Journal of Information Systems Engineering and Management
2025, 10(14s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CNN Versus Conditional Generative Adversarial Network cGAN–Digital Signature Authentication: Case Study

M Ranga Swamy[1], Vijayalakshmi.P[2*], Rajendran.V[3]

[1,2,3]*Department of Electronics and Communication Engineering, Vels Institute of Science, Technology and Advanced Studies, Chennai, TamiL Nadu, India*

[1]*ranga1310@gmail.com*, [2*]*viji.se@vistas.ac.in*, [3]*director.ece@vistas.ac.in*

ARTICLE INFO

Received: 24 Nov 2024
Revised: 10 Jan 2025
Accepted: 21 Jan 2025

ABSTRACT

In this research work, the author gathered digital signature images from students in real time appropriate for identifying the fake signature and classifying the images into real and forgery. Convolutional Neural Network based approach, GAN, ResNet and CGAN techniques were employed to extend the system which can authenticate and identify forged signatures among students. The features are extracted from real time signature images using Principle Component Analysis, the most popular multivariate statistical techniques. Moreover, feature selection has done for choosing subset of best and worst features randomly from signature images, fed signature image parameters into neural network for training the images. The performance of proposed model is evaluated in terms of metrics such as accuracy, F1-measure and precision. Our experimental outcomes reveal that CNN model achieved 100% accuracy outperforms in detecting fake digital signature signed by students helpful in ensuring authenticity, integrity of documents, assignments, preventing frauds as well.

Keywords: Convolutional Neural Network (CNN), Conditional Generative Adversarial Network (CGAN), ResNet model, Digital Signature Application, Principal Component Analysis (PCA).

INTRODUCTION

Authenticity is a necessary component of social interaction. There has been an increase in interest of personal identity authentication in recent years. Nowadays much attention has shifted to fingerprinting due to growing safety concerns. In several universities, individual employee recognition and authorization have been made possible by the application of biometric technology, which has grown in importance in the field of human verification. Individual recognition based on a person's unique traits is referred to as biometric Shervin et al. [1].

Authentication and validation chores are referred to as recognition. Amongst a several recognized users, authentication indicates which person supplies a particular biometric feature. As a result, signature image used for recognition only includes accurate information. Validation, on the other hand, ascertains whether the supplied biometric parameter has been supplied by a particular authorized person or fake individuals. One of the most used methods for determining someone's identification is handwritten signature recognition. However, several researchers focused on authentication rather than recognition due to every day usage of signature verification systems [2].

Signature authentication has two kinds namely online signature which signed in devices and applications whereas offline signature signed in documents directly in-person. The signature's form is recorded in the offline environment. As a result, input data for offline verification systems includes coordinates (x, y) of signatures. On the other hand, while the user is signing online, the system uses gadgets to record more information [3]. Online signatures provide additional data that can be extracted, features including orientation, strain, duration, and pen up/down.

1.1 Why Digital Signature Verification Significant?

Maintaining the validity, truthfulness, and non-disclosure of electronically transmitted documents, messages, or transactions requires digital signature verification. This is why digital signature verification is necessary:

Authentication: Digital signatures confirm the sender's or signer's identity. They make sure the document or message was transmitted by the person who claimed to be the sender and that it wasn't changed in route.

Truthfulness: A digital signature guarantees whether the message or document's contents haven't been altered since it was signed. A failure authentication will occur if the electronically signed data is altered in any manner.

Non-repudiation: A digital signature keeps the sender from claiming they had nothing to do with the creation or delivery of the document or message. It is impossible for the signer to retract their actions once they have been signed.

Legal compliance: Digital signatures are just as legally binding as handwritten signatures in many jurisdictions. Contracts, agreements, money transfers, and other legally binding papers can all be done with them.

Security: Unauthorized parties find it very difficult to counterfeit or alter digital signatures without being detected since cryptographic procedures are used to create distinct signatures.

Trust: When parties exchange documents or conduct electronic transactions, communication, or transactions involving digital signatures, trust is increased. It guarantees the security and dependability of the information shared.

In the current digital environment, digital signature verification is essential to the security of digital transactions, communications, and documents.

1.2 Problem Statement

Various aspects of student's digital signature authentication are

Guarantees the accuracy, legitimacy of assignments, papers, and submissions of student's record on digital signature verification. This confirms that the signature on the document is actually the claimed sender or signer and that it has not been altered.

Academic Integrity - Students' understanding of the value of academic honesty is reinforced by the implementation of digital signature verification.

Stopping frauds - It prevents educational dishonesty such as cheating and copying work by giving an easy way to confirm the legitimacy of contributions.

Effectiveness & Feasibility - Knowing that their validity will be immediately confirmed gives students peace of mind when submitting papers digitally.

In general, the implementation of online digital signature verification among students is beneficial for safeguarding of educational surroundings, organizational effectiveness, and academic credibility. It offers a dependable method for confirming the legitimacy and consistency of computerized records, improving adherence with confidence in learning environments.

To address these issues, this research work listed the following objectives on digital signature recognition and verification using real time student's signature images.

1.3 Objectives

The main intention of this research work listed as follows:

- The authors have been collected digital signature images from students in real time to ensure authenticity, integrity of documents, assignments, preventing frauds.
- Here, Principle Component Analysis technique is utilized for extracting features in the form of standard pixels relevant with decomposition of Eigen values into Covariance matrix/Variance ratio.

- Developed deep learning based models such as ResNet50, Generative Adversarial Network, Conditional Generative Adversarial Network, and Convolutional Neural Network for digital Signature verification using real time signature dataset.
- CNN achieved better results in terms of accuracy, precision, recall as 100% with lesser Loss 0.2 milliseconds when compared to other conventional methods in digital signature verification among students.
- Comparison has done with existing research work on online signature and handwritten signature in terms of accuracy, train: test splitting of images, signature images used, methodology implemented, whether signature verification or detection of real or fake, kind of programming language applied.

BACKGROUND

During the year 1977, several researchers investigated verification of signature on both handwritten as well as online authentication in which the features are extracted from images vertically and horizontally has been described. During 1994, the authors of Yingyong et al. [4] described that signature has been verified using global as well as grid features. Moreover, the authors discussed about the issues facing towards signing documents, and various techniques were used to resolve all such issues. The difference among online and offline verification are listed in Table 1.

