OPEN ACCESS Freely available online

Journal of Research and Development

Research Article

Use of Digital Signature Verification System (DSVS) in Various Industries: Security to Protect against Counterfeiting

V Thangavel*

Department of Library Sciences, St. Francis Institute of Management and Research, Mumbai, India

ABSTRACT

This study proposes a handwritten signature verification method based on improved combined features, which combines dynamic features and static features by using the complementarity between classifiers and score fusion. The significance of this study is for the purpose of verifying the authenticity of the signature and protecting the safety of customer property by extracting more comprehensive and representative signature features. The traditional approach for signature verification in the bank uses the human sense organ of eyes and most of the time human judgment based on what is seen can be queried, especially in cases of impersonation, forgery, identity manipulation to name a few. Today the quest for fast money has driven a lot of frustrated people into various illegal acts and signature counterfeiting is one of the most common of this act. Banks and their customers occasionally fall victim because they lack adequate technology to verify signatures. Recently in most banks there are various cases of banking staff denying services to customers due to signature differences. This has resulted in a lot of misunderstandings, insults, quarrels and even losses to most financial institutions. This work presents a digital signature verification system to enhance customer services in the banking industry, with the aim of improving the staff customer relationship within the Banking domain. This will be developed using image acquisition tool, image processing tools and machine learning. (Clustering technique). Signature has been globally accepted as a general means of official authentication, for legal documents, cheques, bank drafts, tellers, withdrawal slaps, deposit slops, receipts and other official documents. This means has been widely accepted and implemented in all banking sectors due to its simplicity, confidentiality and unique nature, also compared to other biometric verification systems, human signature is one of the few biological modalities that remain the same over time. This authentication means has been abused time and time again through impersonation (identical twins) and forgery, as a result has caused a lot of damage and losses to individuals and financial institutions. This research work addresses this challenge using artificial intelligent technique to present a novel signature verification system that helps authenticate business transactions in all financial institutions. The growing number of online transactions and contracts need stronger protection. Electronic signatures are undoubtedly a huge step forward in efficiency, but electronic signature counterfeiting is extremely real and worrying, especially as large become increasingly dependent on them, especially at a time when the globe is facing a pandemic. Traveling for the sake of conducting business has become a luxury since the world has come to a halt. Today electronic signature is very important in carrying out day-to-day business but at the same time, we need to be increasingly cautious and alert to prevent any e-signature fraud with carefully considered practices and procedures.

Correspondence to: V Thangavel, Department of Library Sciences, St. Francis Institute of Management and Research, Mumbai, India; E-mail: v.thangavel@rocketmail.com

Received: 16-Nov-2023, Manuscript No. JRD-23-28044; **Editor assigned:** 20-Nov-2023, PreQC No. JRD-23-28044 (PQ); **Reviewed:** 05-Dec-2023, QC No. JRD-23-28044; **Revised:** 11-Feb-2025, Manuscript No. JRD-23-28044 (R); **Published:** 18-Feb-2025, DOI: 10.35248/2311-3278.25.13.290

Citation: Thangavel V (2025) Use of Digital Signature Verification System (DSVS) in Various Industries: Security to Protect against Counterfeiting. J Res Dev. 13:290.

Keywords: Digital signature; Signature verification; Vector machine support; Combined signature; Dynamic time warping; Forgery; Bank fraud; Simple forgery; Random forgery; Skilled counterfeiting; IPC; Punishment for fraud; Fake signature; Forging signature; Tracking stimulation; Freehand forgery; Lifted forgery; Misuse of digital signature; Fraud investigation office; Wire fraud; Identity theft; Stolen cheque; Altered cheque; Cheque kitting; Skimming of card; Stealed bank cards; Phishing and internet fraud; International crime; High-tech crime; No-scene crime; Faceless crime; eMus; eMudhra

INTRODUCTION

In recent years it has been seen that personal identity as an authentication is one of the growing interests. Therefore, consider authentication as a deep down part of social life. Higher security in increasing demand puts much more attention on biometrics. Individual recognition based on personal characteristics) for verifying a person. Generally, among distinct biometric parameters for identification of a person on any document drawn through a uniquely outlined writes as an identity using a signature. Any individual daily uses it for any legal documents whenever required. A signature through any person conveys an image of pattern of pixels. Therefore, one of the most common and effective ways to identify a person through signature is handwritten signature identification. From different reviews of distinct proposed systems clarifies more focus on verification than that of identification due to the use of signature in daily life use. So, the serious matter arises with this system when anyone tries to replicate that individual's signature for any purpose. There are mainly two types of verification of signature, i) Offline/Static verification ii) Online/Dynamic verification. Static verification system captures signature shape so input data includes x, y coordinates of signature. The dynamic verification system uses devices for capturing surplus information such as pen up and down, time, pressure, azimuth, etc. Previous research listing and describing the below approaches for signature verification are described at various levels in this article [1].

Online handwritten signature verification process

Online handwritten signature verification is a process of testing whether a signature is genuine or fake. A signature can easily be forged. Forgeries of signatures are classified into three types: Simple, random and skilled counterfeiting.

Random forgery: It is produced by the forger without knowing the writers name as well as real signature.

Simple forgery: In which the forger has no idea what the signature to be forged looks like. This is the easiest type of counterfeit to detect because it is usually not close to the appearance of a genuine signature. This type of counterfeit will sometimes allow an examiner to identify who made the counterfeit based on the handwriting habits that are present in the forged signature.

Skilled forgery: In which the forger has a sample of the signature to be forged. The quality of a simulation depends on how much the forger practices before at-tempting the actual forgery, the ability of the forker and the forgery's attention to detail in simulating the signature. A skilled counterfeit looks more like the genuine signature. The problem of signature verification becomes more and more difficult when moving from simple to skilled counterfeiting. Currently, there is a growing demand for the processing of individual identification to be faster and more accurate, therefore the design of a signature verification system becomes an important challenge.

MATERIALS AND METHODS

Background of signature verification systems

The detailed background about signature verification is discussed. The module of signature verification system is shown in the Figure 1.

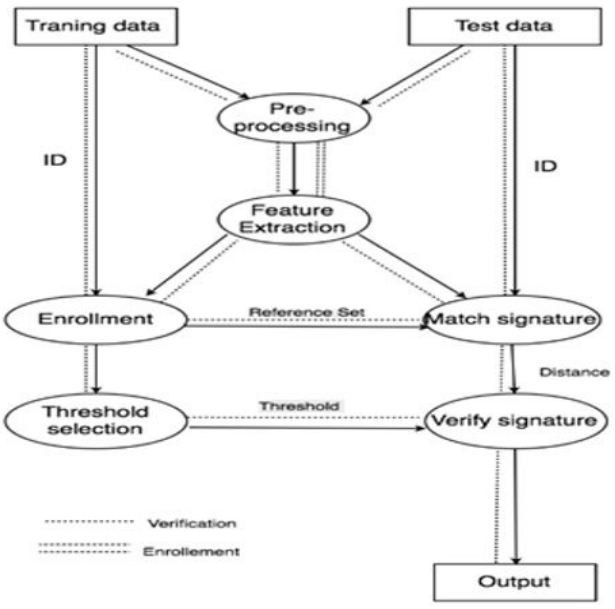

Figure 1: Module of signature verification systems.

Signature database: The biometric research laboratory, ATVS, of the Universidad Politécnica de Madrid, has promoted the plan of action and the development of the MCYT project, in which the design and acquisition of a large scale biometric bi-modal database, involving fingerprints and signature traits, has been accomplished. Although there are some other commercial and forensic partners within. In the case of the MCYT signature subcorpus, 25 client signatures and 25 highly skilled forgers (with natural dynamics) are obtained for everyone. Both on-line information (pen trajectory, pen pressure and pen azimuth=altitude) and offline information (image of the written signature) are considered in the database. Therefore, 330 ×

(25+25)=16500 signature samples are considered in the MCYT baseline on-line corpus. Since the acquisition of each on-line signature is accomplished dynamically, a graphics tablet is needed. The acquisition device used is a WACOM pen tablet, model. The sampling frequency of the acquired signals is set to 100 Hz, taking into account the Nyquist sampler criterion, as the maximum frequencies of the underlying bio-mechanical movements are always below 2030 (Figure 2) [2].

Figure 2: Digital signature-mode.

Pre-processing: Pre-processing of online signatures is commonly done to remove variations that are thought to be irrelevant to the verification performance. Re-sampling, size and rotation normalization are among the common pre-processing steps. In the pre-processing phase, the signature is undergoing some enhancement process for extracting features. The signature images require some manipulation before the application of any recognition technique. This process prepares the image and improves its quality to eliminate irrelevant information and to enhance the selection of the important features for recognition and to improve the robustness of features to be extracted. Moreover, pre-processing steps are performed to reduce noise in the input images and to remove most of the variability of the handwriting. For online signatures, some important pre-processing algorithms are filtering, noise reduction and smoothing. They are also other pre-processing steps such as the pen-up durations and drift and mean removal, time normalization and stroke concatenation before feature extraction. To compare the spatial of a signature, time dependencies must be eliminated from the representation. Certain points in the signature such as the starting points and the end points of a stroke and the points of an orbit change, carry important information. These points are the critical points and are extracted and remained throughout the process (Table 1) [3].

Table 1: List of common features.

S. no	Description
1	Coordinate x(t)
2	Coordinate y(t)
3	Pressure p(t)
4	Time stamp
5	Absolute position $r(t)=\sqrt{x^2(t)+y^2(t)}$
6	Velocity in x v_x (t)
7	Velocity in y v_y (t)
8	Absolute velocity $v(t)=\sqrt{v^2_x}$ (t)$+v^2_y$ (t)
9	Velocity of r(t) v_r(t)
10	Acceleration in x a_x(t)
11	Acceleration in y a_y(t)
12	Absolute acceleration $a(t)=\sqrt{x^2(t)+y^2(t)}$

Extraction: Signature verification techniques employ various specifications of a signature. Selecting the features to be extracted has a huge effect on the accuracy of the signature verification system. It is also the most difficult phase of the signature verification system due to the different shapes of signatures and different sampling situations. The feature extraction process represents a major tackle in any signature verification system. Even there is no guarantee that two genuine signatures of a person are the same. (Intrapersonal variations). Its difficulty also stems from the fact that skilled forgers follow the genuine pattern (Interpersonal variations). This is unlike fingerprints or irises where fingerprint or iris from two different persons varies widely. Ideally, interpersonal variations should be much more than the intrapersonal. Therefore, it is very important to identify and extract those features that minimize intrapersonal variation and maximize interpersonal variations.

Table 1 shows the list of common features. There is a lot of flexibility in the choice of features for verification of a signature extracting information from a signature is classified into two types:

- Parameter function based approach.
- Function feature based approach.

Parameter function based approach: Signature verification systems differ both in their feature selection and their decision methodologies. Features can be classified into two types: Global and local. Global features are features related to the signature, for example, the average signature speed, signature bounding box and Fourier descriptors of the signatures trajectory. Local features correspond to a specific sample point along the trajectory of the signature. Examples of local features include distance and curvature change between successive points on the signature trajectory. The most commonly used online signature acquisition devices are pressure-sensitive tablets capable of measuring forces exercised at the pen-tip, in addition to the coordinates of the pen. The pressure information at each point along the signature trajectory is another. A commonly used local feature. In some of these features are compared to find the more robust ones for signature verification purposes. Other systems have used genetic algorithms to find the most useful features.

Function feature based approach: In the function feature based approach the signature is characterized in terms of a time function whose values constitute the feature set, such as position, speed, pressure, etc.

Verification: After applying the feature extraction process, the test signature and the reference signature are compared with the minimum of the dissimilarity values, average of all the dissemblances and the maximum of all the disparities. Choosing any of the above dissimilarity values a decision is made whether it is a counterfeit signature or a genuine signature. This comparison is done using a threshold value for all the reference and test signature; if the value is approximately equal to the benchmark signal value, then it is assumed to be a genuinely signed signature and if the dissimilarities are above that threshold value the signature is rejected. This threshold value can be identical for all the signature or it can also be different for each of them.

