ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse1381032021.pdf
https://doi.org/10.30534/ijatcse/2021/1391032021

Intelligent Hybrid Fraud Detection Using Biometric and Face Recognition

Hafiz Muhammad Tayyab Khushi, Tehreem Masood, Arfan Jaffar
Superior University Lahore, Pakistan, tkhan283@gmail.com
Superior University Lahore, Pakistan, tehreem.masood@superior.edu.pk
Superior University Lahore, Pakistan, arfan.jaffar@superior.edu.pk

ABSTRACT

Financial transaction is backbone of global market that make it convenient for people to make their transaction easy. People do transaction of money from everywhere using banking system through e-banking or credit card system. That is why banking sectors play a vital role in any country and provide proper structure to any country and make their economy better. However there are many fraudulent who steal the information of any person's account, use the in information for their own purposes and do illegitimate transaction. Fraudster continuously try to get user's account information by applying different tricks to commit fraud that cost huge lose to banking system as well as consumers that's why fraud become major issue for banking sectors. In Banking sectors there are a lot of transaction that operate on each day and increase day by day and it is necessary to make secure of money and transaction as well consumers information that fraudster do not steal easily. To overcome this issue there is a need of an efficient fraud detection method or system that detect fraud quickly and stop fraudster to commit fraud because it is very easy to steal any consumers login information to commit fraud like user name and password but we need a mechanism that can be impossible to crack easily and detect fraud on earlier stage. So in this research work, we discuss the method to prevent illegitimate or fraudulent transaction. For this purpose, we propose hybrid biometric and face recognition system. This system detect fraudulent transaction and stop fraudster to commit fraud and classify transaction as legitimate and illegitimate. This system is beneficial for either online or e-banking and through credit card transaction.

Key words : Illegitimate transaction; legitimate transaction; online banking; credit card; biometric; face recognition.

1. INTRODUCTION

Now a days fraudsters become a challenge for banking Sectors because they are doing illegitimate transactions [1] by stealing the account information of any person and use them for their own purposes. The popularity of banking systems are increasing day by day because people are using banking systems for money transaction, use it for shopping, pay bills and for online transaction in everywhere with in small time period [2]. So with the increase of banking user, frauds have also been on rise. Fraud can cause loss of billions of dollars globally. By this any country can be in huge financial crisis. Fraud can be classified as any activity that can bed one without permission of credit card holder or bank account holder to obtain financial benefit with any manner or trick [3]. Fraud can be committed in many ways. By making fake identity, counter feit credit card, by making clone of original website, by modifying or making magnetic strip present at the end of credit card that contain consumer's information. Fraud can also be done by phishing or by skimming user's data from merchant's side[4]. Fraudsters steal the login information like username and password of any person for online banking and steal credit card detail and pin code for credit card fraudulent transaction [1]. Most commonly used two methods are online banking or e-banking and credit card transactions. For committing credit card fraud, fraudsters access the information of credit card like credit card numbers, user name, password or pin of card by using spy cam that is placed inside the ATM Machine or any ATM place. For online banking transaction, fraudsters use phishing techniques to access the login credentials such as username and password and do illegitimate transaction [8]. Major problem is that fraudster try different ways to commit fraud and total number of fraudulent transaction is much less than total number of real or legitimate transaction. Fraud detection deals with finding fraudulent activity among all genuine transaction which cannot be easy but puts forward a challenge [7]. Another problem is that fraudulent transaction can be done in a way that look like real and in most of cases, fraudulent activity or fraudulent transaction cannot be filed or complained by consumers [10]. To overcome these types of fraud, an automated system is required that can detect fraud and prevent fraudster to do illegitimate transaction. The system can detect fraud at initial state and find such fraudulent transaction among all transaction in an efficient way.

In this paper we present hybrid techniques to prevent illegitimate transaction. In hybrid we use biometric face recognition method. With these proposed methods, we can control almost all fraudulent transactions over internet or credit card. We know fraudulent stole easily user name and password information by applying any way but it is very difficult to crack any consumer facial and biometric information easily and our proposed methodology works on both way of transaction to secure and protect consumers credential information and make them secure and protect their money.

2. RELATED WORK

There are not so many published work on banking fraud system but we discuss some different techniques for prevention

of fraudulent transaction and compare those techniques in this section.

Sonali, Rishita, Sunanada, Sumana [1] described the fraud method recognition to prevent illegitimate transaction by using graph database. In this paper, bust-out fraud and credit-card fraud are discussed. In bust-out fraud, they check the number of links or terminals from where fraudsters can access or do transaction. In bust-out fraud, fraudsters share information like account name, number, address for making illegitimate account in banking and then start illegitimate transaction. Fraudsters make synthetic id that look like real one and bypass security Checks and apply for loan. When they get loan they disappear and bank suffers huge lose.

In credit-card fraud, fraudsters access the credit card number, password or pin, expiration date, cvv no of card by using spy cam and then use for their own purposes. For credit-card fraud, they check the origin from where fraudsters doing illegitimate transactions. For prevention of these fraudulent transaction, they use graph database. In graph database, they use nodes and relationship to represent data. Nodes and relationship have properties that describe themselves.

There is another method of fraud detection in banking sectors. This method was proposed by Suman and Mitali Bansal [2]. In this method, they can take two things for checking fraudulent transactions. One is behavioral characteristics and second is psychological characteristics. By combining both characteristics, they call it as biometric approach.

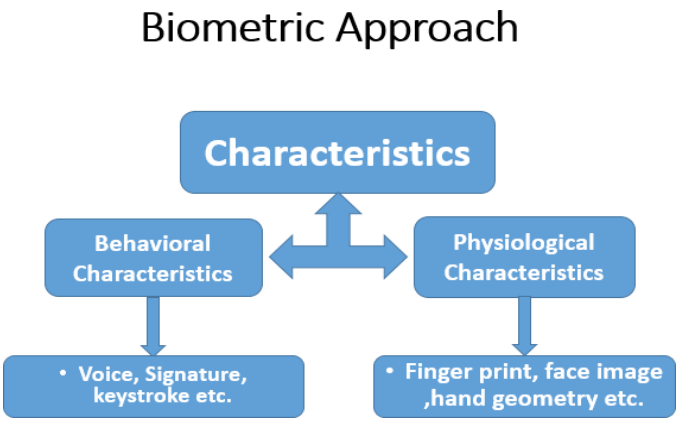

Figure 1.Biometric Approach

In behavioral characteristics they take three parameters for checking fraudulent transaction. These parameters are human voice, signature and keystroke. In physiological characteristics, they also take three parameters. These parameters are face image, finger print and hand geometry as every person have unique finger print or face image. In behavioral characteristic approach, they check the user keystroke method and check how users can stroke the keys as every person have different behavior or unique pattern to stroke the keys. In this way, they detect the legitimate and fraudulent transaction.

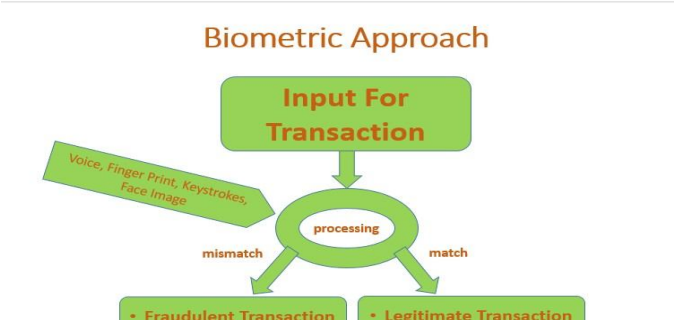

Figure 2.Biometric Approach

There is another method for fraudulent transaction detection that was proposed by Stephan Kovach and Wilson Vicente [3]. This proposed solution is for online banking system. In this method they monitor the device from where transaction has been made with the certain probability of global information. This is based on three assumptions.

- Each device use for e-banking have single identification.
- Probability of illegitimate transaction increase with number of account accessed by same source or destination.
- Fraud has been reported only when customers report it and this is the only way to perpetrated fraud.