Table 1: Difference among Online and Offline Verification

Online verification	**Offline Verification**
No noise	Include lot of noises
Online verification process very fast	Verification process is little slow when compared to online process
The data gathered via devices such as mobile phones, tablets etc.	The raw data collected as scanned signature
Signature accuracy is very high	Here the signature accuracy is fairly high

2.1 Digital signature

Jose Lopes et al. [5] established a number of methods for resolving problems like distinguishing between genuine and false signs in documents. Artificial Neural Network was established by Oladele et al. [6] for detecting forgery signature. The facility of secure digital signature in various industry based application explained by Ananthi Sheshasaayee et al. [7] via cryptographic algorithms like RSA. Followed by that Teng Yang et al. [8] analyzed digital signature based on ISRSAC during the year 2017.

2.2 Handwritten signature

Additionally, the authors of Hsin et al. [9] employed the CNN approach to verify offline signatures and detected fraudulent signatures that were applicable in a variety of business scenarios, such as the human assessment-based bank check payment sign verification procedure. Hashim et al. [10] surveyed various research work during last decades focused on both online as well as offline signature images Ahmad et al. [11] suitable for finding fake and real signature using Hidden Markov model, machine learning approaches Hameed [12] and deep based framework by Shruti et al. [13]. CNN model based 3-dimensional handpose algorithm Jameel et al. [14] was applied on signature images by Eman Alajrami et al [15] for verifying handwritten signature. Bibi et al. [16] reviewed various articles in relevant with both machine learning and deep learning techniques for verifying handwritten signature to enhance the secure documents. Harish et al. [17] and Chinmay et al. [18] used machine learning algorithms such as Naïve Bayes, Random Forest and KNN for identifying handwritten signature via filtering technique, feature extraction and principle component analysis. Debasree et al. [19] applied feature detector technique such as

HARRIS and SURF in which the corners are detected in images finally based on matching factor, handwritten verification has done.

Sadkhan et al. [20] introduced two approaches namely optical mark recognition which finds that signature is real or fake subsequently multi-class CNN model [Gabe Alvarez] especially AlexNet framework which identifies and classifies into real or fake signature. Features of signature are extracted via angle based method by Padmajadevi et al. [21] finally train the parameters using neural network for further identification and verification of signature. Features are extracted via deep based CNN subsequently evaluation had completed with triple loss approach discusses by Shalaw et al. [22]. This research work surveyed various articles regarding signature verification discussed in Table 2.

Table 2:I State of art among conventional approaches on Digital signature authentications

Authors	**Dataset used**	**Methodology**	**Online/Offline**	**Verification/ Detection**	**Programming language**
Hsin et al. [9]	Signature	CNN	Offline	Verification and Detection	Python
Oladele et al. [6]	Signature database	Feature extraction using ANN	Offline	Detection	Java
Alajrami et al. [15]	300 signature images Kaggle dataset	CNN	Handwritten	Verification	Python
Chinmay et al. [18]	Kaggle signature dataset	Machine learning	Handwritten	Verification	Python
Jameel et al. [14]	In-air signature dataset (1800 images)	Deep learning	Offline	Verification	Python
Jivesh et al. [23]	Signature image dataset	Deep CNN+ Crest Trough method	Offline	Verification and detection	Python
Jose et al. [5]	160 signature		Handwritten		Python with OpenCV library
Padmajadevi et al. [21]	MCYT signature database	Extraction of features via angle based method + Neural Network	Handwritten	Both signature recognition and verification	Python
Shalaw et al. [22]	TOW dataset	CNN for extraction from images, estimated via triple loss	Offline	Recognition	Tensorflow + Python pcks
Teng Yang et al. [8]	ISRSAC	RSA + DSA	Digital Signature	Verification	Cryptographic applications

Xinyu Lei et al. [24]	Mnist Handwritten digital Signature images	Dilated CNN model	Digital signature	Classification	Tensorflow + Python pcks

RESEARCH METHODOLOGY

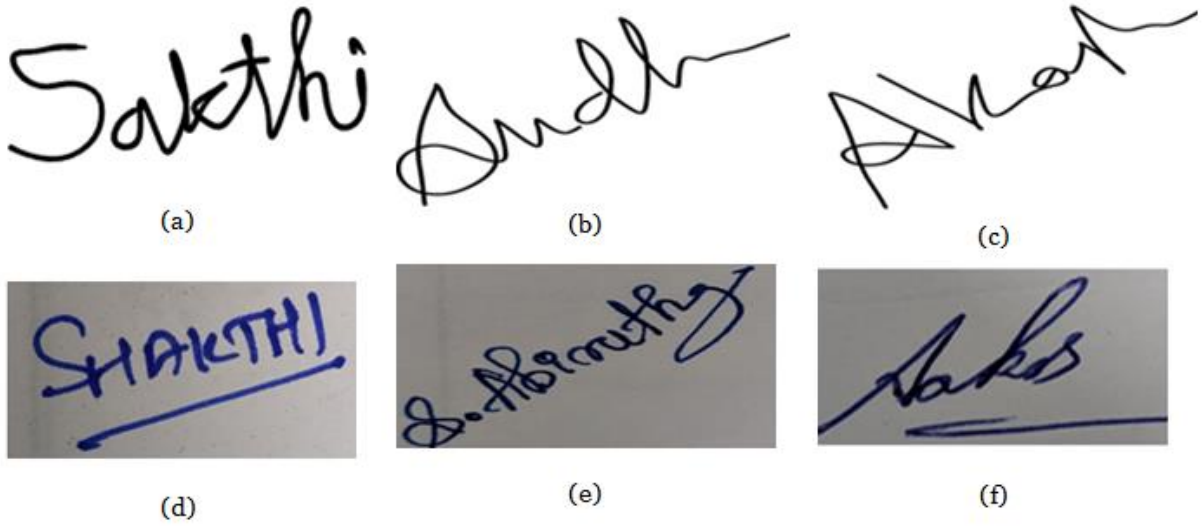
3.1 Dataset Description

The authors gathered digital signature images from students under the Department of computer science and Engineering, Electronics and Communication Engineering of Vels Institute of Science Technology and Advanced Studies, using Electronic Signature Maker application. Such images are separated into fake and real signatures which are saved in drive folder. The real time signature image dataset of student link is mentioned below [25].

https://drive.google.com/drive/folders/15w4yoBD8RNJJf7Bq2Vik-5EpoUzMw8-B?usp=drive_link

3.2 Preprocessing

The primary objective of preprocessing is to enhance the image quality so that it is prepared for further analysis by eliminating or minimizing the extraneous and unconnected background details from digital signature images. The raw input real time signature images utilized in this research work in which fake images are depicted as Figure 1(a) 1(b) and 1(c) whereas real images are shown in 1(d) 1(e) and 1(f).



Pre-processing is therefore necessary to raise the level of excellence. The images of signature will be ready for the subsequent two processes namely extraction of features and classification. Filters eliminate higher-frequency elements and disturbance.