Common threshold: Common threshold is more advantageous because it has the optimal threshed for all the writers. This value is selected after calculating the dissimilarities of the data signatures and a common threshold is chosen based on the minimum error the criterion.

Author/writer dependent threshold: In this type of threshold the writer is limited to one single person. The data for this threshold should be larger compared to the regular data. Here in this type of threshold selection the writer modifies the value every time after each enrolment.

A overview of handwritten signature

Handwritten signatures are widely used in life. With the development of machine learning and artificial intelligence, the research on handwritten signature verification is also deepening.

In terms of signature data collection methods, there are mainly two types. Offline signature image and online signature data.

Offline signature image refers to the handwritten name of the author on the paper, which is then transmitted to the computer through the scanning device to form the signature and then verified according to the image features. Online signature refers to verification based on signature tracks, such as coordinates and pressures during writing. In this paper, an intelligent pen with pressure sensor and camera is used to write the name on the paper with full dots. In the process of writing the signature, the offline image and online data are collected in real time. Signature verification usually includes two stages of training and testing. In the training stage, different numbers of real signatures are used for pre-processing and feature extraction and then put into the classifier to obtain the model. In the test phase, the signatures are put into the classifier for comparison and output verification result. In the feature extraction stage, offline signature image features are called static features, which are mainly divided into local features and global features. Local features are mainly It is divided into texture features and gradient features and global features are mainly geometric features. Online signature data features are called dynamic features, which are mainly divided into parameter based features and function based features. Parameter based mainly refers to the signature duration and the number of pen tip upwards. Functional based features mainly refer to signature trajectories and pressure data. Dynamic features based on functional features generally have better results [4].

Verification methods: There are two main verification methods, model based verification and remote verification. Model based methods mainly describe data distribution by generating models such as Hidden Markov Model (HMM), CNN and SVM. The distance based approach mainly uses the distance measurements to compare the test signature with the reference signature through DTW. This paper uses SVM to process offline signature images and DTW to process online signature data.

There are two main difficulties in signature verification. One is that there is a large intra class and inter class variability. The author's real signature will also change with time, age and other factors and the forger will also imitate the signature with a lot of training in advance, so it is necessary to extract and select more comprehensive and representative signature features. Second, in real life scenarios, only a small number of real signatures can insufficient data is also a problem that needs to be solved. In order to solve these challenges, this paper proposes a score fusion method based on accuracy weighing, which combines the static features of offline signature images and the dynamic characteristics of online signature data through scoring fusion. Specifically, the image and data are pre-processed and feature extracted respectively and then the images and data are verified by SVM and DTW respectively. Through the two classifiers, we can get the verification results and decision scores of offline signature and online signature. Due to the different verification results between classifiers, there is a certain degree of complementarity. Finally, we use score fusion to offline and online combination and solve the problem of complementarity between classifiers. The rest of the paper is organized as follows:

Section 2 introduces related work of this study. Section 3 gives a detailed introduction to the proposed method. Section 4 is the experimental results and discussion. Section 5 presents the conclusion.

Offline signature verification and online signatures verification: In the offline signature verification system an image of a signature is captured by a digital camera or obtained by scanning an signature, which is on a paper or a document and then different features are extracted such as eccentricity, kurtosis skewness etc., while in the case of online signatures verification used the dynamic features of the image which is taken at the time of signature are made such as pressure, coordinates etc.

Punishment for fraud signature in India

India code-section details: Anyone who commits forgery, intending that the forged document or electronic record shall be used for the purpose of fraud, shall be punished with imprisonment of either description for a term which may extend to seven years and shall also be liable to fine.

The law of fake signature: The general penalty for forgery is two years and if forgery committed relating to making false documents, then the penalty can be extended up to ten years and if false will is related to false will or any valuable security then the punishment extended to life imprisonment.

Forging signature crime: Forging a signature is a form of false personification and a designated crime under the IPC (Indian Criminal Code), hence the person forges the signature is always at risk since the person whose signature has been forged, can always file a complaint for the offence by suppressing his prior consent to that effect.

Advice-what can I do if someone forged my signature in India: Submit a complaint with the police alleging forgery by which the matter will proceed to the court and the court upon application from your side orders the signatures to be tested by the forensic lab and that should do.

Types of handwriting forgery

Falsified/Forgery: It is possible to commit a crime by forging your own signature. Forgery is the creation of falsified material or the alteration of any writing with the purpose of defrauding or cheating. There are four basic types of counterfeiting traced, simulation, freehand and lifted. There are four basic types of counterfeiting traced, simulation, freehand and lifted [5].

- Tracking/Tracing
- Simulation
- Freehand
- Lifted forgery

Tracking/Tracing: There are a few different ways to do traced forgeries. With overlays as with tracing paper, transmitted light as with a light board, tracing the indentations left in the page under the original writing and tracing paters of dots that outline the writing to be forged.

Simulations: Simulation involves copying of writing from a genuine article, trying to imitate the handwriting of the original.

Freehand: Freehand forgeries are written with no knowledge of the appearance of the original, just writing off the top of your head and passing it off as something else.

Lifted forgery: The final type of forgery is a lifted forgery, in which sticky type is used to lift a signature from one document and place it on another. Freehand forgars are the easiest to detect. Simulation counterfeits are also easy to detect for several reasons: They are.

- It is very difficult to copy someone else's handwriting.
- They style will not be as fluid because the writing does not come naturally.
- The forged writing will show tremors, hesitations and other variations in letter quality that 'comfortable' handwriting't has.
- Traced counterfeits and lifts are easy enough to detect but the identity of the forger cannot be easily determined.

Forensic science usage: Every person who writes has unique characteristics. Handwriting analysis looks at letter formations, connecting strokes between the letter's upstrokes, retraces, downstrokes, spacing, baseline, curves, size, distortions, hesitations and several other characteristics of handwritten. By examining these details and variations in a possible piece of evidence and comparing them to a sample of known authorship, forensic scientists can say whether the samples were written by the same person.

Handwriting analysis: True handwritten analysis involves careful examination of the design, shape and structure of the handwriting to determine who wrote it. The basic principle of handwriting analysis is that no drag people write something the same way. Handwriting analysis is useful in a range of circumstances. These include:

- Forging bank cheques and withdrawal forms.
- The deliberate alteration of business records and receipts.
- Threatening letters and ransom notes.
- The suicide notes.

Activity: How good a forger you are:

- Your name on a blank piece of paper as you world sign a receipt or some other document.
- Have several friends do the same. And swap apers. Take a few minutes and try to forge each other's signatures.
- Even more difficult, collect some writing samples from a classmate and try to forge a paragraph of their writing. Share the paragraph and the original samples. Can anyone say that the paragraph is a fake?

Sample collections: Summary of the most essential factors for the researcher to remember.

Obtaining/Getting known writing: Handwriting identification depends on the quality of known writing: Handwritten examination begins with the investigator and the results obtained depend on how well the investigator does the job in obtaining handwritten from suspected known writing for comparison with questioned disputed writing.

Comparable: Questioned and known specimens must be comparable: A's cannot be compared with G's John Jones cannot be compared with Samuel Hansen. The J's must be compared with J's and the Ohn's with ohn's. Handwriting cannot be compared to hand printing.

Conditions: Approximate the questioned writing conditions:

- If handwritten-get handwritten known.
- If upper-case hand printing-get upper case printing.
- If written in pencil-get known writing in pencil.
- If ball-point ink-get acquainted with ball-point pen.
- If writing is on a check-get known writing on checks.
- If writing is on ruled paper-get known on ruling paper.
- If a counterfeit-get a copy of authentic signature.

Duplicate the wording: The writing instrument and the space on the paper available for writing.

Appropriate/Adequate: In obtaining dictated known writing, get enough for the document examiner to study the normal variations in that person's writing. Get several specimens for each questioned document.

Do not let suspect see previous specimen-Remove from sight.

Do not let suspect copy questioned writing-Dict the wording to the suspect.

In obtaining dictated known writing, get enough for the document examiner to study the normal variations in that person's writing. Get several specimens for each questioned document.

Sample analyzed: This document is part of a handwritten comparison chart produced for display in court. The left side of the photo contains cut out letters from a forged document. The right hand side shows matching elements taken from a letter known to have been written by the suspect. Take careful note of the small numbers that indicate the matching elements (Figure 3) [6].

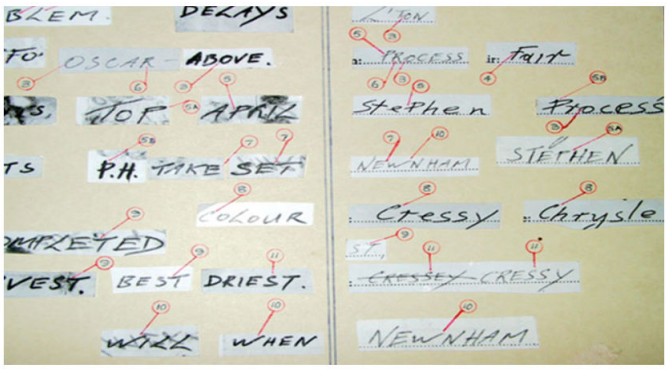

Figure 3: Sample analyzed.

Methodology

This work will use the clustering technique to solve this problem employing image acquisition tools, image processing tools, training image, testing image and unsupervised machine learning technique [1].

Acquisition of image: This is the first step, which involves acquiring the test signature of the customer using preferably HD scanner to test documents.

Imaging processing: This involves various procedures to prepare the signature for feature extraction. The procedures are binarization, segmentation, morphological erosion and dilation and normalization.

Binaryization: This technique is a preliminary processing step that converts the signature image to bi-level format of black and white.

Verification: This is the final process of the signature verification system using a matching point of the feature descriptor predicted by the exhaustive k-nearest neighbour search method according to the equation. However, we recommend approximate k-nearest neighbour method can be used in a larger dataset.

The segmentation: This image processing technique is employed to map the regions, curves and graphological patterns of the signature image.

Morphological dilation and erosion: This technique applies structural element to the signature image, based on the style of the signature and thus create a resulting output of optical character image with similar pattern.

Image normalization: This procedure not only removes noise from the image but also brings the image to a range of intensity value that is normal for feature extraction process.

Feature of extraction: This process involves the dimensional reduction of the signature image into a compact feature vector (i and j) using Hough transform.

Significance of the study

This study will help us to, a) How to obtain a fixed sized vector representation for signatures of varied size, b) How the resolution of the scanned signature impact system performance, c) The impact of fine tuning representations to other operating conditions *i.e.*, different acquisition protocols, signatures from people of different locations, by using transfer learning to other datasets, low number of samples per user for training. Presence of partial knowledge during training.

Change of style: This refers to the methodology by which the new system is introduced to banks. The parallel changeover style is suggested here for use since the banking system is already designed but lacks this verification technology [1]. According to, parallel method is applied when two systems are allowed to operate simultaneously. In this case, the existing system is still in use while the new system is introduced as a supplement (Figure 4).

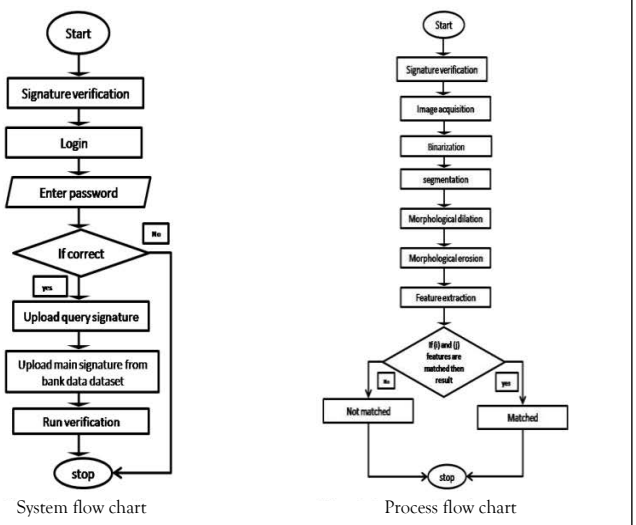

Figure 4: Change of style.

