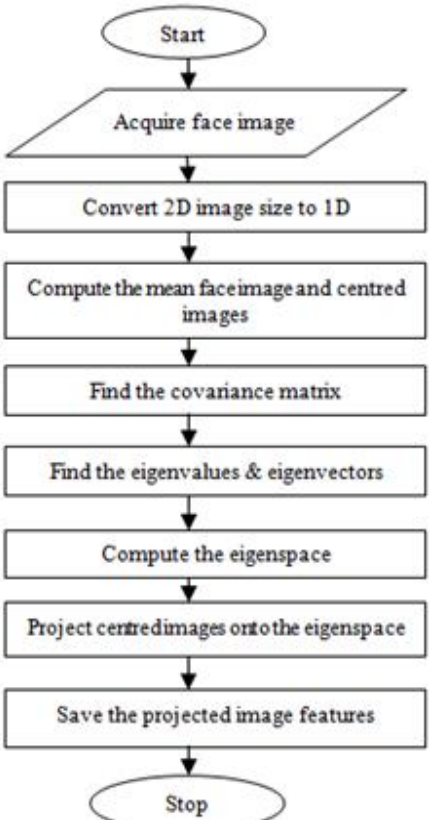

Fig. 1 PCA training

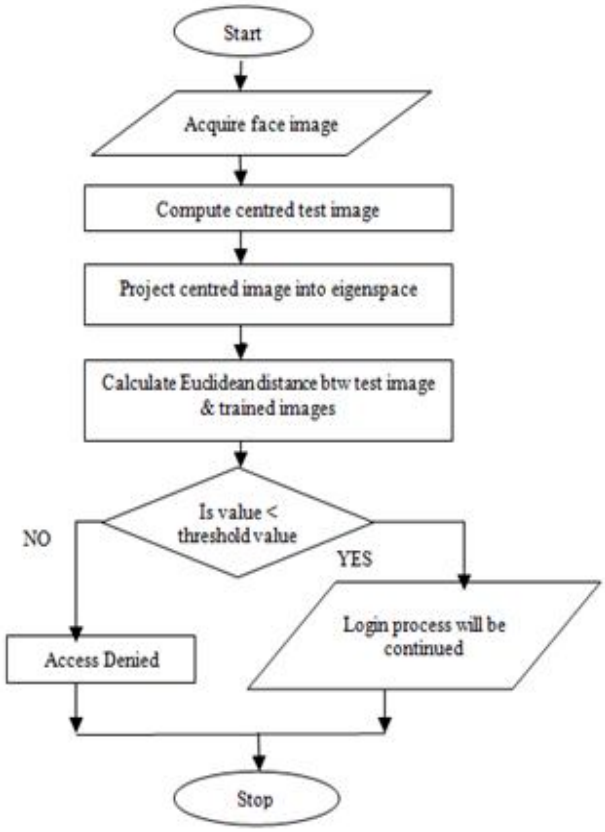

Fig.2 Matching of real test image and image stored in database

C. *Data Security Algorithm*

The data encryption and decryption is done in order to secure the data by transferring the plain text into the cipher text. This is done by using the random permutation algorithm, where the message will be changed to cipher by converting text to binary values and randomizing it and rearranging back to cipher text format. The same will be in reverse for converting cipher text back to plain text. Thus, the information will be secured. This method is used in order to do transaction part where the transaction details will be encrypted and to process further the user keys need to be entered to decrypt the transaction details. Thus the security of information will be achieved.