3.3 Extraction of features

Feature extraction, which is commonly employed in domains like image interpretation, computation of signals, and data retrieving, is more beneficial as rendering aids.

Principle Component Analysis

The basic concept of the principle component analysis is the strong correlation between the individual pixels of signature images which frequently represent virtually identical object attributes. The raw data is transformed using statistical techniques in order to eliminate the pixel-to-pixel correlations. During the procedure, the most successful linear pairing of the source photos that accounts for a particular image's fluctuation in pixel density is found.

Here the authors extracted features using PCA which determines statistical properties of digital signature images moreover observe the correlation on images. The transformation of images into pixels elicited from statistical rule called Eigen-values breakdown of covariance matrix of input images to be investigated.

To compute image pixel vector of signature images, use the formula (1)

$$X_i = [x_1, x_2, \ldots\ldots x_N]_i^T \qquad (1)$$

Where x_1, x_2, ... x_N represents the pixel values from resultant pixel location of input signature image. The size of signature image vector equivalent to number of squares in pixels considered as rows I and columns I, the vectors will be R=r*c specifically i=1, 2, ... r.

For finding mean vector of entire signature image is estimated as eqn. (2)

$$r = \frac{1}{R}\sum_{i=1}^{R}[x_1, x_2, \ldots\ldots x_N]_i^T \qquad (2)$$

Also, the Covariance matrix can be defined as (3)

$$Covariance(x) = E\big(x - E(x)\big)\,(x - E(x))^T \qquad (3)$$

Whereas T signifies Transpose, x represents pixel values, E(x) represents expectation of pixel values. Now apply eqn. (3) in eqn. (2) considered as Covariance matrix formulated as eqn. (4)

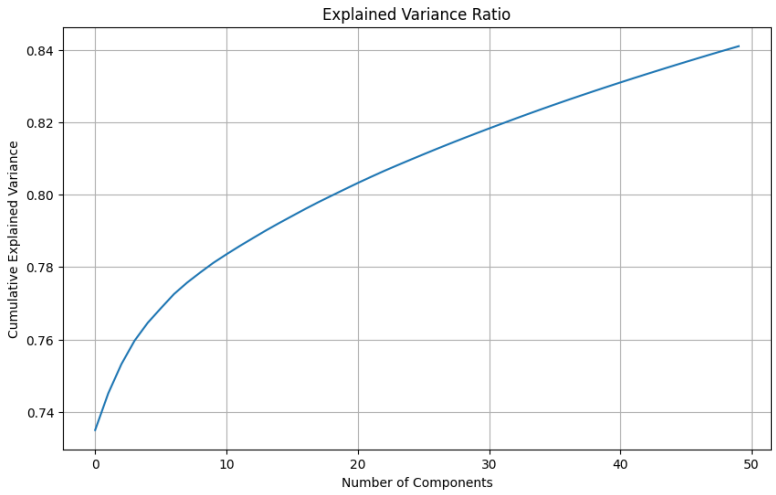
$$Cov_x = \frac{1}{R}\sum_{i=1}^{R}(x_i - r)\,(x_i - r)^T \qquad (4)$$

The Eigen-value based decomposed are underlying the matrix of covariant values, assuming the following format, provides the basis of PCA:

$C_x = ODO^T$, here D= λ_1, λ_2, ... λ_N

Wherein D represents diagonal matrix comprises Eigen values namely λ_1, λ_2, ... λ_N of Covariance matrix. O and O^T indicates Ortho-normal matrix and its transpose.

Every input image are flatten into one-dimensional array based on height and width, such data are normalized/standardized into 255 pixels, perform PCA analysis by adjusting the number of components which are visualized as variance ratio. The variance ratio graph increases as shown in Figure which is plotted among cumulative explained variance and number of components.



A. Features are listed after extracted by PCA

Here are the features (Feature 1 to 50) listed with 10,000 rows which are extracted using Principle Component Analysis.

	Feature 1	Feature 2	Feature 3	Feature 4	Feature 5	Feature 6	....	Feature 49	Feature 50
PC_1	-0.0106	-0.0002	-0.0085	-0.0069	0.0084	-0.0063		-0.0003	-0.0005
PC_2	-0.0105	-0.0005	-0.0089	-0.0064	0.0082	-0.0063		-0.0013	-0.0018
PC_3	-0.0105	-0.0004	-0.0080	-0.0062	0.0086	-0.0070		-0.0022	-0.0051
PC_4	-0.0105	-0.0009	-0.0075	-0.0059	0.0075	-0.0064		-0.0017	-0.0028
PC_5	-0.0106	-0.0015	-0.0075	-0.0068	0.0067	-0.0064		-0.0030	-0.0016
...	...	...	...	...	...	...	...	...	...
PC_9997	-0.0090	0.0029	0.0126	0.0018	-0.0068	0.0113		-0.0009	0.00515
PC_9998	-0.0090	0.0147	0.0106	0.0001	-0.0076	0.0118		-0.0003	0.00725
PC_9999	-0.0092	0.0025	0.0109	0.0006	-0.0070	0.0109		0.00074	-0.0008
PC_10000	-0.0093	0.0032	0.0129	0.0035	-0.0068	0.0079		0.00198	-0.0048

3. 4 Selection of features

Reducing the degree of complexity within the primary issue using specialized strategies is a common option while confronting a substantial amount of supplied features, and it can also occasionally lead to better achievement in learning. Techniques for reducing dimension are often separated into two categories: feature extraction and feature selection. The primary distinctions between these two are: feature extraction picks a subset of the initial traits whereas feature selection blends the primary characteristics to produce an ensemble of novel characteristics. Typical example for describing the difference among feature extraction and feature selection is depicted as Figure 1.

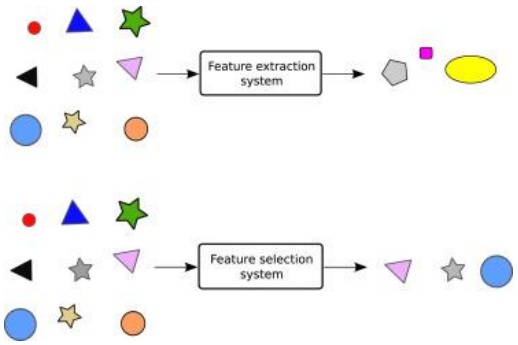


Figure 1: Typical example for describing feature extraction and selection

The features are selected to identify best and worst features by that appropriate classification algorithm can built which undergoes the images are classified into fake and real. Whenever accessibility and data recovery are critical, like image based data, feature selection that creates subset of the unique feature is helpful, even though occasionally it reduces performance. Since the foundation of our work is signature based image input, this research work concentrate on feature selection.

a. Selection of Best features

From digital signature input images, totally 50 features have chosen for finding best features appropriate in model deployment listed in Table 3 and 4 therefore classification of images into fake and real signature among students studied in universities.