Features of extraction: Features extraction is a very important role to play in signature recognition and verification system, features must provide significant difference to the classifier between genuine and forge signature and at the same time should be consistent between different signatures provided by the same signor [4].

Normalization of characteristics: After selecting the appropriate features from the signature, normalization is required as certain features magnitude are very high greater than 100 but at the same time some features have very small magnitude so, if the classification process done without normalization of features, then certain features whose magnitude is large are become dominant.

Classification: After features extraction and normalization certain type of classification process is required in many researches different types of classification system are designed SVM (Support Vector Machine), HMM (Hidden Markov mMdel), VQ (Vector Quantization), backpropagation neural network (Figure 5) [7].

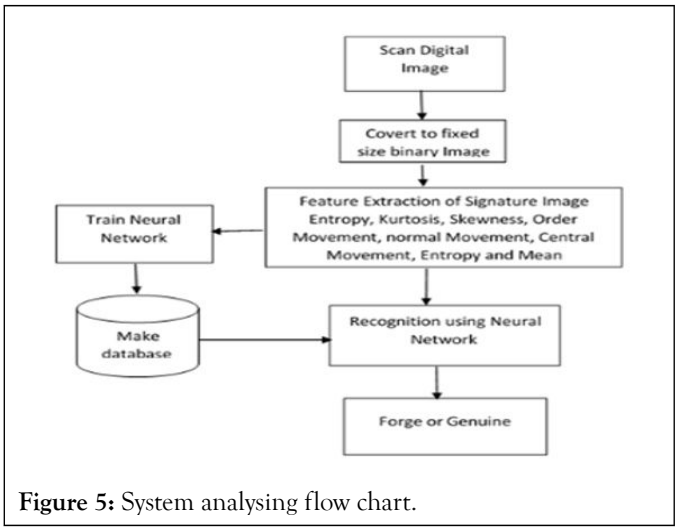

Figure 5: System analysing flow chart.

Digital signature verification models: There are two possibilities, sign then encrypt and encrypt then sign. The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key [8].

Software solution for DSVS: Now a days most of the transaction sectors verifying digital signature through software. Some of the leading software details are given below (Table 2).

Table 2: Software and Appls.

S. no	Software and App
1	Abode Sign
2	DigiSigner
3	eSignlive
4	DocuSign
5	Signo
6	Thunder Sign
7	DigiTech
8	TravicSign
9	CoinsDo
10	Smartwaiver

Mathematical models: In this paper, the offline signature verification is proposed, block diagram of the whole system. In this model's system uses neural network for verification and using general back propagation optimization method for training the neural network. For the first the signature from 6 different uses is taken on blank paper and convert that signature to digital image of jpg format and then applying pre-processing of the image for removing the noise from the image and then convert this noise free image into fixed size binary image of 200 × 200 pixels. After converting the image into binary image and then invert the image for more detail result then different features of that image are extracted from that image these features are as follows:

Skewness: Skewness is a measure of symmetry. A distribution or data set, is symmetric if it looks same to the left and right of the centre point. Skewness is a measurement of the distortion of symmetrical distribution or asymmetry in a data set. Skewness is demonstrated on a bell curve when data points are not distributed symmetrically to the left and right sides of the median on a bell curve.

Where the mean, s is the standard deviation and N is the number of data points. This formula for skewness is called Fisher Pearson coefficient of skewness. The skewness for a normal distribution is zero and any symmetric data should have a skewness near zero. Negative values for the skewness represent that data on which the skewness is calculated is skewed left and positive values indicate that data are skewed right.

Kurtosis: It is a measure of the probability distribution of any real valued random variable. Kurtosis is a measure of shape of a probability distribution and just like skewness, there are different ways of calculating it for a theoretical distribution and corresponding ways of estimating it from a sample of a given population.

$$\text{Kurtosis} = \frac{\sum(x_i - \bar{x})^4}{nS^4}$$

$\bar{x}$ = mean of the given data
S = standard deviation of the data
n = total number of observations

As we already know, skewness is the fourth moment of a distribution. The second moment of a distribution is its variance which will help simplify the equations.

Moment: Moments are scalar quantities used to characterize a function and to capture its significant features. Many types of moments are there and are widely used in statistics for description of the shape of a probability density function. General moment consider a grey-scale image g (x, y) of width w and height h and pixels values in the range 0-255. Geometric moments of a p+qth order of f.

Central moment: Central moment is a moment of a probability distribution of a random variable about the random variable's mean. The rth moment of any point A is called a central moment; it is the expected value of a specified integer power of the deviation of the random variable from the mean.

Entropy: Entropy is a measure of randomness of the pixels that can be used to characterize the texture features of the input image in digital image processing. Entropy is defined as sum (p.*log2 (p)) where p contains the histogram counts.

Mean: It is used to calculate the mean of all the white pixels in image and it can be useful as a feature of image because every signature has different lengths so total white pixels is also different.

The proposed work

Outline system overview: This figure shows the implementation process of the signature verification method [5]. The first is data acquisition. The offline image and online data of the signature are simultaneously obtained through the smart pen and the quality of the signature data is improved through pre-processing and feature extraction to ensure the accuracy of the verification result. For offline images and online data, SVM and DTW were used for verification and two scores score 1 and score 2 were obtained. Finally, the result of fusing offline and online features is obtained through SF-A (Figures 6 and 7).

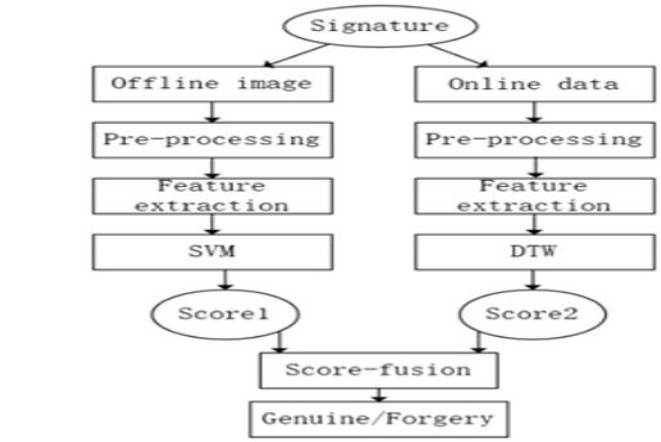

Figure 6: System overview.

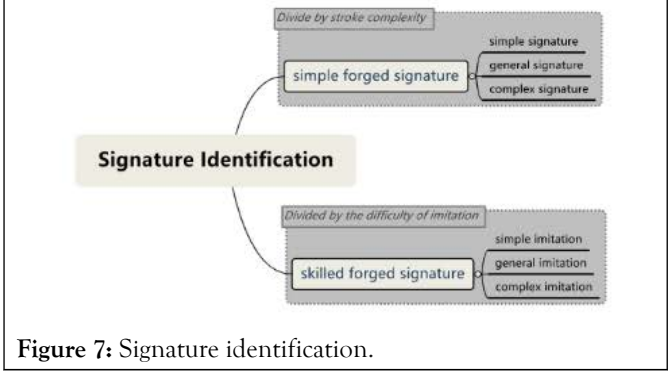

Figure 7: Signature identification.

Judgement orders

Supreme Court Bench of AM Khanwilkar and Dinesh Maheswari JJ has held that for invoking section 17 of the

Limitation Act 1963, tow ingredients *i.e.*, existence of a fraud and discovery of such fraud, must be pleaded and duly proved and that in case of failure to establish the existence of fraud, there is no occasion for its discovery [9].

Background of the case: The disputes dating back to 1990 pertains to a General Power of Attorney (GPA) purported to have been executed by the plaintiff in favour of defendant no.1 and consequently sale deeds executed by defendant no.1 as an attorney of the plaintiff. However, according to the plaintiff, reposing complete trust in her stepbrothers to stepbrothers, she had signed on blank papers under the guise of preparation and processing of documents for the propose of getting the estate left behind by their father mutated in their names. After analysing the evidence on record, the trail court dismissed the suit filed by the plaintiff and this order was upheld by the appellate court. The high court, however, reversed the concurrent opinions of two courts and held that the trail court as well as the first appellate court committed manifest error and misapplied the settled legal position. Challenging the high court decision before the supreme court, the defendants argued that interference by the high court was unwarranted as the same did not involve any substantial question of law. On merits, the aforesaid defendants contended that the evidence of the plaintiff was self-contradictory, as she first claimed that her signature were taken on blank papers and then denied her signature occurring on the 1990 GPA. The plea that the signatures were taken on blank papers was not substantiated as the 1990 GPA was executed on stamp papers.

Analysis: The court held that the diverse grounds urged by the plaintiff in disputing the 1990 GPA and the sale deeds were unsubstantiated and untenable. Here are the key factors taken into consideration by the court.

- As the record revealed that the disputed documents were registered, the court, guided by the settled legal principle that a document is presumed to be genuine it the same is registered, was of the opinion that the initial onus was on the plaintiff, who had challenged the stated registered document.
- As the execuiton of the 1990 GPA and the sale deeds in the present cases was denied by the plaintiff, it became necessary for the plaintiff ot examine the attesting witnesses of the disputed documents to establish her allegation about its non-execution, however, both the attesting witnesses were not examined.

The trail court had justly placed the initial burden of proof upon the palintiff as it was her case that the subject documents were forged or product of froud and moreso because the documents bore her signature. The first appellate court did not eloborate on that aspect even assuming the the burden had shifted upon the defendonts, the witness identifying singnatures of the deed attesting witness was examined by the defendonts. Therefore, the documents stood proved and the burden was duly discharged by the defendants.

The evidence of plaintiffs deed writed (PW$) unveiled that the stated documents were prepared on the basis of instrucitons of the plaintiff and had been duly executed by her in the presence of the attesting witnesses.

The trail court and the first oppellote court had relied upon the evidence of PW$. The high court, however, proceeded on surmises and conuecture and took a view which is perverse and tenuous. In that, the ground on which the high court rejected the evidence of PW$ is that he was known to the defendant No. 4 since his school days. We do not find it to be a correct approach to disregard the credible testimoney of the witness examined by the plaintiff herself (without declaring him as a hostile witness) at the instance of the plaintiff and as such, this port of his testimony would be storing at the plaintiff.

Since the attesting witness had proved the execution of the sale deeds, the primary onus upon the plaintiff had not shifted unto the defendatns. Further, the plaintiff was obliged to rebut the prositive evideance produced by the defendants regarding payment of consideration amount to the plaintiff, but also ought to have independently proved her case of non-receipt of the consideration amount.

Ruling: Concluding that the plaintiff failed to prove that her signatures on the subject document are forged, the court reiterated that the standard of proof required in a civil dispute is preponderance of probabilities and not beyound reasonable doubt. In the present cases, thought the discrepancies in the 1990 GPA are bound to create some doubt, however, in absence of any tangible evidence producted by the plaintiff to support the plea of fraud, it does not take the matter further, rather, in this case the testimony of the attesting witness, scribe and other independent witness plainly support the case of the efeendants. That evidnec dispuls the doubt if any, and tilt the balance in favour of the defendants [10].

Case of law

In Marketlend Pty Ltd v. Blackburn: Illustrates how fraud manifests itself in the context of electronic document execution and how the risk might be reduced. Marketlend provided the cash to a small business that sells mobile homes and residential vans, on the condition that the return would be guaranteed by the company's directors, Matthew and Sarah. Matthew and Sarah were married, but they were no longer together. Marketlend required that agreements be signed electronically using DocuSign. Both Sarah and Matthew had DocuSign accounts. DocuSign, Inc. is an American company headquartered in San Francisco, California, that allows organizations to manage electronic agreements. Marketlend used the DocuSign platform to send many emails to Matthew's company's email address, each with a document attachment. Sarah allegedly used DocuSign to sign each document. Marketland had had no prior contact with Sarah. Matthew was declared bankrupt after the company went into insolvency. Sarah was chased by Marketlend for the remaining cash (almost $ 700,000). The court concluded that Matthew exploited Sarah's account to sign the agreement without her knowledge or consent because she did not sign it when he asked her to. The evidence included DocuSign metadata and mobile phone location information. Sarah was not obligated to pay Marketlend the outstanding balance [11].