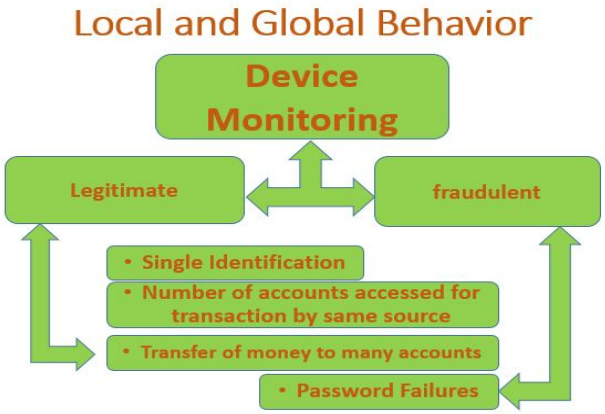

Figure 3: Device Monitoring

This second method is monitoring of local behavior. This method take four parameters for checking online transaction, whether transaction is fraudulent or legitimate. After checking these four parameters, they check three parameters as regard of device monitoring. Four parameters as regard of online banking are given below.

- Many accounts accessed by only one person.
- Transaction money transfer too many accounts in small amount.
- Try to make transaction over the limit of fixed

payment.

- Password failures increase by accessing system

In third technique called local and Global behavior is suitable for checking fraud only in online transaction. In this technique for checking fraudulent transaction monitor the device and account location. This technique use very complex method to detect fraud but not given any suitable solution to find or detect fraud in transaction through card.

Divya Murli and Shailesh Jami [4] proposed a solution of fraud detection through credit card using neural networks. They implemented a mechanism to detect fraud through credit card using neural networks by using Neuroph IDE. They present various parameters on that basis, they train and test neural networks. Neural networks are same like biological neuron that accepts many values as inputs, process that inputs and give result as single output. Perceptron's are basic model of artificial neural networks that consists of two layers. One layer is for input and second layer is for output. Input layer takes different inputs regarding different parameters and send to output layer where all inputs are generalized and categorized according to their functions and specification that are already fed by training the neural networks and apply different values or functions like threshold for classification of inputs. Training can be ceased on some parameters like maximum numbers of iteration, lower and upper bounds on the percentage of errors and many others. By these parameters and technique they detect credit card fraud.

There is another fraud detection technique that is presented by Jyoti R. and Gaikwad [5]. They proposed fraud detection mechanism using decision tree induction algorithm. They have used different approaches of data mining and classification models based on ID3 decision trees and visual cryptography applied on credit card fraud detection problem. In decision tree induction algorithm, they analyses data as data stream and detect fraud. Decision tree induction algorithm is based on recursive partitioning of data that begins with entire body of data. In this technique, data is split in two or more than two subsets based on the values of one or more than one attributes and then each attribute further split into more attribute till last value or stopping criteria of tree leaf nodes. Each node sre present a class and further classified. They have used different approaches to minimize fraud and it is only for credit card fraud detection but not for transaction through e-banking. This mechanism is only applicable for detecting fraud in credit card.

There is another fraud detection technique that is presented by Shailesh S.Dhok [6]. They proposed solution to detect fraud using Hidden Markov Model in credit card. Hidden Markov model have finite set of states and where each state is linked with probability distribution and particular state of observation generated is not visible to external environment. In this technique fraud is detected by observing the spending behavior of credit card holder. First, they estimate transaction ratio as low, medium or high. Then they detect cardholder's spending habit. The implementation of this technique is done through credit card. It create clusters of training sets and identify the cardholder's spending or transaction profile like number of items purchased, types of items that are bought in particular transaction. They had not only focused items but also focused on amount by which items are purchased and further use of processing card. They store data of different transaction in clusters and tries to find out variance in spending behaviors.

Bolton and Hand [7] proposed another mechanism to detect fraud. They proposed supervised or unsupervised statistical fraud detection mechanism. In this proposed solution, behavior of objects are examined and on the bases of behavior, transaction is declared as fraudulent or genuine. In supervised model examination is based on trained existing data and in unsupervised method, classification of objects have been done on real time data and not comparing behavior with existing objects. In this methodology, if observed behavior is normal then allow to proceed else if behavior is not normal then disallow the proceeding of transaction and declared as illegitimate or fraudulent transaction.

There is another fraud detection mechanism that is proposed by S.Saranya[8]. They proposed solution to detect fraud through credit card transaction using Bayesian network. This technique based on conditional probability of Bayes theorem. It is a probability model that is used for automated events detection. This mechanism contain nodes and edges where nodes represent the random variable and edges shows the relationship between random variables and their probabilistic distribution. In this network, predefined maximum and minimum values of probabilities of transaction are used for legal or fraudulent. For new transaction, first check if its probability is less than minimum defined value of legal transaction and greater than maximum defined value of illegal or fraudulent transaction to declare whether transaction is fraudulent or legal. If condition is true then transaction is fraudulent and if condition is false then transaction is legal or legitimate.

There is another fraud detection technique that is proposed by Khurana [9]. They proposed solution to detect fraud using fuzzy logic and neural network in credit card transaction. This technique is implemented where values are not discrete values and are continuous. There are some basic rules and three component in this technique to verify whether transaction is legal or fraudulent. These components are executed in order to verify transactions. In Fuzzification, method transaction is classified according to three categories of high , medium and low monetary based value associated with transaction. In Rule based, transaction is allowed to proceed, if it satisfy given rules and deals with drafting of the rule based on user's behaviors. In defuzzification procedure, if the transaction do not comply with predefined rule than it is not allowed to proceed, stop the transaction and check the consumer's behavior whether it should be granted permission to allow continue or stopped.

There is another fraud detection mechanism that is presented by Demla [10]. They proposed solution to detect credit card fraud by using SVM and reduction of false alarms. In this technique, basic goal is to find hyperplane for which fraudulent transaction is detected. For this purpose, different types of hyperplane are required to find optimal hyperplane. Those support vectors and points are used to detect classes of new data point. When data point put into hyperplane's equation then

result classify which class they belong to and on which side of hyperplane falls on vector space.

There is another technique to detect online transaction fraud that can be presented by M.I. Omogbhemhe, I.B.A. Momodu and S. Awojide [11]. They purposed An Improved Multimodal Biometric Architecture for securing online payment. They used more than one biometric features to be implemented to achieve high security need. They used multimodal biometric architecture. This architecture have different modules of reporting for checking error and recovering from error. For this every module have its own unique database to verifying the biometric data. This architecture requires face image scanner and finger print reader to capture and verifying the biometric data. To implement this technique they used for different module or functions.

- The feature extraction module
- Matching function
- Database template
- Decision module

Feature extraction module used to extract the biometric template by using biometric input device to capturing biometric data and then with comparison of that data with saving data on time of registration and check whether capturing data is present or not in database.

Matching function can compare the biometric data with saved biometric data in database and check whether the data is valid or not. Third module database template is work with matching module to check whether particular biometric data exist or not. Last module Decision module decide whether the particular biometric data is matched or valid to perform online payment or not. if matched then go for transaction.

There is another method of fraud detection that have been represented by Charles and Isioma Ukper [12]. They purposed solution to secure unified e-payment system in Nigeria. In this research work they purposed solution to detect fraud in ATM card with biometric base cash transaction in all banking system. In this system first make single unique credit card for all banks and replace the blank keys with biometric authentication readers to verify the finger print with user card detail like pin, username, gender etc. and make sure the connectivity of all banks with national banking system database to achieve additional security and information and in accident case they verify the blood group also and all these information must be saved in national bank database too. For cash transaction user detail with fingerprint verification must be authenticate before transaction.

There is another technique represented by Aranuwa and Ogunniye[13]. They purposed solution to Enhanced Biometric Authentication System in Nigeria for Efficient and Reliable e-Payment. This technique is applicable for detection fraud of both online and credit card transaction. They used user's bio data with finger print and face enrollment to detect whether transaction is fraudulent or legitimate. To achieve this used of attached camera with ATM machine or any device to verify face and fingerprint scanner to verify fingerprint with user's bio. In addition they used fingerprint pulse to detect fake biometric at sensor also used to handle threats of tempering with biometric features. To verify the transaction first check user's bio like name, Pin, Finger print if valid then go next to verify face by camera. If camera verification is correct then allow to proceed transaction otherwise access denied and illegitimate transaction detected.