Table 3: Best Features Selection

	Feature 1	Feature 2	Feature 3	Feature 4	Feature 5	Feature 6	....	Feature 49	Feature 50
PC_5541	-0.0090	-0.0144	-0.0158	0.0278	-0.0007	0.0271		0.0314	0.0111
PC_4554	-0.0087	0.0100	-0.0052	0.0394	0.02017	0.0163		-0.0040	0.01306

PC_4654	-0.0085	0.0075	-0.0036	0.0354	0.02265	0.0182		0.0255	0.00806
PC_4541	-0.0094	0.0185	-0.0209	0.0248	-0.02074	0.0250		-0.0026	0.03426
PC_6136	-0.0096	-0.0258	-0.0111	0.0111	0.00319	0.02096		-0.0123	0.01059
PC_4934	-0.0088	0.0079	-0.0282	0.0276	-0.02207	0.0240		-0.0627	-0.0224
PC_5529	-0.0090	-0.0069	-0.0237	0.0181	-0.01586	0.0172		0.02026	0.0059
PC_5641	-0.0094	-0.0175	-0.0130	0.0269	-0.00229	0.0185		0.0388	0.0060
PC_4942	-0.0092	0.0058	-0.0217	0.0321	-0.00247	0.0189		0.0014	0.0457
PC_4758	-0.0093	0.0055	0.0052	0.0283	0.03185	-0.009		-0.044	0.0089

Table 4: Selection of Worst Features

	Feature 1	Feature 2	Feature 3	Feature 4	Feature 5	Feature 6	...	Feature 49	Feature 50
PC_36	-0.0097	0.0021	-0.0008	-0.0029	0.0044	-0.0038		0.00005	-0.0012
PC_136	-0.0098	0.0012	-0.0013	-0.0394	0.0044	-0.0043		0.00148	-0.0012
PC_61	-0.0089	0.0046	-0.0051	-0.0006	0.0015	-0.0014		-0.0002	0.00056
PC_56	-0.0091	0.0047	-0.0042	-0.0014	0.0020	-0.0258		0.00032	0.00081
PC_35	-0.0097	0.0018	-0.0012	-0.0032	0.0050	-0.0041		0.00052	-0.0013
PC_134	-0.0098	0.0017	-0.0013	-0.0034	0.0049	-0.0041		0.00005	-0.0013
PC_162	-0.0089	0.0050	0.0054	-0.0006	0.0016	-0.0019		-0.0007	0.00117
PC_130	-0.0099	0.0015	-0.0022	-0.0032	0.0051	-0.0041		0.00011	0.0020
PC_928	-0.0100	0.0010	-0.0023	-0.0034	0.0045	-0.0026		-0.0018	-0.00086
PC_32	-0.0097	0.0019	-0.0019	-0.0034	0.0046	-0.0039		-0.0005	-0.0011

We outline innovative feature selection approaches which are now appreciated within various scientists. Such approaches are described as below:

b. Feature Selection based on correlation

A multivariable filtering technique selects subsets of traits themselves which are incompatible however exhibit a significant association with overall class. The features had chosen based on correlation as Hall et al. [27].

c. Feature Selection based on consistency

Multimodal method that employs inconsistent criteria for determining an appropriate data minimization ratio after choosing selections of traits based on how consistent they appear to be within the group of features Dash et al. [28].

With deep learning tasks, selecting features appears to be an effective preliminary technique. As previously said, it may seem challenging to choose among the increasing variety of feasible selecting techniques. The capability for a variety of cutting-edge approaches to feature selection to address typical issues like data discontinuity, correlation coefficients and redundant operation, disturbances in the features supplied, disturbances in the target category, and getting an excessive amount of features compared to amount of data points has been examined in a prior study Baskar et al. [29].

d. Mean feature loading

“Feature loading” in selecting features describes how every characteristic (or variable) adds onto a certain aspect or paradigm. It is frequently employed in methods such as Factor Analysis and Principal Component Analysis (PCA). The relationship among the initial characteristics with the principal components is referred to as features loading in PCA. The original features are combined linearly to form each primary component, and feature loading indicates the relative contribution for every unique trait to the corresponding factor.

Factor analysis is reminiscent of PCA in that it requires combining the initial characteristics in a sequential manner. During factorization, feature loading provides information on the connection among the fundamental factors and the initial parameters.

By determining which characteristics are particularly important for preserving the basic framework or addressing data deviation, feature loading may assist in choosing features. High loading features on significant components or aspects are frequently kept, whereas weaker loading features could be eliminated to make the model simpler or less multidimensional. The distribution of mean feature loading is plotted among mean loading of image features with frequency depicted as Figure 2.

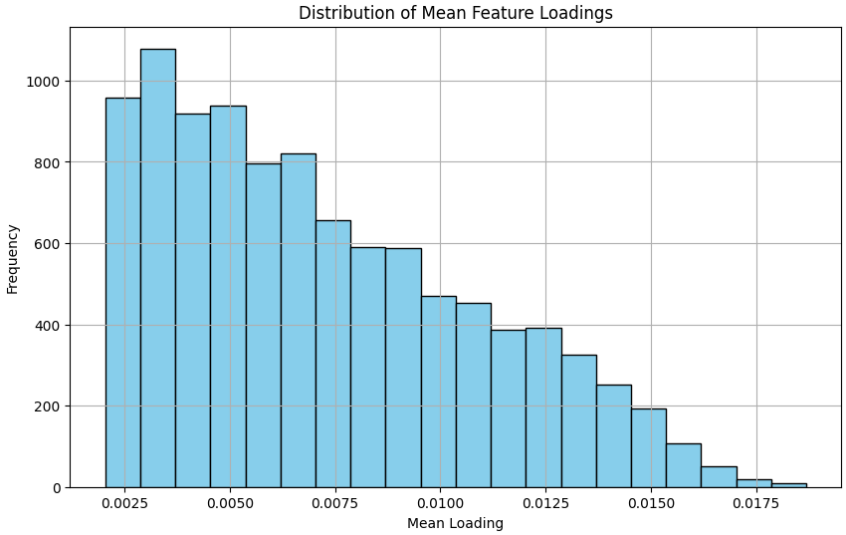


Figure 2: Distibution of Mean Feature Loadings

e. Random best features

Feature extraction and selection algorithms are frequently used to identify the most significant features from signature photos. Whereas feature extraction entails converting the initial collection of characteristics into a new, more informative set of features, feature selection entails choosing a subset of pertinent features from the original set of features. Popular feature selection techniques in the context of image data include filter, wrapper, and embedding techniques. While wrapper techniques assess feature subsets using a particular machine learning algorithm, filter methods utilize statistical measures to determine the relevance of features, and embedding approaches choose features as part of the model-training process depicted as Figure 3.