Barwick v Geico: 2011 Arkansas case where someone who applied for vehicle insurance on the internet was given a policy

by Geico. The applicant waived medical benefits coverage as part of the application procedure and electronically signed a document to that effect. Arkansas law at the time stated that medical benefits coverage could only be denied 'in writing.' Arkansas, on the other hand, had already implemented the UETA when the application was filed. The applicant was driving the insured vehicle when it was struck by another vehicle. Geico denied their claim when they provided medical bills under the coverage. When Barwick sued, Geico cited the applicant's acknowledgment of signing an electronic renunciation of coverage. However, the plaintiff contended that the waiver was ineffective because it was not in writing, as required by law. The court agreed with Geico and a higher court upheld the decision, citing Arkansas' UETA implementation as support.

Misuse of digital signature

Digital signature is a tool for authenticating precious documents. It is handy and feasible, but misuse of a digital nature can create major issues from forgery and fraud (Figure 8).

Figure 8: Digital signature.

India is a country with a high number of internet users and a growing digital economy. However, the use of digital signatures in India is still not widespread and there are proports of misuse of digital signature. A digital signature is basically an electronic signature that can be used to verify the identity of the sender of a message or document. In India, the use of digital signature is regulated by the Information Technology Act 2000. However, there have been reports of misuse of digital signatures in India. For instance, in May 2017, it was reported that around 10,000 tax returns had been filed using forged digital signatures. In another instance, in Nov 2017 it was reported that a fake website was created using a digital signature belonging to the Prime Minister's Office. The misuse of digital signatures can have serious consequences, as it can lead to fraud and identity theft. It is important for users to be aware of the risks associated with the use of digital signatures and to take measures to protect their own signatures [12].

Meaning of digital signatures

DSC Digital Signature Certificate online is a computer generated file that would be issued by a certifying authority (Pant sign CA, Safes crypt, e Mudra, Capricorn, Veasy's. (n) Code Solutions, InDesign CA) on submission of the required documents, Nowadays, due to this handy tool, we can process online applications or return filing easily and effectively.

Functions of digital signatures

Digital Signature Certificate (DSC) can be used for authenticating any document digitally, *i.e.*, by signing the document digitally. We must obtain a digital signature based on individual requirements and it has the following three classes (Table 3).

Table 3: Functions of digital signatures.

Classes of DSC	Functions	Examples
Class 1	These provide a basic level of assurance that the information provided in the application matches with the well-recognized consumer database *i.e.*, the cer tifying authority . It is no t used for document validation or signing a document	Testing purposes *i.e.*, verifying the contact details of a person
Class 2	The assurance provided by these certificates is relevant in an environment where the risk of data assurance is moderate, *i.e.*, It involves a substantial amount of monetary risk. It is used to validate a document and holds validity to signing documents digitally	GST return filings. Income tax return filing. Provident funds filings etc.
Class 3	This signature provides a high level of assurance with involves a high probability of fraud risk. These certificates are issued only on personal or physical appearance	Tender filing, e-binding etc.

Legal consequences of misuse of a digital signature certificate

Information Technology Act 2000: Section 66C Punishment for identity theft: A person who acts fraudulently or dishonestly and makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend up to rupees one lakh.

Section 71: Misrepresentation of suppression of material fact to obtain any license or electronic signature: It is applicable in the following situations:

- If a person makes a misrepresentation to the controller or the certifying authority.
- If a person suppresses any material fact from the controller or the certifying authority.

Such misrepresentaiton or suppression of material fact only with the intent to obtain any license or electronic certificate from the controller or the certifying authroity is punishabel with imprisonment of up to two years and a fine which may extend up to rupees one lakh. The inforamtion to be provided to the controller or the certifying authority should be proper and correct. The presentaiton of wrong, incorrect or false information is an offence under section 71 of the act.

Section 73: Publication of electronic signature, which is false in certain particulars. The following situations shall amount to the publication of false particulars in an electronic certificate:

- Publication of electonic signature certifiat which the certifying authroity has not issued.
- Publication of electronic signature certificate which actual subscriber of the certificate has not accepted.
- Publication of the electronic signature certificate which is revoked or suspened.

Section 74: Information Technology Act 2000: Punishes the creation, publication or providing of an electronic signature certifiate for fradulent or unlawful prupose with imprisonment for a term which may extend up to two years or a fine which may extend upto one lakh. https://legislative.gov.in/actsoofparliamentfromtheyear/inforamtion-technology-act-2000/

The Indian Penal Code (IPC) 1860: Section 463 of INP 1860-Forgery. Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury, to the public or any person or to support any claim or title, or to cause any person to part whith property or to enter into any express or implied contract or with intent to commit fraud or that fraud may be committed, commits forgery.

An explanation for section 463: Where any person either fradulently or dishonestly made, signed, sealed, executed or transmitted a document or electronic record or its part thereof affixed with an electronic signaute.

Where any person without proper authentiacation alters any docuemt or any record maintained electronically or materially its part thereof, executed or affixed with electronic signature either by himself or by any other prerson, whether such person is alive or dead at the time of such alternation.

Where any person acts in a fraudulent or dishonest manner by sign, sealing, executing or altering a document or an electronic record or affixing his or her lectronic signature on any electronic record knowing that such person is of unsound mind and the person is unaware about the contents of the signed document or the type of lateration made.

Section 465 of the INP 1860 punishment for forgery, whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years or with a fine or with both. This offense is biable and triable by the Magistrate first class.

Safety measures to avoid misuse of digital signature

DSC is a facilitative tool but alos comes with a high risk. Following are some measures: Any person should keep the physical custody of the token whith himslelf/herself. If we are signing any document on behald of our client, we should first obtain an authorization letter. We should proceed further with it, eg. A pradcticing chartered accountant signing ITR or other GST returns on behalf of their client because practically, it is not possible to obtain custody of the take at every time of filing there might be a clash of timings. So they should obtain an authroization letter along with its custody.

A myth about digital signature

There is a myth about digital signature revolving among us that signing on a paper and simply scanning it is a digital signature, but this is wrong and might lead to fraud with an unknown person. In actuality, the digital signature is a token generated by the certifying authroity on an application made to them. This token signs the document with the utility of the respective platform.

The misuse of digital signature is a major problem in India and global level also. There are many ways in which people can misuse them and this can have serious consequences. It is important to be aware of the ways in which digital signatures can be misused and to take steps to prevent this from happening [13].

- How can I register for digital signature certificate.
- How can you create a digital signature.

Need for the study

Digital signature verification is a form of identity verification. It works by determining whether a person's signature is genuine according to past iterations. The signature or its image is fed into signature verification software and compared to the image on file. The study is conducted to know the requirements of digital signature, digital signature acceptance documentation evidence, digital signature certificate, purposes of digital signature, importance goals of information security and

prevention by cyber security. Digital signature certificates ensure that businesses save on cost and time with documents and contracts signed. There are huge savings in cost and time especially when the person is required to sign from a different place. The three main purpose of digital signature are used to meet important goals of information security, they are integrity, authentication and non-repudiation. Lastly the security protection against forgery by cyber security. A digital signature is a cryptographic output sued to verify the authenticity of data. A digital signature algorithm allows for two distinct operations, a signing operation, which uses a signing key to produce a signature over raw data.

Requirement for digital signature: Indian individual, bank account passbook, statement containing the photograph and signed by an individual with attestation by the concerned bank official, photo ID card issued by the ministry of home affairs of centre/state government and any government issued photo identity having name and address [14].

Review of related literature

Salem and Kovari: In this work, we studied the effect of the sampling rate of the input devices used for signature acquisition and the number of sample points on the accuracy of online signature verification systems [10]. The researchers proposed online signature verification based on signer dependent sampling frequency and DTW. Several configurations of a DTW-based verification system were used to assess the achievable EER at different sampling rates. Altogether, we conducted 2800 different experiments, which helped generalize the results regardless of the effect of other factors that may affect the system's accuracy. To our knowledge, these properties have never been studied within the scope of online signature verification. The results showed that most of the best results could be obtained using a sampling frequency between 15 and 50 Hz and a sample count between 60 and 240 points. Using frequencies lower than these ranges greatly decreased the accuracy, whereas using higher frequencies decreased or did not affect the accuracy in 92.5% of the configurations of all databases acquired between 100 and 200 Hz. For these databases, 91.25% of the best results were obtained using a sampling frequency of less than or equal to 50 Hz and 93% of less than or equal to 75 Hz. The results showed that using the optimal frequency provides competitive systems for online signature verification. These results are auspicious and suggest that DTW-based online signature verifiers can be improved in the future by using different criteria for choosing the best sampling frequency for each signer.

Sharif and Khan: Biometric verification is a method of identifying the persons by their individualities or traits. Signature verification is the most generally used biometric to maintain human privacy. It is used in many areas as banking, access control, e-business etc and equally important in financial transactions. Research has progressed greatly in the area of signature verification but still, it is hard to discriminate between genuine signatures and skilled forgeries. Based on the idea of best features selection, a novel technique is introduced in this article for an offline verification system [14]. The presented system consists of four major steps: Preprocessing, features extraction, features selection and feature verification. Global features in the proposed work comprise of aspect ratio, the area of signature, pure width, pure height and normalized actual signature height. Local features consist of signature centroid, slope, angle and distance. In features selection component, a genetic algorithm is utilized to find appropriate features set which are later on given to support vector machine for verification. For experimental analysis, the selected datasets are CEDAR, MCYT and GPDS synthetic. The performance of proposed algorithm is based on three accuracy measures as FAR, FRR and AER.

Eman Alajrami, et al.: In their paper revealed that, offline signature verification is not efficient and slow for many documents [9]. To overcome the drawbacks of offline signature verification, we have seen a growth in online biometric personal verification such as fingerprints, eye scan etc. created CNN model using python for offline signature and after training and validating and the accuracy of testing was 99.70%. Every person has his/her own unique signature that is used mainly for the purposes of personal identification and verification of important documents or legal transactions. There are two kinds of signature verification: Static and dynamic. Static of off-line verification is the process of verifying an electronic or document signature after it has been made, while dynamic on-line verification takes place as a person creates his/her signature on a digital tablet or a similar device [15].

The RBI Ombudsman scheme for digital transactions: Defines digital transactions as "a payment transaction in a seamless system effected without the need for cash at least in one of the two legs, if not in both. This includes transactions made through digital/electronic modes wherein both the originator and the beneficiary use digital/electronic medium to send or receive money". However, in our paper, a digital transaction is one where the payer and payee both use digital modes of payment. Policies in many parts of the world are being designed in favour of non-cash payments because of the various problems that cash poses. Cash fuels the parallel or black economy, therefore, phasing it out might solve this problem, especially with large denomination notes. The cost of printing, destroying and other cash related operational expenses in India are estimated at 1.7% of GDP. Cash, however, remains a significant part of all the transactions in most countries. They reveal that the choice of payment method is impacted by a host of consumer specific and technological factors. Transaction size has a significant impact on what mode of payment people choose. A cross-country comparison of payment diary survey data of seven countries showed that cash was the preferred mode of payment for smallest 50% and largest 25% of transactions. In another study, social marginal costs were computed for various instruments for small and large transaction sizes and it was found that for larger transaction sizes, there were significant differences in cost for electronic *vs.* non-electronic payments.

