



# **iJRASET**

International Journal For Research in  
Applied Science and Engineering Technology



---

# **INTERNATIONAL JOURNAL FOR RESEARCH**

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

---

**Volume: 11    Issue: XI    Month of publication: November 2023**

**DOI: <https://doi.org/10.22214/ijraset.2023.56879>**

**[www.ijraset.com](http://www.ijraset.com)**

**Call:  08813907089**

**E-mail ID: [ijraset@gmail.com](mailto:ijraset@gmail.com)**

# Forgery Detection on Handwritten Signatures using Convolutional Neural Networks

Anshika Pradhan

Vellore Institute of Technology

**Abstract:** *Handwritten signatures play a significant part in numerous parts of our day-to-day events and aid in authenticating our personal information all over the world from banks to many government and private institutions. On the other hand, the usage of these handwritten signatures is accompanied by the problems of signature replication, counterfeit signatures and identity theft by both professional and amateur people alike. And so, there is a need for a system to help in differentiating and isolating the real signatures from their copied lookalikes but this task turns out to be really challenging. In recent years, there have been lots of advances in the field of Deep Learning, which is increasingly becoming a part of daily lives. One such deep learning technique called Convolutional Neural Networks, is an interesting tool for analysing pictures and other types of data. This method could be applied to detect and analyse handwritten signatures taken as inputs in order to classify if it is original or forged.*

**Keywords:** *Convolutional Neural Networks, Handwritten Signatures, Forgery Detection*

## I. INTRODUCTION

Handwritten signatures are a non-invasive broadly acknowledged biometric methodology which have been generally used to check the authority over documents [1]. Signature identification and signature verification are two principal issues identified with handwritten signatures. On account of authorization, the process comprises figuring out who is the endorser of a report. On account of authentication, the issue comprises deciding the level of likeness between a test signature and a model signature to choose whether or not this test signature is genuine or a fabrication. One of the key challenges in the two processes is the intrapersonal and relational differences when signing, as the signatures from the same author present varieties because of the accessible space for signing, the kind of pen utilized, the psychological and physiological state of the person signing, and other conditions [2].

In the domain of image forgery detection, there are two classes of picture forgery detection techniques [3], active forgery detection approaches and passive forgery detection methods. In the active picture forgery detection algorithms, a counterfeit is distinguished based on earlier accessible data in the input image, for example, watermarking or digital signature. This additional data may be embedded at the hour of picture procurement or at a later stage utilizing an appropriate instrument. Actually, the passive picture forgery location procedures don't need any sort of earlier data about the input picture to recognize the picture forgery; rather these methods distinguish falsification based on the influences in the intrinsic features of the picture that may have been presented during the manipulation cycle of the picture. The pictures downloaded from the Internet have no prior data, subsequently the active forgery detection procedures are of no use for such sort of forged pictures. Therefore, it is likewise evident that the passive falsification detection methods are similarly more practical today. There are four primary classes of passive fabrication detection methods: copy-move forgery detection, image-splicing forgery detection, re-contacting identification and re-sampling forgery detection procedures. A system to detect forgery in handwritten signatures is essential in order to keep identity falsification cases from taking place in banks and numerous different organizations. Otherwise, there would be tremendous loss of valuable property and information. This would prove to be useful for institutions such as banks that systematically require customer's handwritten signatures to validate their identity. The scope of handwritten forgery detection software is to identify and isolate genuine signatures from their forged counterparts. This can be achieved with the support of a system trained using machine learning and deep learning techniques which constitutes Convolutional Neural Networks (CNNs), which is a part of a concept known as Neural Networks. This system would make it easier to work on resources in order to build and analyze when compared with other systems like ANNs or RNNs.

## II. LITERATURE SURVEY

Several research studies have addressed forgery detection of handwritten signatures over the last five years but so far, the most predominant methods include, copy-move forgery, which is defined as the is the control of a picture's details by reordering starting with one locale then onto the next area inside a same picture, and other forgery detection techniques such as splicing, compression etc.

#### A. Copy-move Forgery Detection Techniques

The Copy-move forgery has had several innovative methods for its detection in the past five years. One detection technique based on tetrolet transform [1] proposes a new copy-move image forgery detection technique based on Tetrolet transform. In this technique, initially the input image is divided into overlapping blocks, then four low-pass coefficients and twelve high-pass coefficients are extracted from each block by applying a Tetrolet transform. Feature vectors are then sorted lexicographically, and similar blocks are identified by matching the extracted Tetrolet features.

- 1) Initially, the input image to be checked for forgery, is converted into grayscale image if it is not in grayscale.
- 2) In order to apply the Tetrolet transform on block level, the obtained grayscale image is decomposed into overlapping blocks of size  $4 \times 4$  pixels.
- 3) For each block, Tetrolet transform is applied and 4 low-pass and 12 high-pass coefficients are calculated.
- 4) The blocks of duplicated regions show some sort of similarities even though the tampered image has undergone post-processing operations. Obtained feature vector matrix Z is lexicographically sorted in order to arrange all rows in lexicographic order.
- 5) Then the method employs rotation invariant and time efficient, approximate nearest-neighbor searching based outliers filtering technique.