There is another technique to prevent fraud and secured transaction to be legitimate in credit card transaction presented by Khudhar, Hameed, Shokhan [14]. They purposed solution to enhance e-banking security by using whirlpool hash function. This technique is for credit card number encryption. In Whirlpool hash function they used Miyaguchi-preneel comparison that based on 512-bit block cipher that is called W. In this has function first step is padding message to ensure message bit to hashed aligned on appropriate bit boundary And resulting data blocked would be organized in 8*8 array of bytes and performed 10 iteration of W cipher to performed on arrays individually. This sequence of encryption can be repeated for all remaining blocks.

ThereisanotherworkpurposedbyA.Salma1,Devi,saranya [15]. In this research work they purposed authentication framework that consist of user's personal information like PIN and user's finger print for identification and verification in ATM to prevent theft or any other illegal activities in ATM machine. For prevention of illegal activities they purposed GSM system that alert and notify nearest police station during detecting of illegal activities in ATM machine. In their research work first user make unique credit card that run on every ATM Machine on user's choice. First user enter or swipe their card details like PIN, fingerprint after verification of this all list of banks appears and user select bank through which he/she is willing to do transaction. After that selecting the bank request sent to bank through network and link with bank server for accessing the database to proceed transaction. If all things verified or then allow to proceed or if In case of theft, or broken ATM machine or any illegal activity the door of ATM Center automatically locked and alarm or buzzer is activated to alert nearest police station or security. In this technique they try to detect or stop illegitimate or invalid transaction.

There is another research work that represented by M. F. Mridha [16]. They purposed solution to Enhance Internet Banking Security. In their research work purposed secured protocol in E-banking system to enhance security. In this research work certificate verification and secure protocol mechanism detect or check first sender authenticity. The new secured protocol provide extra layer for security in E-banking system. When sender send data and data comes through secure channel first data checked than decided whether data go for further processing or not. If found something wrong then data discard and no access to go for further processing. This protocol have basic 4 steps to process. Hand shaking scheme maintain the sequence of record and initiate the process and ask for the certificate. If certificate and signature verified then request for next processing or store data and if verification failed then alert message to sender and discard data and no further allow to processing.

There is another research work that represented by Emeka [17]. They purposed solution to secure Internet Banking System by Using Three-Level Security Implementation. This system used three level security for internet banking. These are banking dongle, Kerberos, and advanced encryption standard and biometric identification. Biometric approach used to implement access control to dongle that provide secure path to internet server. Advanced encryption standard module used to ensure the confidentiality of the transaction information. In their purposed method first user attached USB internet banking dongle to PC or other device and login. For login screen can be prompt for getting PIN or fingerprint by PIN reader or biometric scanner. After verification information send by dongle device to Kerberos server for ticket granting. After the conformation or verification of identity by granting ticket the dongle application connect automatically with internet banking server by using tickets that generated by Kerberos server. User then again enter their login information on internet banking server interface and select operation to be proceed. After these internet banking server and dongle uses symmetric keys to encrypt and decrypt transaction information. When customer logout then all generated tickets and sessions expires and communication between dongle and banking server terminate and dongle application closed automatically and signal or notification sent to user of ending operation.

There is another research work on fraud detection presented by Sayali Kishor Rodge [18]. They purposed solution by using data mining on banking database in fraud detection techniques. In their research work they present some datamining concepts to prevent illegitimate transaction. According to that research work datamining is helpful tool that used to drawing and fetching the data or information and convert them in some patterns to understand the issue regarding data and associated with some algorithms like decision tree, visualization and genetic algorithm to discrete the problems found in data regarding any fraud or illegal activity. Datamining technique can work on following major steps.

- Predictive modeling
- Clustering/segmentation
- Visualization
- Link analysis
- Deviation detection
- Summarization

Predictive modeling used to predict the particular pattern that provide additional information about database or data that leads to detect fraud. Clustering provide clusters of existing database while segmentation provide finer data patterns. While link analysis work on finding related information or data from database and data summarization is final steps of datamining technique that summarized all results on basis of previous gathering information and analysis to prevent or stop fake transactions.

There is another research work related to fraud detection presented by Sahin and Duman [19]. They purposed solution to Detect Fraud by ANN and Logistic Regression in credit card transaction. In their research work they developed two models. One is (artificial neural networks) ANN and (logistic regression) LR and applied on transaction through credit card fraud and prevent fraud. In this research work or technique every account can be monitored separately using suitable description and identified transaction and give them flag of legitimate or fake on base of identification. ANN refers to nonlinear statistical technique while neural network is based on neuron that accepts many inputs and on that inputs or summation generate result and gave values grate than 1 and less than 0. Logistic regression is used to classify problems by predicting binomial and multinomial outcomes and examine the value of its attribute. On the basis of values of attributes tells whether transactions allowed to proceed or not.

There is another research represented by Omogbhemhe Izah Mike [20]. They purposed solution to Securing ATM System by Service Oriented Biometric Model. In this research work they present service oriented model of securing ATM using Bank Verification Number (BVN) with also they present end- transaction biometric-PIN or B-PIN to validate every transaction. This B-PIN is used to act as validate or for any transaction to be done in ATM. The unique thing of this model is if someone tried to bypass first check and do transaction of money but when transaction going to end again ending verification required to finished transaction by unique B-PIN or end-transaction biometric-PIN and all the transaction not be completed without biometric verification and this is suitable technique to prevent fraudulent transaction and they tried to give solution for ensuring secure and accurate transaction within banking service through ATM usage. And this technique can be implemented by them using visual studio tool using C# language.

There is another fraud detection research work that presented by Najwa Azmi & Dewi Nasien [21]. They purposed solution to detect fraud in e-banking and also by credit card transaction using Freeman Chain Code in Signature Fraud Detection that Based on Nearest Neighbor and Artificial Neural Network Classifier. In this research work they purposed signature verification system (SVS). They extracted information from signature picor signature data and on that basis they verified the transaction have being legitimate or fraudulent. Signature verification system can be classified in two stat one is offline and one is online. Offline verification system called static and online verification system called dynamic. In offline users used or write their signatures on paper and detected by camera or any scanning device. In form of online users can enter their signatures digitally in computer or database to perform verification. After getting data on verification traits form data or signature pics can be extracted to verify. In SVS four steps to be followed Data acquisition, Pre- processing, Feature extraction and Verification. In data acquisition sample of data can be converted into digitalized form. In pre-processing features image can be cleaned by applying various filter to remove noise. In feature extraction features from signature image or input can be extracted on that behalf verification can be done to verify whether the transaction being legitimate or fake to proceed transaction successfully.

There is another research work identification and prevention of fraud that presented by Fotak, Baca, Koruga [22]. They purposed solution to detect fraud in e-banking by handwritten signature identification that base on concepts of graph theory. The main idea of this research is to secure transaction and according to them security can be achieved by online verification of handwritten signature. For this purpose they make identification module to verify different sample of signature. That module contain all identification logic and all data can be passed to that module to get results. If result match then go to proceed for matching criteria they take 2 coordinates one is x and other is y and make them in vector. By these coordinates they make graph signature to calculate some graph features and apply system architecture to getting result. After making graph calculating signature graph picture width with x coordinate value by MinX and MaxX. In this research work graph theory can be used and undirected weighted graph used, in graph theory first check or extract information whether graph is connected or not and then check how they are connected to get or extract information from next graph. After making signature graph and extracting information from graph identification or verification process start. If user signature match just only one available information in different graph then its mean verification justified and allow to do transaction. This graph theory signature verification makes suitable implementation and verification of handwritten signature in off- line form.

There is another research work represented by Quratulain, Nida, Asma and Sajjad [23]. They purposed solution to detect suspicious transaction by using Ontology Based Expert-System. In this research work individually transaction being monitored and detect suspicious financial transaction. Ontology used to detect suspicious transaction behavior and comprised on three steps. Ontology construction, Ontology reasoning and Query on inferred ontology. First to construct ontology that provide unambiguous specification of knowledge and this system consist domain knowledge and some rule to supports reasoning and data processing required before to construct ontology. Data pre-processing used to remove noisy data to perform data normalization. The basic purpose of making ontology is to store consumer's transaction record and ontology reasoning is process of getting or extracting new information from existing knowledge. By applying query and reasoning detect suspicious behavior of transaction to detect whether transaction being legitimate or fraudulent.