Shin J and Junichi Sato: In this paper, we propose to reject the possibility to accept the login by someone else, which is not by him or herself at multiuser online Kanji learning system with signature verification. Human's signature is one of the human's

biometrics. Biometrics includes very personal information and characteristics of usefulness because it is human are looking or behaviour feature. By signature verification, we could verify the writer is proper or not with human's writing behaviour, so dishonest writer will be rejected. Using signature verification as self-verification at the system, we could consider two advantages [13]. One advantage is advancement of security which will cause from deterrent of someone else's scamming. The other advantage is advancement of usefulness which will cause from decrease of the number of using input device, only pen device will be need to handle the system. We adopt signature verification as calculating similarity by using some reference signature and the distance which will calculated by DP matching in this research. Input signature's self-similarity will be calculated by dividing the average distance between input and each reference signature data with average distance between each reference signature data. From signature verification's experimental results which changes using features, we adopted to use writing velocity and writing speed differential as using feature to verify the writer for the system. By using signature database which is construct with 20 genuine signatures and 20 forged signatures with 40 writers and written mostly by English or Chinese literal, experimental results of signature verification records 12.71% as maximum EER, 6.00% as minimum EER and 8.22% as average EER. Furthermore, when we establish the threshold as constant, to simulate the signature verification function is implement in actual running system, average of FRR records 10.29% and FAR records 9.72%. From mentioned above, we realized to advance the reliability and usefulness of the multiuser online Kanji learning system [16].

Saeidi M, et al.: Although signature verification is not the safest method of identification, it is extensively used in commercial affairs because of simplicity and ease of use. In this research paper after accomplishment of some pre-processing procedures like normalization of signature size, smoothing and elimination of rotation on signatures using algorithms based on extremum matching of signals and ant colony, their time duration will be equalized. Afterwards, similarities between signatures will be determined using extended regression and finally will try to distinguish between forgery signatures from genuine one using Support Vector Machine (SVM). The suggested online verification system is tested on SVC2004 signature set which is related to the first international signature verification competition and results are compared to respective results of participants [13]. The results state that suggested method exhibits Equal Error Rate (EER) 4.3% of in skilled forger group. From their research its shows that majority of them using digital signature verification system for their future process.

Objectives

Serious fraud investigation office: SFIO is a multi-disciplinary organization under Ministry of Corporate Affairs, consisting of experts in the field of accountancy, forensic auditing, law, information technology, investigation, company law, capital market and taxation of detecting and prosecuting or recommending for prosecution white-collar crimes or frauds.

Objectives: Take up for investigation cases characterized by complexity and having inter-departmental and multi-disciplinary ramifications. Substantial involvement of public interest to be judged by size, either in terms of monetary the possibility of investigation leading to or contributing towards a clear improvement in systems, laws, or procedures.

- Investigate serious cause of fraud received from department of company affairs.
- Investigate into the affairs of a company on receipt of the registrar or inspector under section 208 of the companies Act 2013.
- On intimation of a special resolution passed by a company that its affairs are required to be investigated in the public interest on request from any department of the central government or a state government.
- For more information visit serious fraud Investigation office.

RESULTS AND DISCUSSION

Data analysis and hypothesis

Indian companies engaged in various business activities through online systems (Figures 9-12).

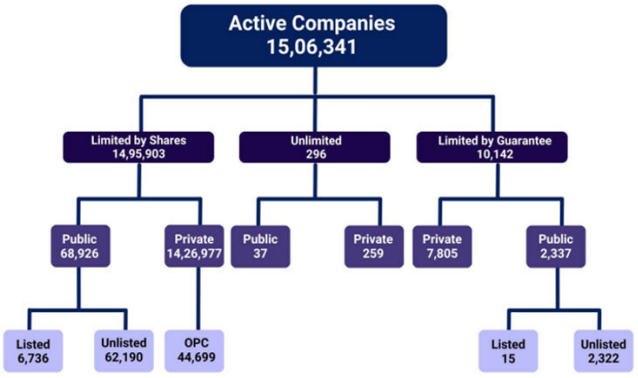

Figure 9: Data from Govt. of India Ministry of Corporate Affairs.

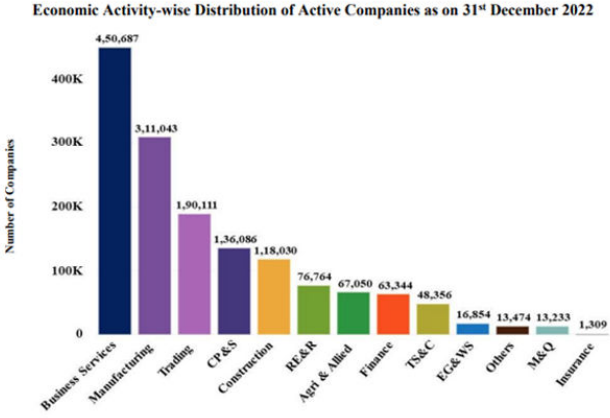

Figure 10: Data from Govt. of India Ministry of Corporate Affairs.

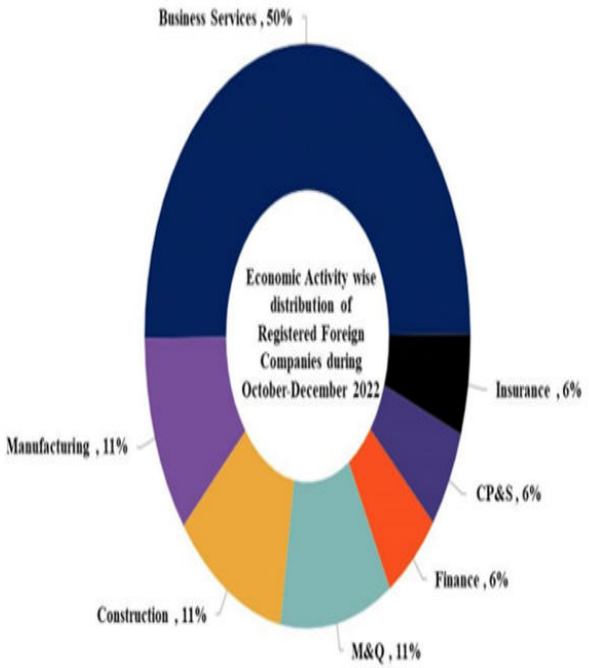

Figure 11: Foreign companies involved in various business activities in India 2022.

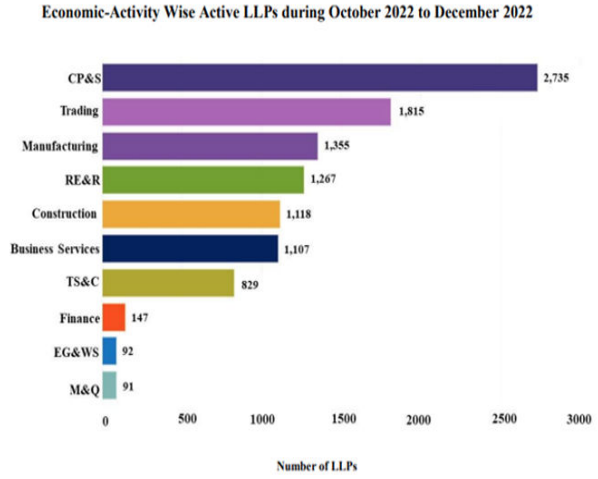

Figure 12: Data from Govt. of India Ministry of Corporate Affairs.

Data analysis

Review of meeting: Some of the salient review meetings were conducted with district and state cooperative banks, financial institutions (Tables 4-6 and Figures 13-15).

Table 4: Source of data from FIU-I.

Year	2015-16	2016-17	2017-18	1018-19	2019-20	2020-21	2021-22
Review meeting	43	16	13	13	36	12	32
Participants	557	208	100	83	166	91	192

Table 5: Data from FIU-I.

Type of reports				
Suspicious Transaction Reports (STR)	Cash Transaction Reports (CTR)	Cross Border Wire Transfer Reports (CBWTRs)	NPO Transaction Reports (NTRs)	Counterfeit Currency Reports (CCRs)

Table 6: Online transaction use of economic activity.

Economic activity	Private		Public		Total	
	Number	Paid up capital	Number	Paid up capital	Number	Paid up capital
Agriculture and allied activities	64,793	22,413.27	2,257	17,625.80	67,050	40,039.07
Industry	434,919	874,391.32	24,241	1,886,364.44	459,160	2,760,755.76

Manufacturing	293,388	560,790.58	17,655	720,866.69	311,043	1,281,657.27
Metals and chemicals and products thereof	100,090	217,662.37	7,639	247,215.28	107,729	464,877.65
Machinery and equipments	68,315	221,517.01	3,362	382,869.86	71,677	604,386.87
Textler	36,239	34,539.40	2,524	34,957.95	38,763	69,497.34
Food stuffs	46,899	49,121.89	2,467	31,471.57	49,366	80,593.46
Paper a paper products publishing printing and reproduction of recorded media	17,707	14,496.51	798	9,987.09	18,505	24,483.60
Others	17,700	17,757.49	505	12,094.86	18,205	29,852.35
Leather and products thereof	3,390	3,129.11	184	1,070.62	3,574	4,199.73
Wood products	3,048	2,566.80	176	1,199.48	3,224	3,766.28
Construction	113,918	147,860.52	4,112	230,636.36	118,030	378,496.88
Electricity gas and water supply companies	15,078	133,724.23	1,776	879,720.49	16,854	1,013,444.71
Mining quarrying	12,535	32,016.00	698	55,140.90	13,233	87,156.90
Services	924,074	978,949.61	42,583	1,321,706.34	966,657	2,300,655.95
Business services	441,076	436,524.88	9,611	615,983.34	450,687	1,052,508.22
Trading	184,571	220,847.26	5,540	54,391.30	190,111	275,238.56
Real estate and renting	74,213	81,730.40	2,551	22,675.74	76,764	104,406.14
Community personal and social services	131,905	72,220.50	4,181	116,824.47	136,086	189,044.97
Finance	44,243	109,211.33	19,101	299,323.50	63,344	408,534.83
Transport storage and communications	46,904	56,485.03	1,452	169,517.35	48,356	226,002.38
Insurance	1,162	1,930.21	147	42,990.64	1,309	44,920.85
Others	11,255	18,116.34	2,219	70,774.50	13,474	88,890.84
Total	1,435,041	1,893,870.53	71,300	3,296,471.08	1,506,341	5,190,341.61

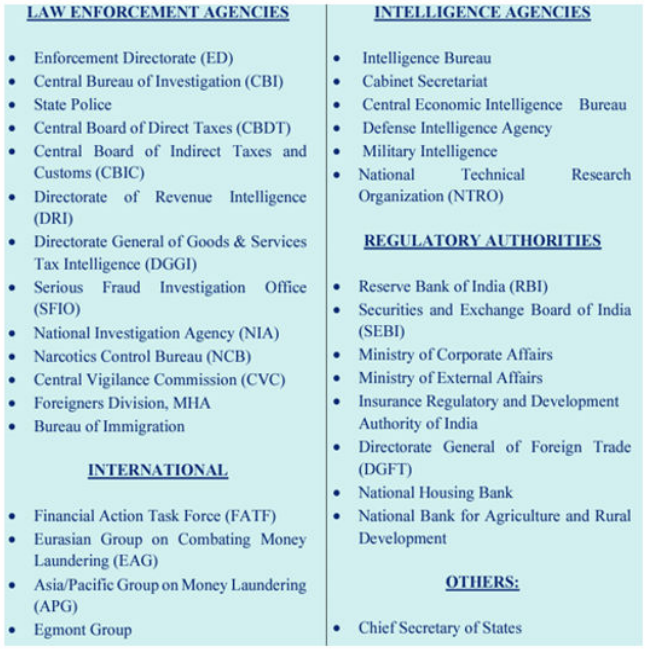

Figure 13: Transaction of use: FIU-India partners.

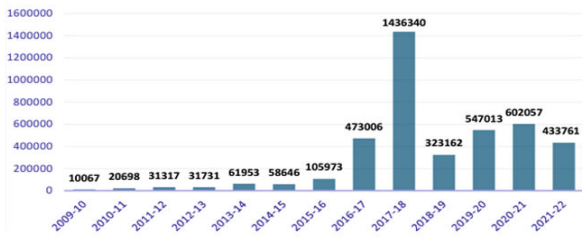

Figure 14: Digital transactions: Data from FIU-I.