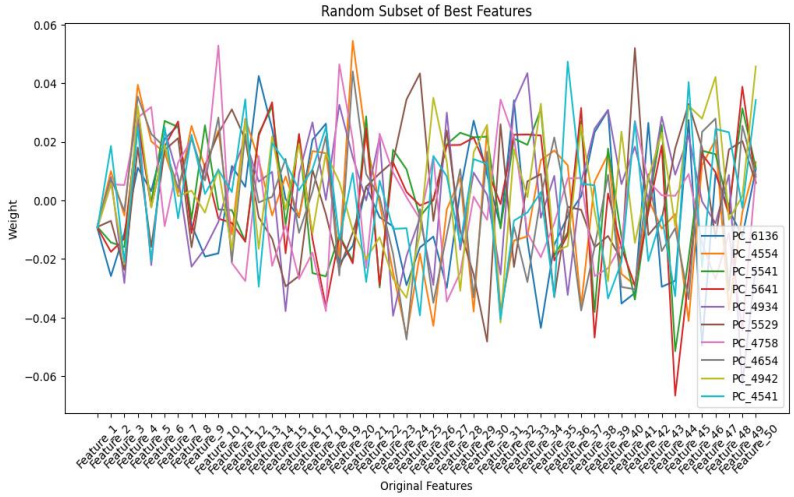


Figure 3: Selection of best features in Signature verification

f. Random Worst features

The general objective of feature selection is to find and keep the most instructive and pertinent characteristics while removing superfluous or unnecessary ones. Randomly choosing the “worst” characteristics is not a frequent

approach in selecting attributes since these defeats the goal of choosing among the most beneficial characteristics to enhance a model's performance. Selecting features at random, particularly the ones deemed "worst," may generate interference and lower the model's overall efficacy. Statistical measurements, predictive capacity, correlation with the target variable, and other criteria are some of the factors that feature selection techniques use to carefully assess each feature's value.

Randomly choosing features or selecting the worst features increases the chance of adding noisy or insignificant characteristics to the model represented as Figure 4. This can cause overfitting, poor predictive accuracy, and outcomes that are harder to comprehend. As a result, rather than choosing or including the worst features at random, the goal of feature selection is to find and keep the best characteristics that significantly increase the model's predictive potential.

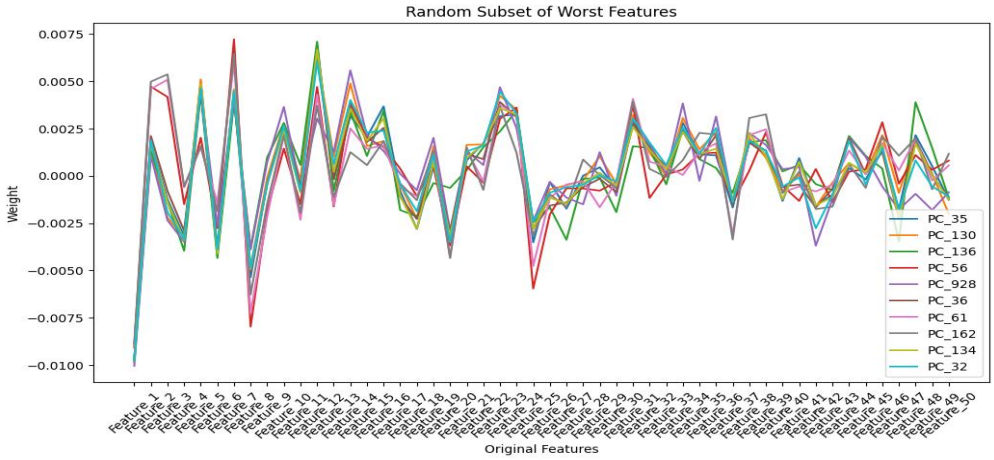


Figure 4: Selection of worst features

MODEL PROPOSED

4.1 ResNet50 model

He et al. (2016) constructed a model called ResNet, or deep residual network 11 [30]. This design was created to overcome challenges in deep learning while training images, which is typically time-consuming and restricted to a particular quantity of layers. The explanation for the complexity that ResNet created is to use an alternative or bypass connectivity. When compared to other architectural models, ResNet model has the benefit of maintaining effectiveness as its framework becomes more complex. Additionally, there is a reduction in computational operations and an improvement in training network capabilities. By bypassing interconnections on up to three layers incorporating batch normalization and ReLU, the ResNet model has been implemented shown in Figure 5. This model outperforms other models in image categorization, demonstrating the quality of the image extraction of features.

$$z = F(y, W + y) \qquad (5)$$

Z represents output layer, y indicates input layer, F represents function which mapped the residual block.

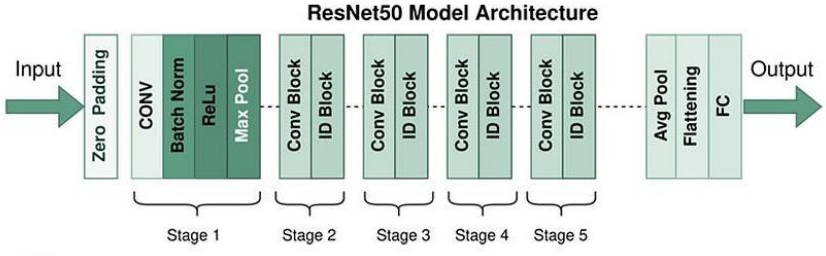


Figure 5: ResNet50 Architecture for Signature Verification

ResNet-50 has shown to be extremely effective across a range of signature image classification applications, including extremely fine identification, object identification, and image recognition. Additionally, it has served as the foundation for a number of applications involving computer vision, such as tracking of objects and segmentation with semantics. All things considered, ResNet-50 is a strong and popular deep neural network framework that significantly raised the benchmark for several image classification tasks. Hence the authors applied this model with four layers Convolutional, Batch Normalization, ReLu and Max pool layer for five stages then fed into pooling layer, passes into flattening layer which is fully connected layer that produces classification of signature images as fake and real.