There is another research work presented by Manish Bendale, Saurabh, Dorle, Pise [24]. They purposed solution to detect fraud in e-banking using Intelligent System by checking Behavior in Internet Banking. This research work done on fuzzy expert systems that identify the user behavior whether the user behavior is normal or suspicious. Normal behavior regarding the person enters their information to system for transaction being normal if no errors detected and suspicious behavior regarding person enters the information for logging getting errors when logging system again and again and detected as suspicious behavior and transaction declared illegitimate or suspicious. For getting result of normal and suspicious behavior first user enter information for login as input parameters and these information examined to further proceeding the result is as output parameters and system is implemented on real environmental input parameters to verify whether transaction being suspicious or normal.

There is another research work done by Sonam, Pradeep [25]. They purposed a solution to detect fraud using Hybrid Model of Multimodal Biometrics System by using Fingerprint and Face as Traits. In this research work they work on multimodal biometric verification using finger print and face traits instead of bimodal biometric verification. Multimodal system of verification use more than one traits to verification and much more complex than bimodal verification system. In multimodal result getting from every single bimodal verification module and then compare all bimodal verification module results to declare whether allow to proceed or not for transaction. They used minutia score matching method for fingerprint and use block filter to scan image at boundary and extract information from thinned image. After detecting information from thinned image apply binarization in that image can be converted into black and white from grey scale. In next applying thinning algorithm stored ucewidth of ridges in image and single pixels. In last stage apply minutiae extraction in which minutiae from thinned image extracted to match with fingerprint verification pattern. To compare with face use Eigenface to recognize face without warping. For face trait verification use face mask by getting face extraction and then fit mask on some traits like nose, eyes, lips etc. to register important face features and then warping. After warping the resulting face should be same geometry as original or references face.

There is another research work purposed by Ravi, K. Raja, Venugopal. [26]. In their research work they purposed finger print recognition or verification using minutia score matching technique. In this technique block filter is used to extract image from boundaries to preserve or save the quality of image and detail information or minutia can be extracted from thinner image part. For giving access to system fingerprint verification find FMR (false matching ratio) and for not giving users to access the system find FNMR (false non matching ratio). To achieve all these detect problem and then pre-processing the fingerprint test and then extract minutia from testing fingerprint data then match the test result with storing image in database on these condition decided whether verification done ornot.

There is another research work done by V.Vijaya Kumari, Amiete, N.Suriyanarayanan [27]. In their research work they compare different local operators to remove noise from image and calculate peak signal to noise ratio. This technique is beneficial where when we have to make pattern recognition for detecting or verification of fingerprint through scanner for various usage. For getting this first detect edges by taking first and second order derivation. Images have some noise to remove noise apply some external noise filter like salt and pepper, speckle then apply segmentation and find peak signal to noise ratio that's is used to reconstruction quality of image during image compression and getting by dividing maximum valuesof pixels by square root of mean square error.

There is another fraud detection approach presented by C. Sudha,T.NirmalRaj[28].In their research work they purposed

solution to detect fraud technique using K-Nearest Neighbor Algorithm in credit card transaction. This algorithm depend upon three factors. One is distance metrics, second is value of K and third one is distance rule. In algorithm distance metrics used to find or measure to locate nearest neighbors while distance rule decides nearest neighbor lies on which class according to their classification or properties and values of k decide total of number of neighbors to compare. Basically the value of k is chosen on prediction and dataset can be trained by training to compare neighbors on their classification or properties. After getting result done on result base which transaction being legitimate or illegitimate through creditcard.

There is another credit fraud detection mechanism presented by Venkata Ratnam Ganji, Siva Naga Prasad Mannem [29]. In their research work they purposed data stream outlier detection algorithm to detect credit card fraud that totally opposite to K- Nearest Neighbor Algorithm. This technique is basically depend on Unsupervised Learning Approach instead of supervised learning approach. Because in supervised learning algorithm dataset trained to be detect transaction fraudulent or not or also depend on existing record but unsupervised learning approach have no need trained data set to detect fraud and don't depend on existing data. Its only depend on currently normal or abnormal behavior of users who entering data so in given research technique is depend on three things one is stream manager second is query manager and third one is entire window from where user enter data and when enter data values doesn't go to data table for matching or searching record just only scan or current window with object whose k nearest neighbors influenced. By this algorithm fraud can be detected to allow or disallow to proceed transaction.

There is another research work presented by Fang Yu,Wang [30]. In this research work they purposed solution to detect credit card fraud by outlier detection mechanism that based on distance sum. This technique also called outlier mining and is a field of datamining. This algorithm basically check that whether

it is outlier to the nearest object or not of given data objects and detecting those objects that detached with current system or nearest neighbors on that calculate the distance sum. On getting summation values deciding transaction being genuine or not if not genuine then getting attributes of users or customer's behaviors and on bases of those attributes values calculating distance sum between observed values and predefined values and compare them. On base of result decided whether transaction being fraudulent or allow to proceed.

There is another research work done by Prajal, Pranali, Ketan. Jain, Neha [31]. They purposed solution for detecting credit card fraud by decision tree with using two other algorithm. One is luhn's algorithm and other is hunt's algorithm. Where luhn's algorithm used to detect card number, addresses like billing, shipping addresses. This technique use six steps to verify the transaction. In first step check or validate card number by luhn's algorithm with matching address and find outlier detection on base of three values move next to ward four steps to match valid pattern. If pattern matched then apply bayes theorem to detect fraud. If fraud detected then disallow to proceed transaction otherwise transaction being legitimate.

There is another research work presented by Silvia Parusheva [32]. In their research work they comparatively discuss the biometric technologies to authenticate online banking. In this research work two online banking scheme they discussed. One is Single factor identification and second is Multi factor identification. In single factor identification only single factor is involved to proceed or verification that is user name or user id and password. The main problem in single factor identification is password and user id can be cracked easily and bypass by some hackers.In multifactor identification more than one factor can be involved for verification. Mostly common is user id or name with password and some security questions but there are also more multi factors verification factors are common like password with biometric authentication.

There is another research work presented by Alireza, Majid and Alireza [33]. In their research work they purposed new technique to detect fraud in online banking by using hybrid feature of genetic and selection algorithm. In their solution they used neural networks to solving different learning problems by monitoring and neural networks could be diving in input and output layers. In their solution observed silent features of transaction while genetic algorithm used to optimize the searching or observing during transaction and on that observation base transaction being procced or declared fraudulent.

There is another research work done by Pooja,A.D.Thakare, Prajakta, Madhura and Priyanka[34].They purposed solution to detect fraud by genetic k-means algorithm in credit card transaction. In their purposed solution k-mean algorithm used to group distinct attribute values based on transaction and genetic algorithm applied to optimized the values and k-mean algorithm make clustering on increasing number of distinct values or attribute increase. First load or enter the dataset as an input values. Then generate three different values of risk level by applying kmeans clustering algorithm on their critical values that getting on every transaction. After getting risk values by applying genetic algorithm on medium or high risk cluster until obtained results found and then evaluate the fitness of each transaction and that basis decide whether transaction is fraudulent or genuine to proceed.

3. COMPARISON TABLE

All the discussed techniques are compared in the form of table based on parameters as shown in Table I. In this Table, we compare three different fraud detection methods. In the first technique, we see graph database is used that is good for detecting fraud in ATM card transactions. This technique use user account information like name, expiry date, address etc. to check whether transaction is legitimate or fraudulent.