IV. IMPLEMENTATION RESULTS

A. *E-Banking Homepage*

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 shown in Fig.3

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

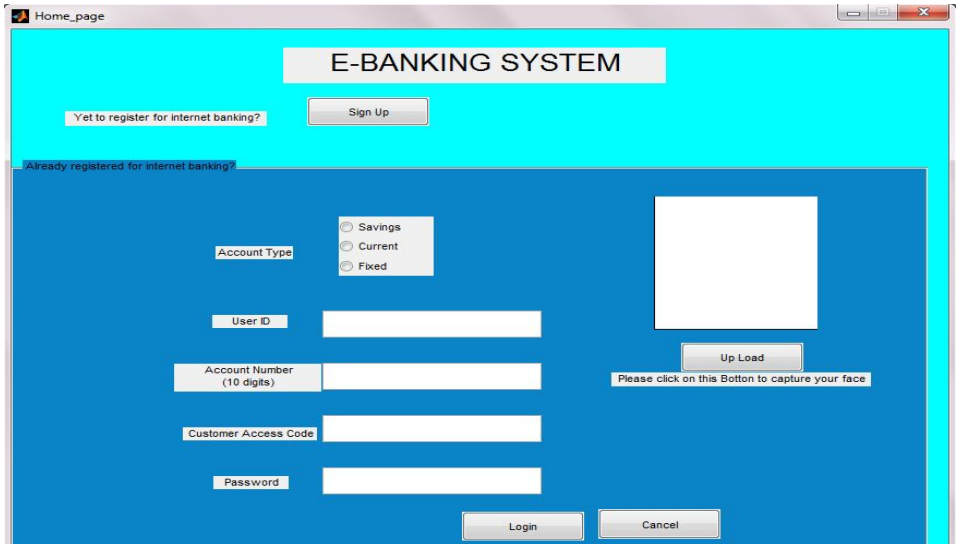

Fig.3 E-Banking Homepage

B. *Registration Interface*

If person is not registered then by 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. At this part it will capture an image and this will be trained with PCA and the features will be saved for future use. If password doesn't matches it will display the error message as "password doesn't match".

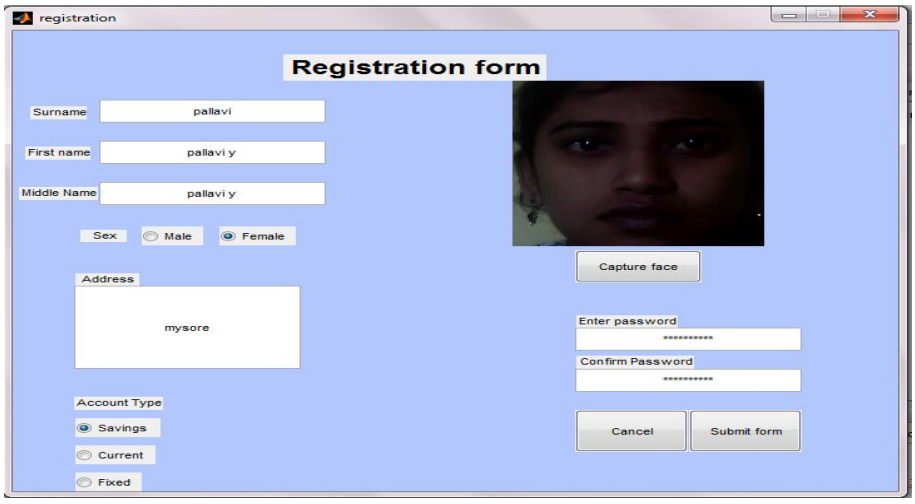

Fig.4 Registration Interface

C. *Access Code, Account No., UserID and the Private keys generate automatically*

Immediately, the customer has finished 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 as

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

shown in Fig.5 else if any of the entered detail is not in the correct format an error message is displayed as "Invalid user". Here random generation process is used for the generation of the access code, account number, ID and user keys to the users. The automatically generated details will be saved or will be sent to user mobile by adding another option, in order to access account in future. Thus the part of registration form to access the account formalities will be completed. One thing should be kept in mind that without having any one among this five security keys one cannot access the account. Hence these details should be kept secretly such that any third person should not come to know about this otherwise the third person may try to access your account.