4.2 CNN model for Signature Authentication

Convolutional neural network is a kind of feedback neural network that is commonly used to analyze signature data. The CNN structure's architecture can produce multilayered representations while successfully maintaining the underlying data's layout. Multifaceted computational levels in a CNN framework are typically arranged ascending from left to right. Four distinctive kinds of tiers are commonly seen in CNN: convolutional, pooling, fully connected, and classifying layers. The key components of the layout include pooling and convolutional layers, which are usually used in the initial stages which are fed into flatten layer, then fully connected layer passed into output layer that predicts the probabilistic distribution either real signature or fake.

The typical Convolutional Neural Network model for Signature verification and classification is depicted in Figure 6.

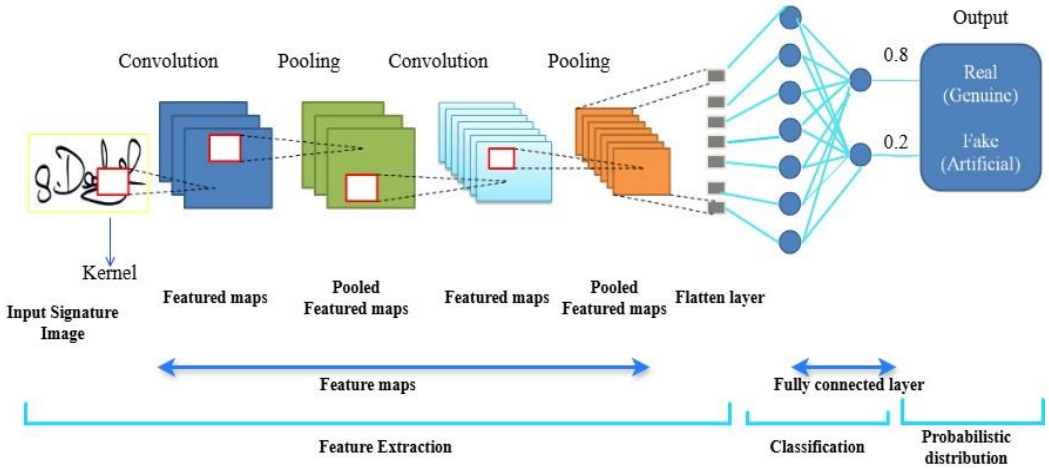


Figure 6: CNN Framework for Digital Signature verification

Sequential Model

Layers	Dimensional	Layers with function
Conv2D	2-D	(32,(3,3)), activation="ReLu"
MaxPooling2D	2-D	((2,2))
Conv2D	2-D	(64, (3, 3)), activation = "ReLu"
MaxPooling2D	2-D	((2,2))
Conv2D	2-D	(64, (3, 3) , activation = "ReLu")

Dense	1-D	64, activation = “ReLu”
Dense	1-D	1, activation=”Sigmoid”

The most popular continual and smoothing activating function is the sigmoid function, sometimes referred to simply as the logistical function. Therefore the actual numbers in images are translated into binary classification as class 0 and class 1, and it is utilized in the outcome of neuron in a hidden layer. This can be formulated as eqn. (6)

$$f(x) = \frac{1}{1 + e^{-x}} \qquad (6)$$

Rectified Linear Unit function solves the vanishing gradient issues which can be formulated as eqn. (7)

$$f(x) = \max(0, x) \qquad (7)$$

After training the features via layers in neural network, the model is compiled and optimized using Adam optimizer however losses are estimated using binary cross entropy, furthermore the model is trained with ten epochs finally the model evaluated in terms of accuracy.

4.3 GAN and cGAN model

An artificial intelligence algorithm called generative adversarial networks was created to address the generative modeling issue. A generative model looks at a set of training examples and aims to identify the probability distribution that produced each one. The estimated probability distribution can then be used to create more instances using Generative Adversarial Networks (GANs). A “generator” network’s objective in the GAN framework is to trick a “discriminator” network into thinking that signature sample images it is using are actual data. We also give each network the option to rely on any additional information that can be used to define the imagery that has been produced or recognized.

The cGAN, or conditional generative adversarial network, is a fundamental modification of the GAN model that enables the simulation to be constrained on signature image data. It was first suggested with preliminary tests in [31]. This allows for the learning of many “modes” for the previously acquired generative framework by the application of various context-related data. The discriminator network in BEGAN is likewise intended to determine the loss model value, much to Conditional GAN. Reducing the disparity among the original image and the resultant loss of information is the aim of the discriminator network.

PERFORMANCE EVALUATION

It is necessary to ascertain various evaluation metric attributes in order to assess the efficacy of the suggested filtering technique. To determine whether filtering technique can significantly improve outcomes for digital image signature verification, a thorough experimental analysis is conducted. Real-time images [25] of digital signatures are employed for research purposes. In essence, metrics are used to track and assess a model’s performance both during the training and testing phases; they are not required to be differentiable. We consider the following four performance measures in order to estimate the performance of our unique deep learning models.

Precision- Precision indicates the ratio of truly identified positive digital signature image from predicted digital signature predicted positively described as eqn. (8).

$$Precision = \frac{Truly\ identified\ positive\ samples}{Positively\ predicted\ samples} \qquad (8)$$

F1 Score- F1-Score is defined as the harmonic mean of both precision and recall which can be formulated using eqn. (9)

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \qquad (9)$$

Accuracy- Classification accuracy is a potentially very basic statistic that is calculated by dividing the total number of predictions by the number of right predictions, then multiplying the result by 100. In this case, differentiating

between the digital signature verification and true sign from fraudulent sign depends on the classification accuracy. Accuracy can be calculated using eqn. (10)

$$Accuracy = \frac{Amount\ of\ positively\ predicted\ with\ distinguished\ image\ sample}{Total\ number\ of\ signature\ images} \times 100\% \quad (10)$$

Loss- The loss function is characterized as a function that demonstrates the model's performance and is also used to train deep learning techniques, such as CNN, ResNet50, GAN and CGAN, through multiple optimization categories that are typically distinguishable in the model's dataset.

EXPERIMENTAL RESULTS

6.1 Experimental testbed with its real time dataset

The following components of the experimental setup are used in this paper: The PC has TensorFlow, a deep learning framework, and an IntelI CoreI i5-6700HQ CPU running at 2.60GHz with a GPU of NVIDIA GeForce GTX 1070. The physical memory (RAM) is 16.0 G.

Conventional techniques for getting student signatures might be imprecise or necessitate invasive techniques, which can be uncomfortable and dangerous. Deep learning methods have shown promise in reducing student pain and increasing the reliability of digital signature authentication. In this work, we proposed a deep learning-based approach leveraging real-time dataset photos for digital signature authentication.

6.2 ResNet50 model

From the table 5, it is clearly explained that ResNet50 model has been evaluated for identifying the fake signature and undergoes classification of fake and genuine signs. Based on number of epochs, the images are trained using neural network in which the features are trained thereby losses and accuracy are evaluated.