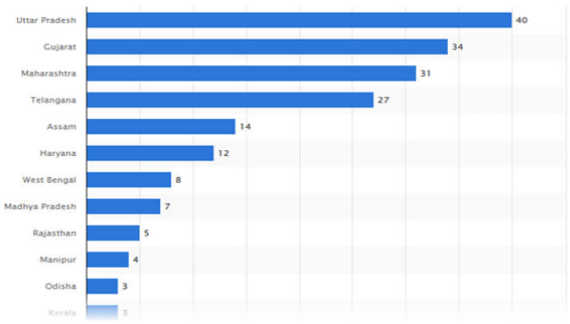

Figure 15: Number of digital counterfeiting incidents across India in 2021 by leading state.

Testing the hypothesis: From this study of research reveals that its null hypothesis. So, the online transaction is very helpful and most of the user is satisfied with these facilities and it would have good future with safety monitoring systems (Table 7 and Figure 16).

Table 7: User satisfaction with online services.

Service	Satisfied	%
Good	673	95
Bad	37	5
Total	710	100

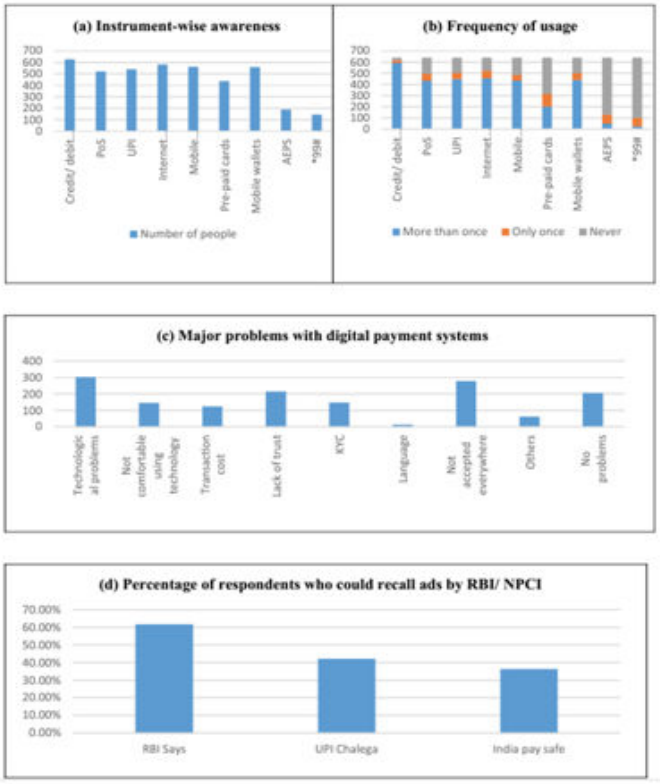

Figure 16: Awareness, frequency of use digital payment problem with percentage-data from IRRBT.

Purpose of the study: The purpose of this study citation methods has been adopted 93 research articles has been cited by the researchers in global level and 25 other websites have been published various disputes related to the signature fraud and online transactions technologies by the fraudulent acquests in the different modes of digital payment systems. Our study aims are understanding the impact of user satisfaction level, trust in payment systems, experience in online fraud, awareness about digital signature and online banking. Statistical tools have been used at various levels for testing hypothesis being tested at various stages. The research analysis of various baselines modes to utilize the transaction facilities *i.e.*, paying cash, digital transactions and others.

Parameter model used to know the usage by the utilizers. The model has j=1, 2 .... J categories for the dependent variable y and x are the matrix of independent variables. In a multinomial logit model, estimate a set of coefficients $\beta_j=(\beta_1, \beta_2)$ corresponding to each outcome j. Setting j=1 as the reference or base category (*i.e.*, $\beta_1=0$).

$$\Pr(y=1|X)=\frac{1}{1+\sum_{j=2}^{J}\exp(x_i\beta_j)} \quad \text{for } j=1$$

In these categorical independent variables, the following multinomial logistic model is estimated. The dependent variable is coded as:

y=0 for cash reference

y=1 for digital payments

y=2 for some times cas flow in other payment mode

$$\ln\left[\frac{\Pr(y=1|X)}{\Pr(y=0|X)}\right]=\beta_{01}+\beta_{11}gender_i+\beta_{21}age_i+\beta_{31}education_i+\beta_{41}income_i+\beta_{51}occupation_i+\beta_{61}placeofresidence_i$$

$$\ln\left[\frac{\Pr(y=2|X)}{\Pr(y=0|X)}\right]=\beta_{02}+\beta_{12}gender_i+\beta_{22}age_i+\beta_{32}education_i+\beta_{42}income_i+\beta_{52}occupation_i+\beta_{62}placeofresidence_i$$

Role of the Reserve Bank of India in fraud by banks

The committee is required to examine the role of the reserve bank of India regarding frauds reported by banks. The committee has examined the position obtaining in respect of commercial banks (other than Regional Rural Banks) in this regard. It is observed that the Reserve Bank of India has a comprehensive reporting mechanism whereby all banks are required to report actual/suspected frauds either to the central office or regional offices of the Department of Banking Supervision (DBS) of RBI. The banks are required to report all actual/suspected frauds more than Rs. 1 lakh each to the Regional Offices of DBS with full particulars in the prescribed proforma as soon as such frauds come to their notice but within three weeks of detection. The central office of DBS receives individual reports on actual/suspected frauds of Rs.1 crore and above and in respect of frauds by unscrupulous borrowers involving an amount of Rs.5 lakh and above. The fraud reports are required to indicate, among other things, the modus operandi of the fraud, amount involved, the amount of expected loss and chances of recovery, staff involvement and the action taken against the delinquent members of the staff. Cases of individual frauds involving amounts up to Rs.1 lakh each are not required to be reported individually. The banks are, however, required to report such frauds in a consolidated form category wise on a quarterly basis in the prescribed format. Besides, to enable Reserve Bank of India and the Government of India to have full information about the incidence of frauds and the action taken by banks to prevent them, the banks are required to furnish to RBI certain statements on quarterly/half-yearly basis. While quarterly statements deal with further developments in respect of frauds reported to RBI, half-yearly statement on frauds is required to indicate the stage of Police/CBI investigation as well as the recoveries made. Quarterly statements are also required to be sent by the banks on frauds outstanding and closed during the quarter. Besides, there are reporting systems in place for following up vigilance aspects in the public sector banks [17].

The above reporting system seems to have been designed to serve the following objectives:

- To examine new modus operandi, if any, adopted in respect of a fraud and circulate the same among banks.
- To issue caution advice to banks giving details of unscrupulous borrowers so that they will be careful while dealing with such borrowers.

- To ensure that banks have taken prompt steps to recover their dues and have reported to fraud cases to CBI/Police.
- To collate date relating to frauds and vigilance cases to report to the Board for Financial Supervision.
- To consolidate data pertaining to frauds/vigilance cases (in respect of public sector banks) to report to Government of India/Parliament from time to time. The committee feels that while violations of any regulation come within the purview of the regulator, any act of omission or commission by a bank or any of its employees or constituents or others attracts the provision(s) of a criminal law, it goes outside the purview of the regulator. The regulator has no further role to play. The committee is, therefore, of the view that the present system for monitoring fraud and its investigation is burdened by too many layers imposing large regulatory costs on the banks. Furthermore, it is felt that rather than following up each individual case of fraud, the RBI as a regulator/ supervisor should be more concerned about the systemic impact of such fraud. For instance, a fraud of Rs. 10 crore in a large public sector bank may not be of much regulatory/ supervisory concern; at the same time, a similar fraud in a small private sector bank may be of serious concern to the regulator/supervisor. It is, therefore, felt that the response of the RBI to such frauds should consider the whole picture. Furthermore, individual monitoring of frauds could be left to the banks themselves. A review of such monitoring could be made at the time of the periodical inspections of the banks. The investigating agencies, CBI and the police take unduly long time to complete the investigation and to close a case. In view of this, the RBI would be spreading its supervisory resources too thin if it were to follow up each individual fraud case up to its logical end. The committee is, therefore, of the view that the reporting system for frauds needs to be rationalized so that there is no duplication of efforts and that the reporting is done only in respect of information necessary for the Reserve Bank of India in exercising its regulatory/ supervisory responsibilities.

Credit transaction data registration and information sharing: In India there is no one law for credit transaction, no public registry and sharing of information. We follow the common law system of privity of contract. But there has been system reform in the home country of common law, but we have not changed. There is no one law for security interest creation, priority determination and enforcement. All these supplemented with no information sharing amongst the institutions and with the regulator concerned, cripple the financial service industry. Fraud is only the resultant action. Control, prevention and prohibition of financial fraud call for reform in both financial sector law and criminal law.

Recommendation for the future

The future work should address the challenges and issues involved in online sig nature verification and there is always a scope for new approach which may improve the performance, the future works may involve in exploring new features and new approaches which may be more effective in distinguishing forgeries from genuine signatures. There is a scope for reducing number of signatures required for training the model for reliable authentication. Comparison techniques LCSS and DTW can be used in combinations with other classifier models like HMM MLP model, SVM and other NN models. These classifier models can also be used in combination with other distance-based approaches like edit distance, Euclidean, city block distance computation techniques [18].

The RBI recommendation

Prologue: The committee, in its critical review of the system as obtained presently, observed two very wide systemic gaps in the law and practice in dealings of the banks and financial institutions with the public frauds. These systemic gaps are as follows: Firstly, wide gap in the law and practice of banking law and practice. As for example:

- No clear and certain best practice code in the organization.
- Weak internalization system of the rule of law being the best practices in the organization and management.
- No discipline in the use of discretionary power to be used in the manner and circumstances as laid down.
- No appreciation of administrative law to use discretionary power as being the judging power that involves decision and reasoning to be well documented and
- No institutional plan for the judging power to be linked with incentive and promotional system in the organization.

Secondly, the poverty in the criminal jurisprudence is also very apparent in India. Many jurists argued for a long time that criminal law in India is heavily class biased. Absence of financial fraud in the list of offences in the penal code is evidence that 'white collar crime' is treated differently in India with all leniencies. The committee has, therefore, prepared its suggestions in two parts.

Part I: Deals with the preventive aspects of management of financial fraud to keep it happen only in rare cases. This part suggests steps to contain a clean in-house financial management.

Part II: Deals with prohibition of financial fraud and introduction of a deterrent jurisprudence so that financial fraud, being a serious offence to derail a system, is adequately and firmly dealt with.

Bank fraud

Fraud is any dishonest act and behaviour by which one person gains or intends to gain advantage over another person. Fraud causes loss to the victim directly or indirectly. Fraud has not been described or discussed clearly in The Indian penal code but sections dealing with cheating, concealment, forgery counterfeiting and breach of trust has been discussing which leads to the act of fraud. In contractual term as described in the Indian contract act, sec 17 suggests that a fraud means and includes any of the acts by apart to a contract or with his connivance or by his agents with the intention to deceive another party or his agent or to induce him to enter a contract. Banking frauds constitute. Banking frauds constitute a considerable percentage of white collar offences being probed by the police. Unlike ordinary thefts and robberies, the amount misappropriated in these crimes runs into lakhs and crores of

rupees. Bank fraud is a federal crime in army countries, defined as planning to obtain property or money from any federally insured financial institution. It is sometimes considered a white collar crime.

The number of bank frauds in India is substantial. It in increasing with the passage of time. All the major operational areas in banking represent a good opportunity for fraudsters with growing incidence being reported under deposit, loan and inter-branch accounting transactions, including remittances. Bank fraud is a big business in today's world. With more educational qualifications, banking becoming impersonal and increase in banking sector have given rise to this white collar crime. In a survey made till 1997 bank frauds in nationalised banks was of Rs.497.60 crore. This banking fraud can be classified as:

- Fraud by insiders
- Fraud by others

Fraud by insiders

Rouge trader: A rogue trader is a highly placed insider nominally authorized to invest sizeable funds on behalf of the bank; this trader secretly makes progressively more aggressive and risky investments using the bank's money, when one investment goes bad, the rogue trader engages in further market speculation in the hope of a quick profit which would hide or cover the loss. Unfortunately, when one investment loss is piled onto another, the costs to the bank can reach into the hundreds of millions of rupees; there have even been cases in which a bank goes out of business due to market investment losses.