TABLE 1: COMPARISON OF FRAUD DETECTIONTECHNIQUE

Research paper Reference #	Technique/ algorithm	For Credit card	E-banking	Fingerprint usage	Face image usage	Hybrid biometric (Finger & Face)	Comments/ Review
1	Graph database	Yes	No	No	No	No	Use different algorithm
2	Biometric approach	Yes	No	Yes	Yes	No	Use of different parameters
3	Local and global behavior	No	Yes	No	No	No	Complicated process
4	Neural networks	Yes	No	No	No	No	
5	Decision Tree induction algorithm	Yes	No	No	No	No	
6	Hidden Markov model	Yes	Yes	No	No	No	Tough to detect behavior of consumers
7	Supervise d un-supervised	Yes	No	No	No	No	Different techniques to detect fraud and vary by condition and difficult to implement and only suitable for e-banking
8	Bayesian Network	Yes	No	No	No	No	
9	Fuzzy Logic and neural networks	Yes	No	No	No	No	
10	Data Mining Using Support Vector Machines	Yes	No	No	No	No	
11	Improved Multimodal Biometric Architecture	No	Yes	No	No	Yes	
12	secure unified e-payment system	Yes	No	Yes	No	No	

TABLE II: COMPARISON OF FRAUD DETECTIONTECHNIQUE

13	Enhanced Biometric Authentication System	Yes	Yes	Yes	Yes	No	Use different parameters to detect fraud like matching face and fingers with name, pin and pulses
14	whirlpool hash function	Yes	Yes	No	No	No	Some techniques are not suitable for detecting fraud during transaction by credit card and some through e-banking and rarely use of face and fingerprint to verify genuine transaction and some use signature verification to detect fraud, some use biometric pin to detect fraud
15	GSM system	Yes	No	Yes	No	No	
16	secure protocol and certificate verification mechanism	No	Yes	No	No	No / signature verification	
17	Three-Level Security Implementation	No	Yes	No	No	No	
18	datamining concepts	No	Yes	No	No	No	
19	ANN and Logistic Regression	Yes	No	No	No	No	
20	Service Oriented Biometric Model	Yes	No	No	No	No/ Biometric PIN	
21	Freeman Chain Code Representation	Yes	Yes	No	No	No/ Signature verification	
22	handwritten signature identification using graph theory	No	Yes	No	No	No/ Signature verification	
23	Ontology Based Expert-System	Yes	Yes	No	No	No	
24	Detection of User Behavior	No	Yes	No	No	No	
25	Hybrid Model of Multimodal Biometrics	Yes	Yes	No	No	Yes/ face traits	Use face traits to detect fraud
26	minutia score matching technique	No	Yes	Yes	No	No	Mostly techniques or algorithm not suitable for e-banking and some of them use fingerprint and some of them used it in limit conditions and no use of face recognition is available and in some cases different security questions used to verify genuine transaction and difficult to implement algorithms
27	pattern recognition	Yes	Yes	Yes	No	No	
28	K-Nearest Neighbor Algorithm	Yes	No	No	No	No	
29	data stream outlier detection algorithm	Yes	No	No	No	No	
30	outlier detection based on distance sum	Yes	No	No	No	No	
31	Decision tree using luhn's and hunt's algorithm	Yes	No	No	No	No	
32	single factor and multi factor identification	No	Yes	Yes (in some case)	No	No/ Security questions	
33	hybrid feature of selection and genetic algorithm	No	Yes	No	No	No	
34	genetic k-means algorithm	Yes	No	No	No	No	

In the second technique, biometric approach is used for detecting fraud.This technique is good for credit-card transaction but not suitable for online transaction. In this technique, user voice, face image, hand geometry and fingerprint are used for checking whether transaction is legitimate ornot.

In the third technique called local and Global behavior is suitable for checking fraud in online transaction. In this technique, authors monitor the device and account location.This technique use very complex method to detect fraud but did not provide any method to detect fraud in credit-card transaction.

In the fourth technique, neural networks are used for detecting fraud. This technique is only suitable for detecting credit card fraud and not suitable for online fraud detection.They have not used face recognition and biometric and is not suitable fore-banking. Practical implication of this technique is very low.

In the fifth technique called credit card fraud detection using decision tree induction algorithm, there is no use of finger print and face recognition.This technique is only applicable for credit card fraud detection and not support to detect e-banking fraud. Moreover, this technique is complicated to implement because of different condition applied to detect fraud.

In the sixth and seventh techniques, called fraud detection using hidden Markov model and unsupervised profiling. These techniques are good for only detecting credit card fraud detection and somehow suitable for detecting e-banking transaction fraud. They have not used face recognition, biometric and tough to detect consumer's behaviors as these techniques only detect fraud by knowing consumer's behaviors.

In eight, ninth and Tenth techniques are fraud detection using Bayesian network, fraud detection using fuzzy logic, fraud detection using SVM and reduction of false alarm. These techniques are difficult to implement because of various condition and only applicable for credit card fraud detection. They have not used face recognition and biometric and are not suitable for detecting e-banking fraud.

Last three techniques are fraud detecting with use of holistic matching method, classical machine learning and voice base authentication. These techniques are complex to implement. In Holistic matching technique all parts of user face detected for verification and also use some hybrid method to detect facial parts. In classical machine learning and voice based authentication there is no use of face images and finger print verification instead of this used voice based authentication that is difficult to recognize and tough to detect fraud and fraudster can commit fraud easily.

4. PROPOSED METHODOLOGY

There are many techniques or method of fraud detection that we have discussed in this research work.In the comparison table of section III, some methods are used to detect fraud both in e- banking or credit card transaction but mostly methods are not suitable to detect fraud for both kinds of transaction. Some Techniques have used hybrid or multimodal biometric parameters to detect fraud and some of them used bimodal biometric parameters to detect fraud. Some of them used signature verification for detecting fraud and some technique used some algorithms to detect fraud. We have identified some gaps in those methods and want a methodology by which users' personal information can be secured and stop fraudster to commit fraud at earlier stage of transaction. For this purpose, we propose a solution to handle both kinds of transaction such as e-banking or credit card transaction to improve security.

4.1 Gaps in different Techniques

There are many technique or method of fraud detection we discussed in this research work. Some fraud detection method are close to our purpose solution and upon all other methods we chose three closest techniques to compare and below are some gaps in techniques. After finding gaps between these techniques we can purposed new fraud detection techniques to overcome banking fraud rate.

Below figure shows the gaps between those different fraud detection methods.

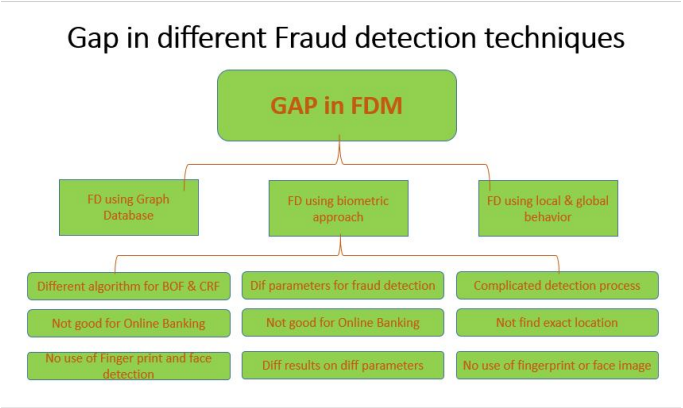

Figure 4: GAP in FDM

In above figure we show the gaps in different fraud detection techniques. All the techniques have some gaps regarding to credit card fraud or online banking. In graph database technique there is no method to prevent online illegitimate transaction and use different algorithms for BOF (Bust out Fraud) and CRF (Credit Card Fraud) to detect credit card fraud detection.

In biometric approach there are different parameters or characteristics to detect fraud and each parameters give different results and this technique is not suitable for online banking transaction.

In local and global behavior we monitor device and locate location of account holders but we don't find exact location and there are a lot of complicated steps to perform detection steps. This technique is not suitable for credit card fraud detection.

4.2 Proposed Solution

There are many method of fraud detection we discuss in this research work. We can find some gaps in every techniques that we discussed above in this paper so now us presenting a method of fraud detection that will overcome the issue of fraud in banking sectors. In this solution we deal both way of transaction one is by credit-card transaction and other is online transaction. In credit-card transaction we use finger print for comparison whether transaction is legitimate or fraudulent and for online or e-banking transaction we use face-image for comparison on run time on login with account holder so we can find by face-image whether online transaction is legitimate or fraudulent and by biometric verification find credit card transaction is genuine or not and detect fraud at earlier stage. This method is better than others because by finger print we can overcome both credit-card and bust-out fraud and by face-image we can overcome all online transaction issues.

4.3 Pseudo Algorithm

Step 1: Load dataset

Step 2: Check the transaction

Step 3: If transaction is online then compare face with your existing face images.

Step 4: If match then proceed transaction.

Step 5: else: Do not allow to proceed transaction and go for again to compare face.

Step 6: If transaction is by credit-card then compare finger print with your existing fingerprints.