Table 5: Evaluation of ResNet50 model

Epochs	Execution time (s)	Validation Loss	Validation Accuracy
1	286	-40.232	0.3327
2	298	-247.466	0.3346
3	278	-703.706	0.3346
4	281	-1423.278	0.3346
5	277	-2434.156	0.3346
6	277	-3711.348	0.3346
7	277	-5300.864	0.3346
8	277	-7115.284	0.3346
9	275	-9202.716	0.3346
10	277	-11516.895	0.3346

6.3 CNN model

As can be seen from the table 6, CNN model has been assessed for detecting phony signatures and is classified as either genuine or fake. The images are trained using a neural network that learns the features through a series of epochs, after which accuracy and losses are assessed.

Table 6: Performance estimated on CNN model

Epochs	Execution time (s)	Training Loss	Training Accuracy	Validation Loss	Validation Accuracy
1	2	1.018	0.566	0.339	0.7614
2	14	0.649	0.639	0.5196	0.8910
3	15	0.399	0.8715	0.3903	0.8846
4	14	0.316	0.8896	0.304	0.8974
5	14	0.2442	0.8896	0.277	0.9103
6	13	0.2006	0.9317	0.2935	0.9103
7	14	0.1674	0.9398	0.479	0.8654
8	14	0.2317	0.9197	0.228	0.9295
9	13	0.129	0.9458	0.2357	0.9487
10	13	0.1016	0.9639	0.1936	**1.0004**

6.4 GAN and CGAN model

From the Table, it is clearly explained that GAN and CGAN model has been evaluated for identifying the fake signature and undergoes classification of fake and genuine signs. Based on number of epochs, the images are trained using neural network in which the features are trained thereby losses and accuracy are evaluated. Less losses achieved as 0.26 in GAN model whereas 0.66 which greater than CGAN. Moreover execution time, D-loss and validation accuracy are evaluated listed in Table 7.

Table 7: II Validation on GAN and CGAN approaches

Epochs	Execution time (ms)		D Loss		Validation Accuracy		G Loss	
	GAN	CGAN	GAN	CGAN	GAN	CGAN	GAN	CGAN
1	155	186	0.8198	0.6972	26.56	10.94	0.7085	0.6906
2	**58**	**72**	**0.3622**	**0.4297**	57.81	50.00	0.5472	0.6870
3	**58**	**62**	0.3727	0.3709	56.25	60.94	0.4398	0.6834
4	59	99	0.4146	0.3548	57.81	73.44	0.3686	0.6812
5	97	60	0.4673	0.3490	53.12	73.44	0.3090	0.6753
6	105	63	0.6025	0.3413	50.00	79.69	**0.2634**	**0.6659**
7	71	62	0.5823	0.3340	57.81	76.56	0.3225	0.6432
8	60	59	0.6461	0.3285	56.25	71.88	0.3561	0.6565
9	71	62	0.6522	0.3062	57.81	79.69	0.4041	0.6713
10	62	61	0.6406	0.3093	**65.62**	**82.81**	0.5795	0.6509

The Overall performance of various models are compared and evaluated are discussed in Table 8 and Figure in terms of precision, F1-score and accuracy. Among four models, CNN attained greater accuracy of 100% whereas CGAN 20%, GAN 67% and ResNet50 80%.

Table 8: Performance Metrics Evaluation

Methods	Performance Metrics		
	Precision	F1 Score	Accuracy (%)
CGAN	0.33	0.33	20
GAN	0.66	0.66	66.6
ResNet50	1.00	0.8	80
CNN	1.00	1.00	100

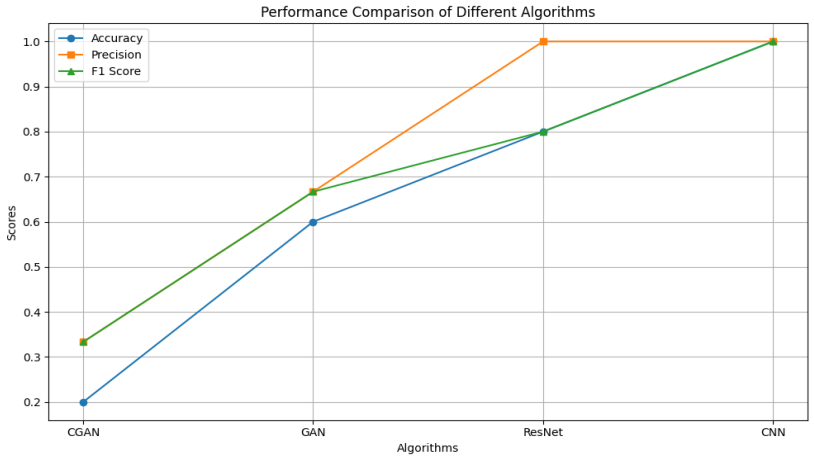


Figure 7: Performance comparison graph with precision, F1-score and Accuracy

Survey analysis of accuracy prediction using machine and deep learning techniques are discussed in Table 9.

Table 9: Survey analysis of Accuracy prediction

Authors	Techniques applied	Split: Train : Test	Accuracy
Eman Alajrami et al. [15]	CNN	80:20	99.7
		70:30	98
		60:40	97
Chinamay et al. [18]	Naïve Bayes	70:30	57%
	KNN	70:30	82
	Random Forest	70:30	81.5
Debasree et al. [19]	Feature detector HARRIS & SURF	-	-
Jameel et al. [14]	Deep based dynamic Time Wrapping	-	67.6
Jivesh et al. [23]	CNN + Crest Trough + SURF algorithm	70:30	94
Jose et al. [5]	Deep CNN based AlexNet framework	-	85
Padmajadevi et al. [21]	Neural Network	80:20	97.61%
Shalaw et al. [22]	Convolutional Siamese Network	Fix Threshold as 0.2	84%
Xinyu Lei et al. [24]	Dilated CNN	Train the images repeatedly by varying batch size and epochs	92%

CONCLUSION

In summary, the implementation of online digital signature verification among students is beneficial for the privacy of educational circumstances, effectiveness in administration, and academic reliability. It offers a dependable method for confirming the legitimacy and consistency of electronic records, improving adherence with confidence in learning environments. The authors employed deep CNN model, ResNet 50, GAN and CGAN model for identifying digital signature authentication among students which makes the documents such as official university correspondence, loan correspondence, entry in mentor book, etc secure and most effective. Among such deep models, Convolutional Neural Network provides effective outcomes evaluated in terms of validation accuracy, precision and Recall as 100%, moreover it produces least loss as 0.2 % execution time around 13 seconds for verifying University student's digital signature and classifying the signature into fake and real.