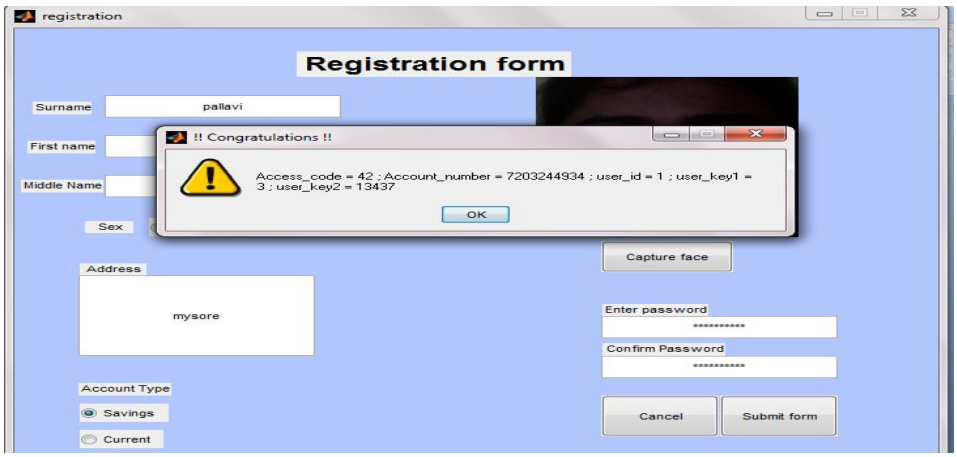

Fig.5 Access Code, Account No, UserID and the Private keys automatically generated

D. *Verification Interface*

This is where the customer sign up by entering the userID, account number, access code, password and select the type of account, upload the picture for verification on clicking on the login button as in Fig.6. At this part this picture will be matched with the stored database if this matches with threshold value as designed then the process of accessing the account will be continued further. Thus a new window is displayed for transaction else if the details are not supplied in the correct format an error message is displayed or even if image mismatches an error message will be displayed.

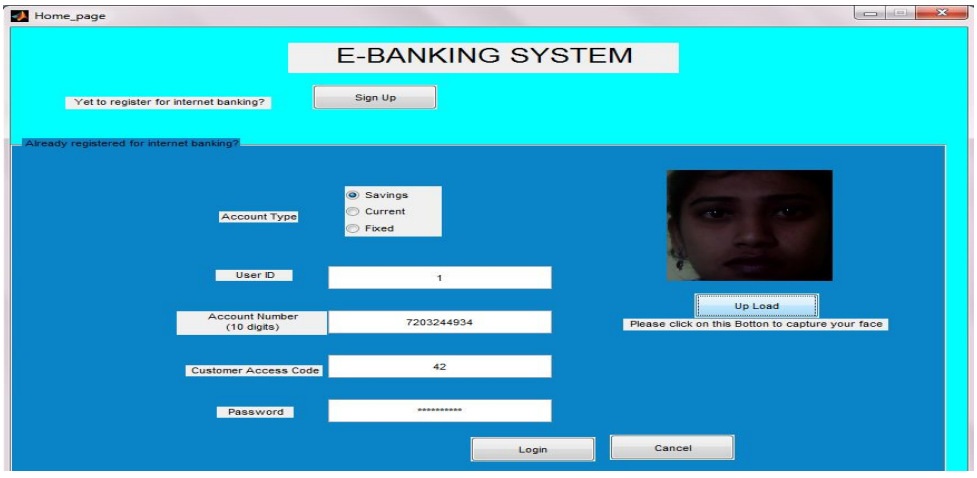

Fig.6 Verification Interface

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

E. *The Encrypted Transaction Interface*

The transaction details appear in an encrypted format as shown in Fig.7 to the customer that will be in the 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 in order to get the information on the transaction interface which will be decrypted to the plaintext.