Step 7: If match then proceed transaction.

Step 8: Else: Do not allow to proceed transaction and go for again to compare fingerprints.

Step 9: If transaction does not match then transaction is fraudulent and start investigation.

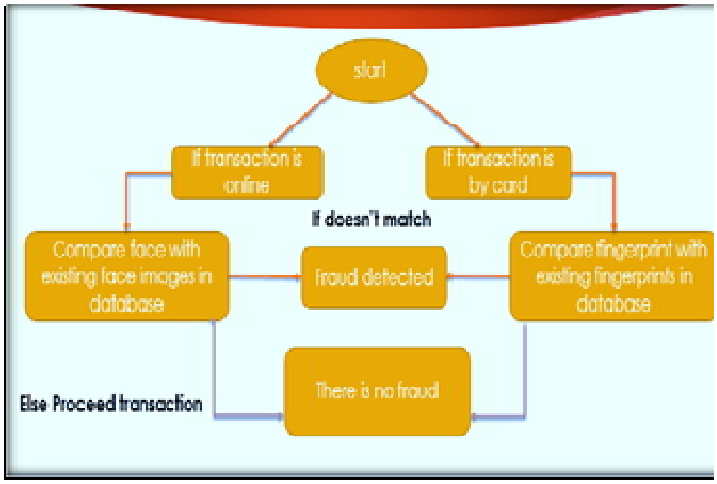

Figure 5. Graphical representation of Proposed System

4.4 Working and implementation of the system

This proposed solution is implemented on MATLAB. For implementation first we create dataset then load and apply verification method to verify user information and detect fraud.

This technique is implemented through Eigen vectors and Eigen values. Images of faces and fingerprints taken during getting consumers information on creation of accounts, then these images scanned during transaction and matched them on basis of Eigen values. Eigen vector is basically a non-zero vector that changes at most by a scaler factor when linear transformation applied and their corresponding Eigen values denoted by lambda λ. Consumers images already saved in database and data store in form of tables just like matric and when user try to perform verification user facial and biometric information scanned and verifying with already saved images on bases of Eigen vectors and Eigen values and on that values we allow users to proceed transaction or declare transaction fraudulent if doesn't matched.

$$\mathbf{A}\cdot\mathbf{v} = \lambda\cdot\mathbf{v}$$

Here A is basically matrix and V is Eigen vector and λ is Eigen Value.

$$\mathbf{A}\cdot\mathbf{v}-\lambda\cdot\mathbf{v} = 0$$
$$\mathbf{A}\cdot\mathbf{v}-\lambda\cdot\mathbf{I}\cdot\mathbf{v} = 0$$
$$(\mathbf{A}-\lambda\cdot\mathbf{I})\cdot\mathbf{v} = 0$$

To perform this evaluation or verification we do some steps.

- **Dataset Preparation**

For implementation, data set is organized for 40 persons and every person has 10 different images of face and fingers with different poses. Therefore, the total number of images are 400. For arrangement of dataset, we have created 40 folders for 40 persons and each folder contain 10 images of individual person. Folder names start from s1 to s40 and every image in folder named with 1 to 10 integer values. These images are in greyscale form. Greyscale images are those in which each pixel has single value. All images have same dimension, same resolution and also have the same extension. Dimensions of every image is 92 * 112 pixels and there extensions are.pgm.

- **Dataset Loading**

After arranging dataset, next step is to load dataset in MATLAB. For loading dataset, we make function load_database (), no value is passed to this function but this function return numeric values of images where returned numeric value is stored in variable named‘ output_ value’. After this, we take two variables named ‘loaded’ and ‘numeric_images’. After that, we use if condition to check whether loaded variable is empty or not. If the loaded variable is empty then load dataset and dataset is saved permanently. The dimension of every image is 92*112 pixels that is equal to 10304 pixels so we take 10304 zeros for 40 times because we take images of 40 people. And later pixels values of images replace these zeros. After that, we use ‘strcat_function’ inside loop to concatenate the names of folders s1 to s40 and names of images from 1 to 10 with extensions of images.

- **Read the Dataset**

In the next step, we use 'imread_function' to read all concatenated images and then load the images.After that we use 'reshape_function' to convert the images into single column matrix and then use 'size_function' to get size of rows and columns of images. For memory reduction, we convert images into 8bit unsigned integers by using 'uint8' function. Last step is to declare 'loaded' variable with 1 because we don't want more dataset to load and prevent function to load dataset that's why we declare loaded=1.

- **Dataset Verification**

For face and finger recognizing we first load dataset and after apply' random' function to generate random index. By using the sequence of random index image that will recognize loaded and other images also loaded in other variable named 'rest_of_images'. After that we calculate the mean of all images and subtract the mean value from images.

$$|A|$$

$$A-|A|$$

After it we calculate eigenvectors on those images and upon having eigen values created the matrix where each row contain the signature of individual image. In the last step, we subtract the mean value from image which we want to recognize and multiply it with Eigenvector.

$$D = (|A| - \text{IMAGE SELECTED})$$

$$E = D * \text{Eigen Value (Lambda)}$$

Finally, based on difference between current signature of image and first signature of image that we calculated E we predict the recognized face and finger intelligently. The accuracy of this method is almost 90%.

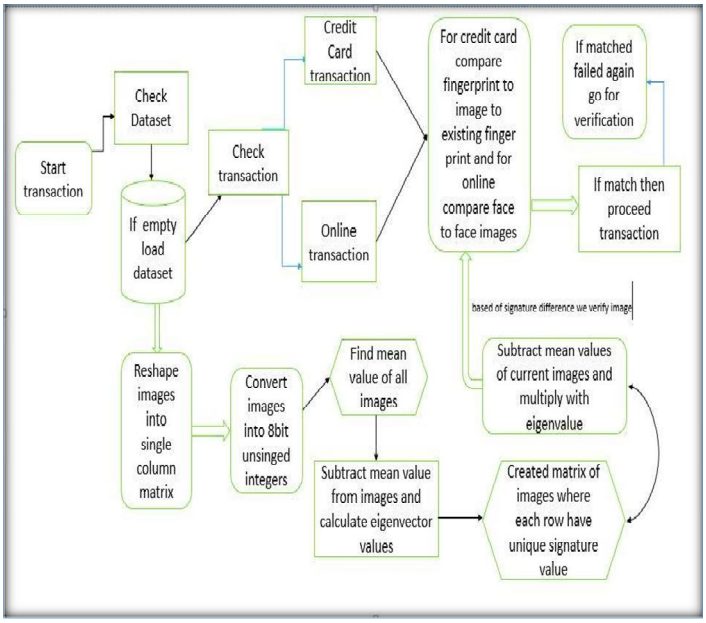

Figure 6. Work flow of the system

Now Above Diagram is Graphical representation of Whole Proposed Methodology and How Our Proposed System Work efficiently and intelligently and detect fraud at initial state and differentiate genuine and fraudulent transaction.

5. EVALUATE THE RESULTS

In this section, we discuss the different outputs of proposed face recognition and fingerprint detection method. From the implementation, we analyze the results of proposed system. Proposed system is implemented and validated in two steps. First step is face recognition while second step is fingerprint recognition. Face recognition is used during the verification of online or e-banking transaction while Finger print recognitionis used during the verification of credit card transaction. We get almost 90% accurate result during verification by both way of transaction.

5.1 Face Recognition:

Proposed face recognition method is almost 90% accurate regardingfaceverifications.Figure4showsthefacerecognition results part1

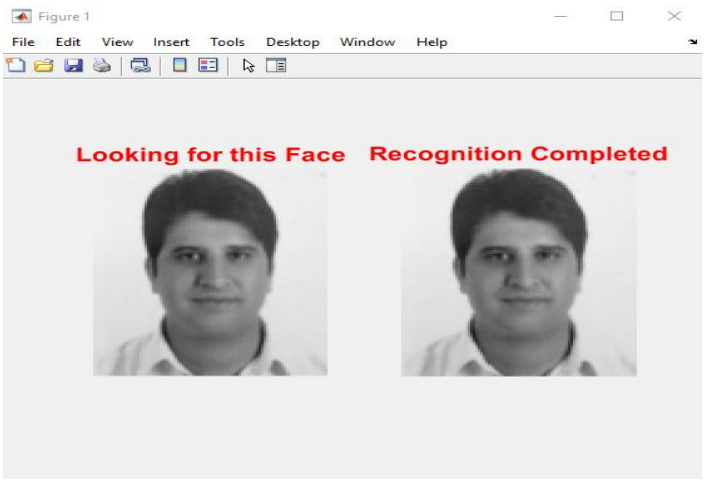

Figure 7. 1st facial image result

Above figure shows the result of successfully transaction by recognition of face with existing face image while performing transaction through E-Banking. This result is captured during verification process of online transaction and face is almost matched to existing face image in dataset and face is matched intelligently on different poses. In above result right side image shows the save face images in dataset while left side image shows the capturing face during verification and above figure clearly show facial recognition and verification on different poses.