REFERENCES

[1] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometrics recognition using deep learning: a survey," Artificial Intelligence Review, 2023, doi: 10.1007/s10462-022-10237-x.

[2] Jahandad, S. M. Sam, K. Kamardin, N. N. Amir Sjarif, and N. Mohamed, "Offline signature verification using deep learning convolutional Neural network (CNN) architectures GoogLeNet inception-v1 and inception-v3," Procedia Computer Science, vol. 161, pp. 475–483, 2019, doi: 10.1016/j.procs.2019.11.147.

[3] D. Menotti et al., "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection," IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 864–879, 2015, doi: 10.1109/TIFS.2015.2398817.

[4] YINGYONG "SIGNATURE VERIFICATION USING GLOBAL AND GRID FEATURES", Pattern Recognition , Vol. 27, No. 12, pp. 1621 1629, 1994
[5] J. A. P. Lopes, B. Baptista, N. Lavado, and M. Mendes, “Offline Handwritten Signature Verification Using Deep Neural Networks,” Energies, vol. 15, no. 20, pp. 1–15, 2022, doi: 10.3390/en15207611.
[6] T. O. Oladele, K. S. Adewole, and A. O. Oyelami, “Forged Signature Detection Using Artificial Neural Network,” African Journal of Computing & ICT, vol. 7, no. 3, pp. 11–20, 2014.
[7] Ananthi Sheshasaayee "Digital Signatures Security Using Cryptography for Industrial Applications", International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2017),
[8] S. X. and Y. Z. T. Yang, Y. Zhang, “Digital signature based on ISRSAC,” 2021, vol. 18, no. 1.
[9] Hsin-Hsiung Kao and Che-Yen Wen " An Online Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach", Appl. Sci. 2020, 10, 3716, Pp: 1-15.
[10] Zainab Hashim " A Comparative Study among Handwritten Signature Verification Methods Using Machine Learning Techniques", Hindawi Scientific Programming Volume 2022, Article ID 8170424, 17 pages https://doi.org/10.1155/2022/8170424
[11] Ahmad Sanmorino, " A Survey for Handwritten Signature Verification", 2012 International Conference on Uncertainty Reasoning and Knowledge Engineering, 978-1-4673-1460-2/12, 2012 IEEE.
[12] M. Muzaffar Hameed " Machine Learning-based Online Signature Verification Systems: A Systematic Review",
[13] Shruti Jadon " An Overview of Deep Learning Architectures in Few-Shot Learning Domain", arXiv:2008.06365v3 [cs.CV] 19 Aug 2020
[14] JAMEEL MALIK " DeepAirSig: End-to-End Deep Learning Based In-Air Signature Verification", IEEE Access 2020, Digital Object Identifier 10.1109/ACCESS.2020.3033848
[15] Eman Alajrami1, Belal A. M. Ashqar et al. Handwritten Signature Verification using Deep Learning, International Journal of Academic Multidisciplinary Research (IJAMR),ISSN: 2643-9670, Vol. 3 Issue 12, December – 2019, Pages: 39-44
[16] Kiran Bibi, " Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities", Multimedia Tools and Applications, https://doi.org/10.1007/s11042-019-08022-0
[17] H. Srinivasan, S.N. Srihari, and M.J. Beal "Machine Learning for Signature verification", ICVGIP 2006, LNCS 4338, pp. 761–775, 2006.
[18] Chinmay Lokare "Offline handwritten signature verification using various Machine Learning Algorithms", ITM Web of Conferences 40, 03010 (2021) ICACC-2021, https://doi.org/10.1051/itmconf/20214003010
[19] Debasree Mitra, Aurjyama Baksi, Alivia Modak, Arunima Das, Ankita Das " Machine Learning Approach for Signature Recognition by HARRIS and SURF Features Detector", International Journal of Computer Sciences and Engineering, Volume 7, Issue 5, 2019.
[20] S. B. S. and R. S. B. Sadkhan, “Analysis of Different Types of Digital Signature,” in 8th International Engineering Conference on Sustainable Technology and Development (IEC), Erbil, Iraq, 2022, pp. 241–246.
[21] Padmajadevi G, Dr. Aprameya K.S, " Offline Signature Verification & Recognition Using Angle Based Feature Extraction & Neural Network Classifier", International Journal of Electronics Engineering Research. ISSN 0975-6450 Volume 9, Number 5 (2017) pp. 711-725
[22] Shalaw Mshir, Mehmet Kaya "Signature Recognition Using Machine Learning", 978-1-7281-6939-2/20/$31.00 ©2020 IEEE
[23] J. Poddar, V. Parikh, and S. K. Bharti, “Offline Signature Recognition and Forgery Detection using Deep Learning,” Procedia Computer Science, vol. 170, no. 2019, pp. 610–617, 2020, doi: 10.1016/j.procs.2020.03.133.
[24] XinYu Lei, Hong Guang Pan "A Dilated CNN Model for Image Classification", Voulme 7, 2019, IEEE Access
[25] https://drive.google.com/drive/folders/15w4y0BD8RNJJf7Bq2Vik-5EpoUzMw8 B?usp=drive_link
[26] Craig Rodarmel and Jie Shan "Principal Component Analysis for Hyperspectral Image Classification" Vol. 62, No. 2, Surveying and Land Information Systems · January 2002
[27] M. A. Hall, Correlation-based feature selection for machine learning, Ph.D. thesis, The University of Waikato (1999).
[28] M. Dash, H. Liu, Consistency-based search in feature selection, Artificial Intelligence 151 (1) (2003) 155–176.

[29] K.Baskar, D. Seshathiri, “A Survey on Feature Selection Techniques in Medical Image Processing”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 NCICCT' 14 Conference Proceedings.

[30] He K,ZX,RS,SJ. Deep residual learning for image recognition. In in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition; 2016. p. 770– 778.

[31] Z. Zhang, X. Liu, and Y. Cui, “Multi-phase offline signature verification system using deep convolutional generative adversarial networks,” Proceedings - 2016 9th International Symposium on Computational Intelligence and Design, ISCID 2016, vol. 2, pp. 103–107, 2016, doi: 10.1109/ISCID.2016.2033.

[32] M. Ranga Swamy, “Online Signature Authentication using Pre-trained Optimization Techniques ”, Int J Intell Syst Appl Eng, vol. 12, no. 3, pp. 3928 –, Mar. 2024.

[33] M Ranga swamy,, P, Vijayalakshmi, Rajendran, V, "Deep learning approaches for online signature authentication: a comparative study of pre-trained CNN models", Eng. Res. Express 7 01523, 2025