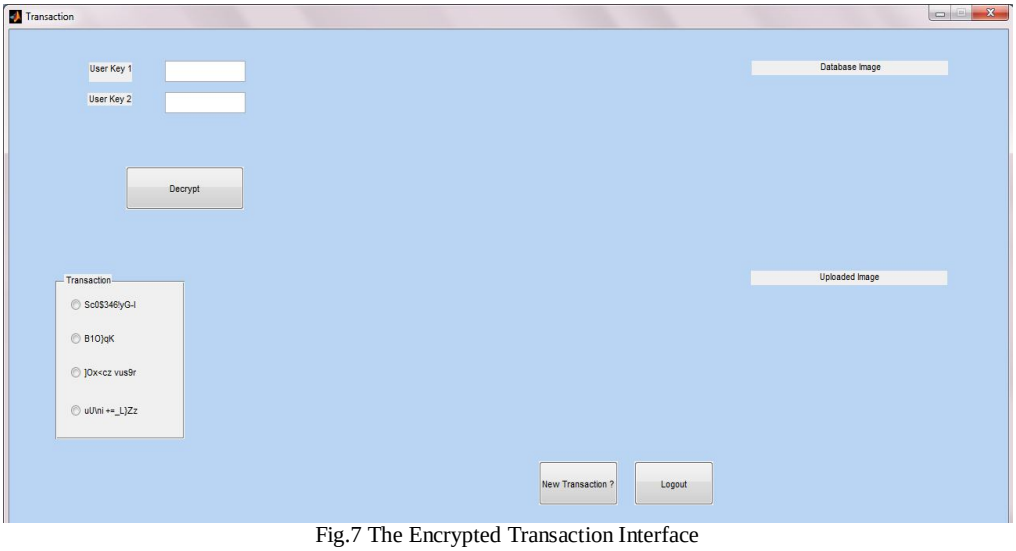

Fig.7 The Encrypted Transaction Interface

F. *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 necessity. The customer can select any of the operations such as withdraw, money transfer, e-payment, check balance or check the statement of account. For example the check balance and money transfer part is shown in Fig.8 and Fig.9 respectively. Here for each transaction the separate windows will be displayed so that comfortably the users can do their transactions. The different types of transactions are shown below as follows: Check Balance, Easy recharge, Money Transfer and Account Statement. After transaction happen users can logout from account.

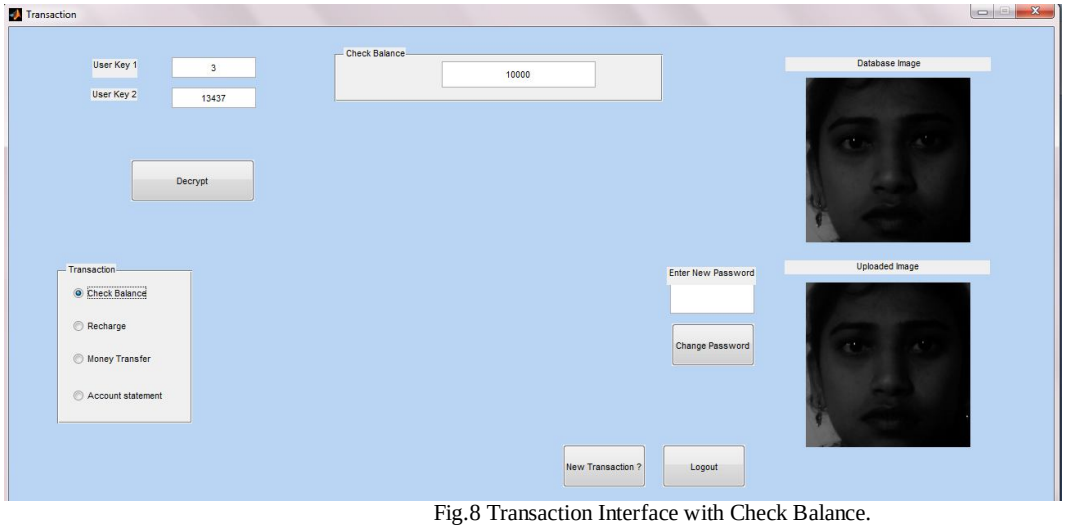

Fig.8 Transaction Interface with Check Balance.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