Figure 8. 2nd Facial image result

Above figure 8 shows the result of successfully transaction by recognition of face with existing face image while performing transaction through E-Banking. This result is captured during verification process of online transaction and face is almost matched to existing face image in dataset and face is matched intelligently on different poses. In above result right side image shows the save face images in dataset while left side image shows the capturing face during verification and above figure clearly show facial recognition and verification on different poses.

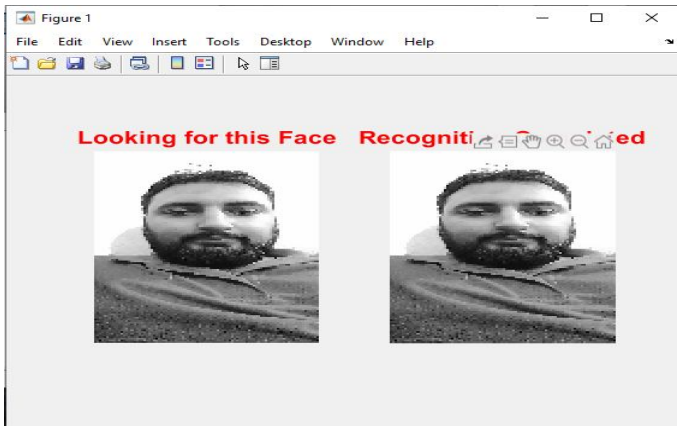

Figure 9. 3rd Facial image result

Above figure shows the face verification during e-banking transaction. Left side image is required to verify and right side image taken during face scanning and verification done on different face side. Above results show face recognition with different face pose but this result show face verification from different face sides. Left image required face from left side and scanned image have rightside of face.This methodology works on verifying face with different face poses and positions.

Figure 10. 4th Facial image result

Above figure shows the result of successfully recognition of face during online transaction. We know this algorithm works on verification of face on different pose so in above pic it's clearly shows that left side of image that we required during online transaction have different face pose then the image scanned on run time. Right side image scanned during transaction and have open eyes but we required scanned image that have same to left side image with closed eyes. This result shows the accuracy and reliability of algorithm that we are using for transaction verification and system intelligently verified required faces.

Figure 11. 5th Facial image result

Above image shows the result of successfully transaction of e-banking done by lady. In above image we can clearly see that the left side of image is actually what we required for verification and the right side of image has taken during online transaction that later matched to left side or saved image of lady in data base and on this verification system successfully grant permission to lady to do transaction. In both images we can see that verification done on different poses of faces intelligently.

Figure 12. 6th Facial image result

Above image shows the face verification result of transaction bye-banking that dine by man with different face pose.The left side of image is actually what we required for verification and saved in database and right side image is scanned during verification process. We clearly see that both images belong to same person with different face poses. Image that captured during verification have closed eyes and doing smile while image that we require have open eyes and without smile. This algorithm works efficiently and intelligently to verify faces with different face poses.

Figure 13. 7th Facial image result

Above figure shows the face verification during e-banking transaction. Left side image is required to verify and right side image taken during face scanning and verification done on different face side. Above results show face recognition with different face pose but this result show face verification from different face sides. Left image required face from left side and scanned image have right side of face.This methodology works on verifying face with different face poses and positions.

5.2 Fingerprint Recognition:

Proposed fingerprint recognition method is almost 90% accurate regarding fingerprint verifications. Figure 6 shows the fingerprint recognition results part 1.

Figure 14. 1st biometric result

Above Figure 14 shows the result of successfully recognition of finger print with existing finger prints while performing transaction through credit card. Above result is captured during the verification process while doing transaction through credit card. The right side image is basically already saved in dataset and system looking for the required fingerprint from dataset that user scan during verification process and after successful getting required result recognition completed and grant access to do transaction and shows the result.

Figure 15. 2nd biometric result

AboveFigure15showstheresult of successfully recognition of finger print with existing finger prints while performing transaction through credit card. This is the second result that taken during credit card transaction after verification of fingerprint. In result the right side image is basically saved in

dataset and system looking for the required fingerprint from dataset that user scan during verification process and after successful getting required result recognition completed and grant access to user to do transaction.

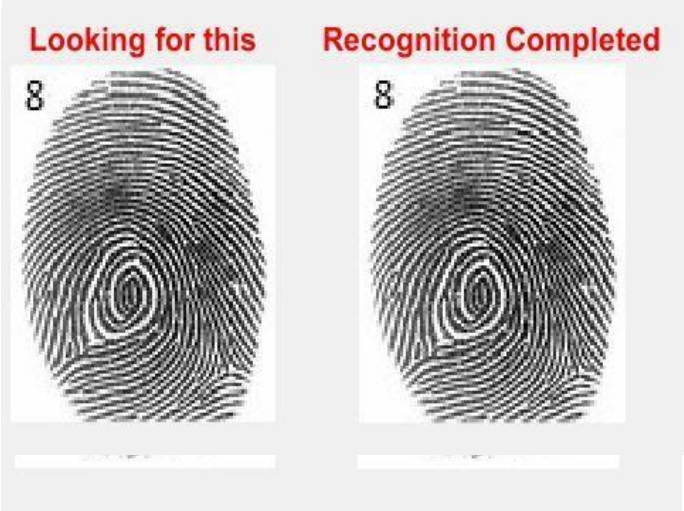

Figure 16. 3rd biometric result

Above figure shows the result of fingerprint verification taken during transaction by credit card. Result shows two images one is on leftside and other is on rightside.The leftside image is that already saved in dataset and we looking this for verification while right side image is taken during fingerprint scanning and in result its clearly shows that scanning fingerprint matched to saved fingerprint in dataset and system allow user to do transaction and user did it successfully.

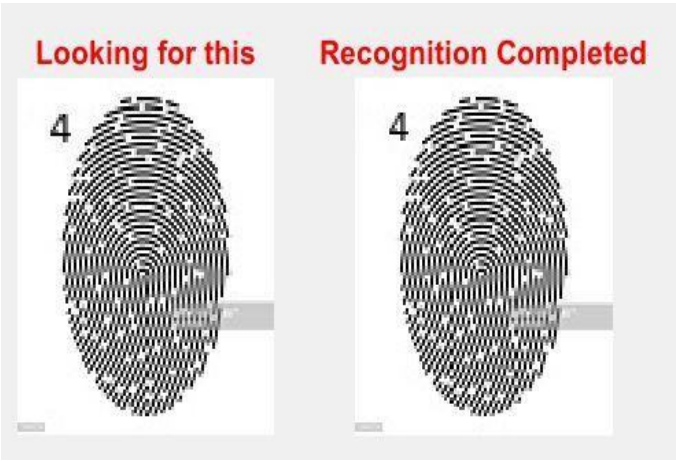

Figure 17. 4rth biometric result

Above figure also shows the result of verification of fingerprint during transaction through credit card. Right side of image scanned during verification and left side of image is actually what we required for transaction or verification and saved already in dataset while user make account. In above result it clearly mention about successfully recognition of scanning fingerprint with save fingerprint image and on that base system allow user to do transaction.

Above figure also shows the result of verification of fingerprint during transaction through credit card. In above figure Right side of image scanned during verification and left side of image is actually what we required for transaction or verification and saved already in dataset while user make account. In above result it clearly mention about successfully recognition of scanning fingerprint with save fingerprint image and on that base system allow user to do transaction.