Fraudulent loans: One way to remove money from a bank is to take out a loan, a practice bankers would be more than willing to encourage if they know that the money will be repaid in full of interest. A fraudulent loan, however, is one in which the borrower is a business entity controlled by a dishonest bank officer or an accomplice; the "borrower" then declares bankruptcy or vanishes and the money is gone. The borrower may even be a non-existent entity and the loan merely an artifice to conceal a theft of a large sum of money from the bank.

Wire fraud: Wire transfer networks such as the international, interbank fund transfer system are tempting as targets as a transfer, once made, is difficult or impossible to reverse. As these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while banks have put checks and balances in place, there is the risk that insiders may attempt to use fraudulent or forged documents which claim to request a bank depositor's money be wired to another bank, often an offshore account in some distant foreign country.

Fake or fraudulent documents: Forged documents are often used to conceal other thefts; banks tend to count their money meticulously so every penny must be accounted for. A document claiming that a sum of money has been borrowed as a loan, withdrawn by an individual depositor or transferred or invested can therefore be valuable to a thief who wishes to conceal the minor detail that the bank's money has in fact been stolen and is now gone.

Uninsured deposits: There are several cases each year where the bank itself turns out to be uninsured or not licensed to operate at all. The objective is usually to solicit for deposits to this uninsured "bank", although some may also sell stock representing ownership of the "bank". Sometimes the names appear very official or very similar to those of legitimate banks. For instance, the "Chase Trust Bank" of Washington DC appeared in 2002 with no license and no affiliation to its seemingly apparent namesake, the real Chase Manhattan Bank, New York. There is a very high risk of fraud when dealing with unknown or uninsured institutions.

Theft of identity: Dishonest bank personnel have been known to disclose depositors' personal information for use in theft of identity frauds. The perpetrators then use the information to obtain identity cards and credit cards using the victim's name and personal information.

Demand draft fraud: DD fraud is usually done by one or more dishonest bank employees that is the Bunko Banker. They remove few DD leaves or DD books from stock and write them like a regular DD. Since they are insiders, they know the coding, punching of a demand draft. These demand drafts will be issued payable at distant town/city without debiting an account. Then it will be cashed at the payable branch. For the paying branch it is just another DD. This kind of fraud will be discovered only when the head office does the branch wise reconciliation, which normally will take 6 months. By that time the money is unrecoverable.

Fraud by others

Counterfeit/Forgery and altered cheques: Thieves have altered cheques to change the name (to deposit cheques intended for payment to someone else) or the amount on the face of a cheque (a few strokes of a pen can change 100.00 into 100,000.00, although such a large figure may raise some eyebrows). Instead of tampering with a real cheque, some fraudsters will attempt to forge a depositor's signature on a blank cheque or even print their own cheques drawn on accounts owned by others, non-existent accounts or even alleged accounts owned by non-existent depositors. The cheque will then be deposited to another bank and the money withdrawn before the cheque can be returned as invalid or for non-sufficient funds.

Stolen cheques: Some fraudsters obtain access to facilities handling large amounts of cheques, such as a mailroom or post office or the offices of a tax authority (receiving many cheques) or a corporate payroll or a social or veterans' benefit office (issuing many cheques). A few cheques go missing; accounts are then opened under assumed names and the cheques (often tampered or altered in some way) deposited so that the money can then be withdrawn by thieves. Stolen blank cheque books are also of value to forgers who then sign as if they were the depositor.

Accounting fraud: To hide serious financial problems, some businesses have been known to use fraudulent bookkeeping to overstate sales and income, inflate the worth of the company's assets or state a profit when the company is operating at a loss. These tampered records are then used to seek investment in the

company's bond or security issues or to make fraudulent loan applications in a final attempt to obtain more money to delay the inevitable collapse of an unprofitable or mismanaged firm.

Bill discounting fraud: Essentially a confidence trick, a fraudster uses a company at their disposal to gain confidence with a bank, by appearing as a genuine, profitable customer. To give the illusion of being a desired customer, the company regularly and repeatedly uses the bank to get payment from one or more of its customers. These payments are always made, as the customers in question are part of the fraud, actively paying all bills raised by the bank. After certain time, after the bank is happy with the company, the company requests that the bank settles its balance with the company before billing the customer. Again, business continues as normal for the fraudulent company, its fraudulent customers and the unwitting bank. Only when the outstanding balance between the bank and the company is sufficiently large, the company takes the payment from the bank and the company and its customers disappear, leaving no-one to pay the bills issued by the bank.

Cheque by kiting: Cheque kiting exploits a system in which, when a cheque is deposited to a bank account, the money is made available immediately even though it is not removed from the account on which the cheque is drawn until the cheque clears. Deposit 1000 in one bank, write a cheque on that amount and deposit it to your account in another bank; you now have 2000 until the cheque clears.

In-transit or non-existent cash is briefly recorded in multiple accounts

A cheque is cashed and before the bank receives any money by clearing the cheque, the money is deposited into some other account or withdrawn by writing more cheques. In many cases, the original deposited cheque turns out to be a forged cheque. Some perpetrators have swapped checks between various banks daily, using each to cover the shortfall for a previous cheque. What they were doing was check kiting; like a kite in the wind, it flies briefly but eventually must come back down to the ground.

Credit card fraud: Credit card fraud is widespread as a means of stealing from banks, merchants and clients. A credit card is made of three plastic sheets of polyvinyl chloride. The central sheet of the card is known as the core stock. These cards are of a particular size and many data are embossed over it. But credit cards fraud manifest in several ways. They are:

- Genuine cards are manipulated.
- Genuine cards are altered.
- Counterfeit cards are created.
- Fraudulent telemarketing is done with credit cards.
- Genuine cards are obtained on fraudulent applications in the names/addresses of other persons and used.
- It is feared that with the expansion of e-Commerce, m-Commerce and internet facilities being available on massive scale the fraudulent fund freaking credit cards will increase tremendously.
- Counterfeit credit cards are known as white plastics.

Booster cheques: A booster cheque is a fraudulent or bad cheque used to make a payment to a credit card account to "bust out" or raise the amount of available credit on otherwise-legitimate credit cards. The amount of the cheque is credited to the card account by the bank as soon as the payment is made, even though the cheque has not yet cleared. Before the bad cheque is discovered, the perpetrator goes on a spending spree or obtains cash advances until the newly "raised" available limit on the card is reached. The original cheque then bounces, but by then it is already too late.

Stolen payment cards: Often, the first indication that a victim's wallet has been stolen is a 'phone call from a credit card issuer asking if the person has gone on a spending spree; the simplest form of this theft involves stealing the card itself and charging several high ticket items to it in the first few minutes or hours before it is reported as stolen. A variant of this is to copy just the credit card numbers (instead of drawing attention by stealing the card itself) to use the numbers in online frauds.

Duplication or skimming of card information: This takes several forms, ranging from a dishonest merchant copying clients' credit card numbers for later misuse (or a thief using carbon copies from old mechanical card imprint machines to steal the info) to the use of tampered credit or debit card readers to copy the magnetic stripe from a payment card while a hidden camera captures the numbers on the face of the card. Some thieves have surreptitiously added equipment to publicly accessible automatic teller machines; a fraudulent card stripe reader would capture the contents of the magnetic stripe while a hidden camera would sneak a peek at the user's PIN. The fraudulent equipment would then be removed and the data used to produce duplicate cards that could then be used to make ATM withdrawals from the victims' accounts.

Impersonation and identity theft: Theft of identity has become an increasing problem; the scam operates by obtaining information about a victim, then using the information to apply for identity cards, accounts and credit in that person's name. Often little more than name, parents' name, date and place of birth are sufficient to obtain a birth certificate; each document obtained then is used as identification in order to obtain more identity documents. Government-issued standard identification numbers such as "Social security numbers, PAN numbers" are also valuable to the identity thief. Unfortunately for the banks, identity thieves have been known to take out loans and disappear with the cash, quite content to see the wrong persons blamed when the debts go bad.

Fraudulent loan applications: These take several forms varying from individuals using false information to hide a credit history filled with financial problems and unpaid loans to corporations using accounting fraud to overstate profits to make a risky loan appear to be a sound investment for the bank. Some corporations have engaged in over-expansion, using borrowed money to finance costly mergers and acquisitions and overstating assets, sales or income to appear solvent even after becoming seriously financially overextended. The resulting debt load has ruined entire large companies, such as Italian dairy conglomerate Parmalat, leaving banks exposed to massive losses from bad loans.

Phishing and internet fraud: Phishing operates by sending forged e-mail, impersonating an online bank, auction or payment site; the e-mail directs the user to a forged web site which is designed to look like the login to the legitimate site but which claims that the user must update personal info. The information thus stolen is then used in other frauds, such as theft of identity or online auction fraud. Several malicious "Trojan horse" programmes have also been used to snoop on Internet users while online, capturing keystrokes or confidential data to send it to outside sites.

Money laundering: The term "money laundering" dates to the days of Al Capone Money laundering has since been used to describe any scheme by which the true origin of funds is hidden or concealed.

Operations work in various forms

One variant involved buying security (Shares/stocks and bonds) for cash: The securities were then placed for safe deposit in one bank and a claim on those assets used as collateral for a loan at another bank. The borrower would then default on the loan. The securities, however, would still be worth their full amount. The transaction served only to disguise the original source of the funds.

Forged currency notes: Paper currency is the usual mode of exchange of money at the personal level, though in business, cheques and drafts are also used considerably. Bank note has been defined in Section 489A. If forgery of currency notes could be done successfully then it could on one hand made the forger millionaire and the other hand destroy the economy of the nation. A currency note is made from a special paper with a coating of plastic laminated on both sides of each note to protect the ink and the anti-forgery device from damage. Moreover, these notes have security threads, water marks. But these things are not known to most of the population. Forged currency notes are in full circulation and it's very difficult to catch hold of such forgers as once such notes are circulated it's very difficult to track its origin. But the latest fraud which is considered as the safest method of crime without making physical injury is the computer frauds in banks. Computerization of banks had started since 1994 in India and till 2000. 4000 banks were completely and 9000 branches have been partially computerised. About 1000 branches had the facilities for international bank transaction. Reserve bank of India has evolved working pattern for local area network and wide area network by instituting different microwave stations so that money transactions could be carried out quickly and safely. The main banking tasks which computers perform are maintaining debit-credit records of accounts, operating automated teller machines and carry out electronic fund transfer, print out statements of accounts create periodic balance sheets etc.

Internet facilities of computer have revolutionized international banking for fund transfer and for exchanging data of interest relating to banking and to carry out other banking functions and provides certain security to the customers by assigning different pin numbers and passwords.

Computer depredations have been by some classified as:

- Computer frauds
- Computer crimes

Computer frauds: Computer frauds are those involve embezzlement or defalcations achieved by tampering with computer data record or programme, etc. Whereas computer crimes are those committed with a computer that is where a computer acts as a medium. The difference is however academic only.

Computer crimes of banks: Computer crimes are committed mainly for money, however other motive or The Mens rea can be:

- Personal vendetta
- Black mail
- Ego
- Mental aberrations
- Mischief

Bank computer crimes have a typical feature, the evidence relating to crime is intangible. The evidence can be easily erased, tampered or secreted. Moreover, it is not easily detectable. Moreover, the evidence connecting the criminal with the crime is often not available. Computer crimes are different from the usual crimes mainly because of the mode of investigation. There is no eyewitness, no usual evidentiary clues and no documentary evidence. It is difficult to investigate for the following reasons:

Hi-tech crime: The information technology is changing very fast. The normal investigator does not have the proper background and knowledge. Special investigators must be created to carry out the investigations. The FBI of USA have a cell, even in latest scenario there has been cells operating in the Maharashtra police department to counter cybercrimes. C.B.I also has been asked to create special team for fighting cybercrimes.