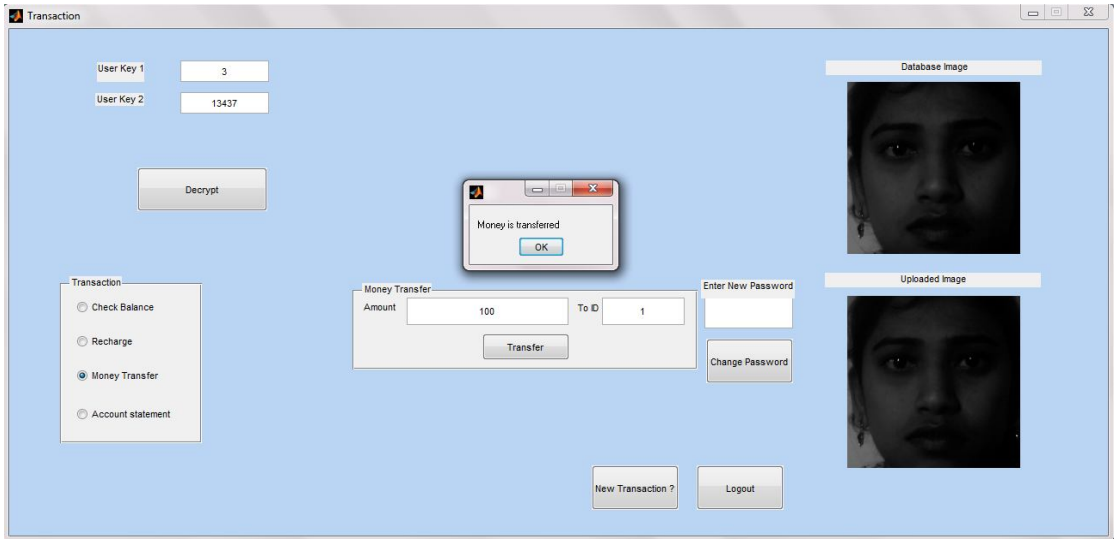

Fig.9 Transaction Interface with Money Transfer.

The e-Banking system also consists of the facilities to change their password when they required according to their convince and can access the account with their newly changed password.

V.CONCLUSIONS

E-Banking industry in today's technology is facing several major challenges and issues. First, and perhaps most important is the security concern. Customers are certainly concerned of giving their bank account information online or paying an invoice through internet. Another challenge facing e-banking industry and the e-business in general is the quality of delivery service – including both delivery speed *i.e.*, short advance time required in ordering and delivery reliability *i.e.*, delivery of items or services on time. E-banking system at present is using the username and password security mechanism which can easily reached by mere guess work and password can be hacked. 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) M. Kirby and L. Sirovich, "Low-Dimentional Procedure for the Characterization of Human Faces", Optical Society of America A-Optics, Image Science and Vision, Vol.4, No.3, march 1987, pp.519-524.
2) M. Kirby and L. Sirovich, "Application of Karhunen-Loeve Procedure for the Characterization of Human Faces", IEEE Transactions on pattern Analysis and Machine Intelligence, Vol.12, No.1, January 1990, pp.803-808.
3) Hernando & Neito ,"E-Banking Management –Issues, Solution & Strategies " , Information Science Reference Hushey, Newyork 2007.
4) Jiaqin Yang and Kh Tanveer Ahmed "Recent trends and developments in e-banking in an underdeveloped nation – an empirical study ," Int. J. Electronic Finance, Vol. 3, No. 2, 2009.
5) Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain "Biometric Cryptosystems Issues and Challenges"Proceedings of the IEEE 2004.
6)

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2014

BIOGRAPHY

Nagraj Kyasa. received BE degree from G.N.D College of Engineering, Bidar. India in 2005. MTech degree from Dayananda Sagar College of Engineering, Bangalore, India in 2008. Presently working as Assistant Professor in Don Bosco Institute of Technology, Bangalore, India. Presented paper in conference ICRTSIV-14. And guided many UG and PG projects.

Pallavi Y. received BE degree from S.J.B Institute of Technology, Bangalore, India in 2011. Then worked as Software Test Engineer in C.T.D, Bangalore, India. Presently PG student in Don Bosco Institute of Technology, Bangalore, India. Presented paper in NaCoNIM-2014 at K.S.I.T, Bangalore.