6. CONCLUSION AND FUTURE WORK

We provide an optimal solution to overcome the issue of fraud detection in banking sectors. A number of fraudster try to access user's confidential details to commit fraud and many researchers give solution to detect and prevent fraud. We have to give best solution for securing both way of transaction and prevent fraudster to commit fraud by using intelligent hybrid fraud detection mechanism with facial recognition and fingerprint verification. In our proposed method we try to overcome two types of frauds and provide solution for both way of transaction. One is online banking fraud and other is credit card fraud. To prevent the credit card fraud we compare finger prints with existing finger prints and to prevent the e-banking transaction fraud we comparing face with existing face images on different poses. For this we scan face or facial expression and fingerprints of users during transaction process and comparing it with our saved dataset of users who try to perform transaction. After evaluation this solution is almost work 90% accurate on comparing fingerprints and face images during transaction on different poses and by this system intelligently verify and differentiate fraudulent and genuine transaction. So our proposed solution will play important role for society and banking system and give efficient results for detecting fraud and this should be beneficial for users who use banking systems for their accounts and transaction. For future we left the problem of transaction by check and hope so we will overcome this issue soon.

REFERENCES

[1] Sonali Sen, Trishita Mukherjee, Sunanda Pal, Sumana Ghosh, Fraud pattern recognition in banking sector using graph database,Vol6,Issue 6, jun 2018,JCSE.

[2] Suman, Mitali Bansal, Survey paper on Credit card fraud detection, Vol 3, Issue 3, March 2014,IJARCET.

[3] Stephan Kovach, Wilson Vicente Ruggiero, Online banking fraud detection on local and global behavior, 2011,ICDS.

[4] Divya Murli, Shailesh Jami, DevikaJog, SreeshaNath,Credit Card Fraud Detection Using Neural Networks, Vol 2 (02), March-April 2014, ISSN 2321-2543, pg.84-88.

[5] Jyoti R. Gaikwad, Amruta B. Deshmane, Harshada V. Somavanshi, Snehal V. Patil, Rinku A. Badgujar, Credit

Card Fraud Detection using Decision Tree Induction Algorithm, ISSN: 2278-3075, Volume-4 Issue- 6, November2014.

[6] SHAILESH S. DHOK, Credit Card Fraud Detection Using Hidden Markov Model, ISSN: 2231-2307, Volume-2, Issue-1, March2012.

[7] R. J. Bolton and D. J. Hand, "Unsupervised profiling methods for fraud detection", in Conference on Credit Scoring and Credit Control 7", Edinburgh, UK, 5-7 Sept.,2001.

[8] D. S. G. S.Saranya, "fraud detection in credit card transaction using bayesian network," international research journal of engineering and technology, vol. 4, no. 4, April2017.

[9] a. a. pansy khurana, "credit card fraud detection using fuzzy logic and neural network," SpringSim,2016.

[10] A.A.Nancydemla,"credit card fraud detection using svm and reduction of false alarms," International journal of innovations in engineering and technology, vol. 7, no. 2,2016.

[11] M. I. Omogbhemhe1*, I. B. A. Momodu2 and S. Awojide3, 1-6, 2018 "An Improved Multimodal Biometric Architecture for Securing Online Payment". 28(5):; Article no.CJAST.31471 ISSN:2457-1024.

[12] Charles K. Ayo and Wilfred Isioma Ukpere 4 August, 2010 "Design of a secure unified e-payment system in Nigeria: A case study", African Journal of Business Management Vol. 4(9), pp. 1753-1760,. ISSN 1993- 8233 ©2010 Academic Journals.

[13] F.O. Aranuwa and G. B. Ogunniye, September 2012. "Enhanced Biometric Authentication System for Efficient and Reliable e-Payment SysteminNigeria",InternationalJournalofAppliedInformationSystems (IJAIS) – ISSN : 2249-0868 Volume 4–No.2,

[14] Doaa Yaseen Khudhur, Saif Saad Hameed, Shokhan M. Al-Barzinji (2018) "Enhancing e-banking security: using whirlpool hash function for card number encryption", International Journal of Engineering & Technology, 7 (2.13)281-286.

[15] A.Salma1, C.Sarada Devi2, V. Saranya3, April 2014. "Smart Card for Banking with Highly Enhanced Security System", SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE)– volume1 issue2.

[16] Mridha M., Kamruddin N., Aloke K., Saha, Akhtaruzzaman A., 2017 "A New Approach to Enhance Internet Banking Security", Vol. 160, No. 8, International Journal of Computer Applications.

[17] Emeka Reginald Nwogu "Improving the Security of the Internet Banking System Using Three-Level Security Implementation", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.6, December2014.

[18] Sayali Kishor Rodge , May-2016. "study of data mining on banking database in fraud detection techniques", Volume: 03 Issue: 05, International Research Journal of Engineering and Technology(IRJET).

[19] E. D. Yusuf Sahin, 2011 "detecting credit card fraud by ann and logistic regression".

[20] Omogbhemhe Izah Mike, August 2018 "Service Oriented Biometric Model Suitable for Securing ATM System," Vol 9, Issue 8ISSN.

[21] Aini Najwa Azmi & Dewi Nasien "Freeman Chain Code (FCC) Representation in Signature Fraud Detection Based On Nearest Neighbour and Artificial Neural Network (ANN)Classifiers".

[22] Tomislav Fotak, Miroslav Baca, Petra Koruga "Handwritten signature identification using basic concepts of graph theory".

[23] QuratulainRajput,NidaSadafKhan,AsmaLarik&SajjadHaider,2014. "Ontology Based Expert-System for Suspicious Transactions Detection", Vol. 7, No. 1; Computer and Information Science.

[24] Manish Bendale , Saurabh Dorle, Dr. Nitin N. Pise, "An Intelligent System for Detection of User Behavior in Internet", International Journal of Advance Research, Ideas and Innovations in Technology.ISSN:2454- 132X.

[25] Sonam Shukla, Pradeep Mishra, March 2012 "A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits". Volume-2, Issue-1, International Journal of Soft Computing and Engineering (IJSCE) ISSN:2231-2307.

[26] RAVI. J, K. B. RAJA, VENUGOPAL. K. R, 2009 "FINGERPRINT RECOGNITION USING MINUTIA SCORE MATCHING", Vol.1(2), , 35-42, International Journal of Engineering Science and Technology.

[27] V.Vijaya Kumari, Amiete, N.Suriyanarayanan, "performance measure of local operators in fingerprint detection".

[28] T. R. C.Sudha, 2017. "credit card fraud detection in internet using k nearest neighbour algorithm," vol. 5, no. 11, IPASJ international journal of computer science.

[29] Venkata Ratnam Ganji, Siva Naga Prasad Mannem, "Credit card fraud detection using anti-k nearest neighbor algorithm", International Journal on Computer Science and Engineering(IJCSE).

[30] N. W. Wen -Fang Yu, 2009. "Research on credit card fraud detection model based on distance sum," in International joint conference on artificial intelligence, Hainan Island, China.

[31] Prajal Save, Pranali Tiwarekar, Ketan N. Jain, Neha Mahyavanshi, March 2017 "A Novel Idea for Credit Card Fraud Detection using Decision Tree", Volume 161 – No 13,. International Journal of Computer Applications (0975 –8887).

[32] Silvia Parusheva, September 2015. "A comparative study on the application of biometric technologies for authentication in online banking", Vol. 39 No. 4.Egyptian Computer ScienceJournal.

[33] Alireza Pouramirarsalani, Majid Khalilian, Alireza Nikravanshalmani, August 2017. "Fraud detection in E-banking by using the hybrid feature selection and

evolutionary algorithms", VOL.17 No.8, IJCSNS International Journal of Computer Science and NetworkSecurity.

[34] Pooja Chougule, A.D. Thakare, Prajakta Kale , Madhura Gole, Priyanka Nanekar,"Genetic K-means Algorithm for Credit Card Fraud Detection", Vol. 6 (2) International Journal of Computer Science and Information Technologies, , 2015,1724-1727.

[35] Stephen Gbenga Fashoto, Olumide Owolabi, Oluwafunmito Adeleye and Joshua Wandera,"Hybrid Methods for Credit Card Fraud Detection Using K-means Clustering with Hidden Markov Model and Multilayer Perceptron Algorithm", British Journal of Applied Science & Technology Articleno.BJAST.21603.