International crime: A computer crime may be committed in one country and the result can be in another country. There has been lot of jurisdictional problem a though the Interpol does help but it too has certain limitations. The different treaties and conventions have created obstructions in relation to tracking of cyber criminals hiding or operation in other nations".

No-scene crime: The computer satellite computer link can be placed or located anywhere. The usual crime scene is the cyber space. The terminal may be anywhere and the criminal need not indicate the place. The only evidence a criminal leaf behind is the loss to the crime.

Unknown/Faceless crime: The major advantage criminal has in instituting a computer crime is that there is no personal exposure, no written documents, no signatures, no fingerprints or voice recognition. The criminal is truly and in strict sense faceless. There are certain spy software's which is utilized to find out passwords and other vital entry information to a computer system. The entry is gained through a spam or bulk mail. The existing enacted laws of India are not at all adequate to counter cybercrimes. The Indian penal code, evidence act and criminal procedure code has no clue about computers when they were

codified. It is highly required to frame and enact laws which would deal with those subjects which are new to the country especially cyber law; intellectual property right etc. The reserve bank of India has come up with different proposals to make the way easier, they have enacted electronic fund transfer act and regulations, have amended, the reserve bank of India act, bankers book evidence act etc., experience of India in relation to information and technology is limited and is in a very immature state. It is very much imperative that the state should seek the help of the experienced and developed nations.

Mode of operation: The method of alterations of cheques drafts receipts and other fiduciary documents are comparatively simple both manually and with the help of technology.

The bank rules

After receiving xerox papers (which were forged by the offenders) of the property, the bank passed the same on to the legal section. After scrutiny, the legal consultant told the bank that the xerox documents were 'perfect' and to release loan after execution of sale deed. The bank rules state that loan applications can be examined "even with xerox copies of documents. The alleged greediness of employees to give their salary slips and other documents on payment of some money made the job of the cheats easier. This is not an isolated case. With a similar modus operandi, a gang cheated three banks to the tune of Rs. 1 crore in Saroornagar police station area. The police opine that unless bankers evolve a fool proof system, the offenders continue to take advantage of the lapses. Though computer-based banking crimes are yet limited but it is increasing with a huge pace. Their investigation is highly intricate and daunting. Prevention is the best alternative. It is comparatively easier, though even with the best laws, efficient investigation team the successful conclusion of most cybercrimes will remain a remote possibility. Therefore, emphasis is more on prevention. In bank administration, one feels that not much attention is paid to preventive measures. Bank managements must direct their orientation towards preventive rather than detective or punitive measures. Preventive vigilance must be the prime agenda to bring down the occurrence of fraud in banks.

Illustration

A classic case is the recent loan racket busted by the Uppal Police in State Bank of India (SBI)'s Chikkadpally branch. The modus operandi adopted by the racketeers was interesting. A gang of four members approached owner of a newly constructed apartment building saying they were interested in buying the flats. The gang took xerox copies of the building documents after entering into an oral agreement of sale with the builder by paying Rs. 2 lakhs as an advance. Later, they created forged documents in the name of building's owner establishing that the latter had sold five flats to five defence employees. Incidentally, the salary slips and other documents submitted by the loan seekers were found to be genuine. "This was made possible because the gang paid money to the defence employees to utilise their documents," says an investigator. The gang hired an impostor who executed the sale deed posing as the original building owner. "We could not establish criminal negligence on the part of the bank manager and hence he was not arrested," say the detectives. The police learnt that the main lapse in the system is that the banks never asked for the original documents at any stage except for the sale deed for execution of which the offenders planted an impostor.

Secure banking using digital signatures

eMudhra helps large banks in India secure login authentication and fund transfers using digital signatures.

About eMudhra: eMudhra is a global digital identity and leading trust service provider with a focus on digital transformation and cybersecurity initiatives. Through its headquarters in Bangalore, India and offices in Singapore, Dubai and USA, eMudhra works with over 400 large enterprises including 45 banks to deploy proprietary solutions for eSignatures, public key infrastructure, predictive analytics and blockchain across the globe. eMudhra is a licensed certifying authority under ministry of information technology, India and has issued digital signatures to over 40 mn customers in India. eMudhra is a key partner in several digital India initiatives and is the first eSign service provider. eMudhra also holds the vice chairmanship of Asia PKI Consortium, Chairmanship of the India PKI Consortium and is a member of the UN council on blockchain. At eMudhra, innovation is one of our core principles and our product development efforts are towards building cutting edge IP that can accelerate the world's transition to a secure integrated digital society.

The banking regulator in India and The Central Bank-The Reserve Bank of India came out with a detailed study on enabling public key infrastructure and digital signature in the banking system. The report highlighted that the interbank clearing for electronic payment systems used PKI and this constituted over 90% in terms of value of transactions in the year 2012-13. With increasing cyber frauds, the Reserve Bank of India felt the need to extend digital signature usage to end customers of corporate and retail Internet banking since digital signatures offer very high security, enable risk containment and provide legal non-repudiation. Enhancing the security of online banking transactions and electronic payment systems. Banks must create an authentication environment for password based two factor authentication as well as PKI based system for authentication and transaction verification. Customers must be informed of risks; existing security measures and they must be given a choice to select different methods of authentication that matches their security requirements.

Banking security: With increasing transactions taking place over mobile and Internet, the banking regulator the reserve bank of India felt the need to comprehensively enhance security measures in online banking to enhance privacy, confidentiality, authenticity and legal non-repudiation wherever required.

Business needs: Enabling two factor and multi factor authentication for online banking using digital signatures, one time passwords etc based on risk assessment of transactions.

Approach: Deploy an integrated solution for multi factor authentication including digital signatures to allow customers to securely login and conduct online transactions.

Digital signature technology

The digital signature technology works on the public key infrastructure framework which uses a cryptographic key pair-private and public key for secure access and transmission of information. The public key infrastructure framework is prescribed in a model law provided by UNCITRAL (A United Nations body) for international trade and commerce. The emAS solution provides the following broad modules:

emAS: To authenticate, verify digital signature certificates on real time basis

Configuration module: Signature, Encryption and HSM.

Hardware security module: FIPS 140-2 level 3 certified physical computing device that safeguards and manages digital keys for strong authentication and provides cr2 level cessing.

Certificate issuance: To manage the issuance, revocation of digital signature certificates.

Certificate of download: For downloading digital certificates from Certifying Authority (CA) as a soft or crypto token.

Certificate of registration: To allow the customer to register their digital signature on the application.

Benefits: Banks have reaped significant benefits by implementing digital signature-based authentication and fund transfers. These includes:

- Legal non-repudiation thereby reducing frauds.
- Enabling enhanced security through the full chain of electronic payments from initiation to settlement.
- Offering anywhere, anytime filing of forms for customer onboarding, service requests etc.
- Faster turnaround time, increased employee efficiency, productivity and transparency meeting compliance and regulatory requirements.

Solution: Benefits eMudhra being a Licensed Certifying Authority in India and a PKI solution provider implemented emAS-eMudhra authentication server to enable digital signature based login and fund transfer. emAS is a plug and play authentication server that is implemented in over 45 banks in India across a variety of core banking/internet banking applications. emAS works on top of the internet banking platform to provide digital signature signing and authentication. It works with leading core banking platforms such as Finacle, Flex cube, Bancs etc (Figure 17).

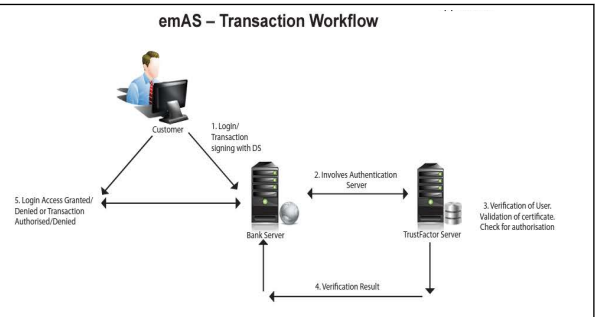

Figure 17: Transaction work flow.

CONCLUSION

Signature is widely used as a means of personal recognition and verification process; and neural network is the verification system that is based on the human brain approach for pattern recognition, so when neural networks are used to verify handwritten signature then the efficiency of the verifying system increases by a great amount. In this paper the offline signatures verification system is used for the verification of signature image. In this approach a signature image is first pre-processed for the removal of noise and converted into binary image of 200 × 200 Pixels and then the features, such as Eccentricity, Kurtosis, Skewness etc., are extracted from the image and then normalization of the features are done and after that These normalized features are used to train the neural network using back-propagation technique. The proposed algorithm provide more robust verification system when compared to other methods and this improvement is mainly due to normalization of the features before used in classification process which prevent the dominance of certain features over others.

REFERENCES

1. Chijindu AT, Angela UE, Steven A. Digital signature verification system to enhance customer services in the banking industry. Int J Eng Comput Sci. 2019;8(6):24686-24692.
2. Patil P, Patil B. A review-signature verification system using deep learning: A challenging problem. Int J Sci Res Sci Technol. 2021;2021:295-298.
3. Tariq U, Hu Z, Tariq R, Iqbal MS, Sadiq M. High-performance embedded system for offline signature verification problem using machine learning. Electronics. 2023;12(5):1243.
4. Trikha M, Singhal M, Dutta M. Signature verification using normalized static features and neural network classification. Int J Electr Comput Eng. 2016;6(6):2665.
5. Zhou Y, Zheng J, Hu H, Wang Y. Handwritten signature verification method based on improved combined features. Appl Sci. 2021;11(13):5867.
6. Shashidhar S, Sravya A. Online handwritten signature verification system: Using Gaussian mixture model and longest common sub-sequences. 2017.
7. Thangavel V. Use of Digital Signature Verification System (DSVS) in various industries: Security to protect against counterfeiting. Z-Global Bank eJournal. 2023;15(2).
8. Alajrami E, Ashqar BA, Abu-Nasser BS, Khalil AJ, Musleh MM, Barhoom AM, et al. Handwritten signature verification using deep learning. 2020.
9. Saleem M, Kovari B. Online signature verification using signature down-sampling and signer-dependent sampling frequency. Neural Comput Appl. 2021:1-3.
10. Saeidi M, Amirfattahi R, Amini A, Sajadi M. Online signature verification using combination of two classifiers. In 2010 6th Iranian Conference on Machine Vision and Image Processing. Isfahan, Iran. 2010 (pp. 1-4).
11. Yanikoglu B, Kholmatov A. Online signature verification using Fourier descriptors. EURASIP J Adv Signal Process. 2009;2009:1-3.
12. Shin J, Sato J. Signature verification for multiuser online kanji learning system. Comput Technol Appl. 2012;3(3).

13. Sharif M, Khan MA, Faisal M, Yasmin M, Fernandes SL. A framework for offline signature verification system: Best features selection approach. Pattern Recognit Lett. 2020;139:50-59.
14. Chang WD, Shin J. DPW approach for random forgery problem in online handwritten signature verification. In2008 Fourth International Conference on Networked Computing and Advanced Information Management. 2008;1:347-352.
15. Nakajima S. On-line signature verification using pen inclination. IEICE Technical Report. 1998.
16. Shree S, Pratap B, Saroy R, Dhal S. Digital payments and consumer experience in India: A survey based empirical study. J Bank Financial Technol. 2021;5:1-20.
17. Maiorana E, Campisi P, Neri A. Template protection for dynamic time warping based biometric signature authentication. In2009 16th International Conference on Digital Signal Processing. Santorini, Greece. 2009. (pp. 1-6).
18. Shin J, Takeda A. Character learning system using inter-stroke information. InKnowledge-Based Intelligent Information and Engineering Systems: 8th International Conference, KES 2004, Wellington, New Zealand. 2004, pp. 165-174). Springer Berlin Heidelberg.