6) Finally, for locating the forged areas in an image, a binary map with all elements as zero and with size equal to input image is created. Then the binary map is utilized to create a colored forgery map by overlaying it on the input RGB image.

This technique can detect and locate the duplicated regions in the images very accurately, even when the copied regions have undergone some post processing operations blurring, color reduction, adjustment of brightness and contrast, rotation, scaling, JPEG compression. Also it is able to detect very small duplicated regions and multiple forgery cases, even when the image is smooth.

This technique cannot detect the copy-move forgery in noisy and distorted forged images.

Another copy-move forgery method [2] describes a new robust algorithm to detect copy-move forgery based on Speeded Up Robust Feature (SURF) descriptor, Approximate Nearest Neighbor (ANN) as a feature matching, Simple Linear Iterative Clustering (SLIC) used as a clustering algorithm to divide the whole image into superpixel blocks. The doubted regions are determined by replacing the matched feature points with corresponding superpixel blocks then the neighboring blocks have been merged based on similar Local Color Features (LCF). Finally, morphological close operation applied to elicit the doubted forged regions.

Evaluation was done based on values of Accuracy and the dataset used were CoMoFoD, MICC-F2000, MICCF220, and MICC-F600. The highlights of this approach are: This schema provides a new feature of producing forged MRs more wider than original MRs, so investigators can detect forged regions from original ones from the first look.

The drawbacks of this method are as follows, Detection accuracy needs does not cover more complex and hard copy-move forgeries. This method does not extend to cover other forgeries forms.

A novel approach [3] based on Automatic Threshold Estimation was later introduced. The proposed method is based on automatic estimation of the clustering threshold. The cutoff threshold of hierarchical clustering is estimated automatically based on clustering evaluation measures. The proposed method detects copy move forgery based on SIFT features and agglomerative hierarchical clustering.

- 1) In this detection scheme, the image is first preprocessed.
- 2) Then, features are extracted using SIFT. Distinctive SIFT keypoints are then matched between each other using a fast approximate nearest neighbor method.
- 3) After that, hierarchical clustering is applied on the matched points. Finally, the image is filtered, and tampered regions are localized.

The advantages of this approach is that this method yields higher precision and recall, and lower false negative values compared to alternative similar works. However This method cannot handle some types of image forgery like image splicing.

Copy-move forgery can be classified into keypoint-based and block-based methods. This paper [4] collated a lot of different types of keypoint based copy-forgery techniques and compared their stats and uses a custom built dataset from 15 older papers. The usual methods i.e. accuracy, true positive rates etc. are used for performance analysis.

An Iterative Copy-Move Forgery Detection [5] based on a new Interest Point Detector was introduced that proposed a new interest point detector specifically designed for CMFD. In this new scheme, the entire image, even low contrast regions, is covered adaptively based on a distinctiveness metric. The interest point density can also be automatically adjusted over the image in order to concentrate more on the suspected regions. Finally, an appropriate descriptor is employed for the detected interest points. In the rest of this section, the details of our contributions are portrayed. First of all, interest points are detected and then described using Polar



Cosine Transform. After that, an improved version of the adaptive matching is utilized. Next, falsely matched pairs are discarded by an effective filtering algorithm. In order to enhance the result, the whole process can be iterated regarding the prior information. The pros of this method are that: 1) It has a very effective filtering stage, 2.) This system has a great accuracy 3.) And it is better than 60% of the models compared to for accuracy.

The drawback is that the dataset used is relatively small, so results could be inaccurate.

A hybrid between keypoint-based and block-based copy-move forgery [6] that had the plan in which an image is first adaptively divided into non-overlapped regions, using simple linear iterative clustering (SLIC) algorithm. Then, SIFT is used to detect keypoints in the whole image, and based on whether the ratio of keypoints' number to the pixels' number is less than a threshold, a region is classified as a smooth region or keypoints region. Afterwards, a multiple keypoints matching procedure is performed in keypoints regions to decide candidate forgery regions, and RANSAC is used to prune outliers. Finally, if there are more than two smooth regions in the image, Zernike moments are used as block features to detect forgery in smooth regions. Upon testing on a database constructed which consists of 48 high-resolution base images. 4 images from MICC-F220 and 4 images from CoMoFoD good level of precision was obtained which was the second highest level of recall from the 5 other methods compared. However the level of precision isn't as good as some methods like SURF or SIFT.

A novel technique [7] derived from scaled ORB describes the four main steps involved: identify the pyramid scale space, extract scaled ORB feature, match the feature and remove the false matching. This methodology was tested on 214 images. The real images come from Columbia University natural images library and Internet. To assess the performance of a copy-move forgery detection method, true positive rate (TPR) and false positive rate (FPR) criteria are used, where TPR is the fraction of tampered images correctly identified as such, while FPR is the fraction of original images that are not correctly identified. The benefits of this way is that it takes less time for both feature extraction and feature matching compared to the SIFT and SURF algorithms and the proposed algorithm is very robust against images with noise. The limitation is that the SIFT algorithm has less false matches.

In [67] this review a few specific techniques which includes an Active/ intrusive/non-blind method and a passive/ non-intrusive/ blind method. Passive technology for image forensics is a new research area. Unlike the signature-based and watermark-based methods, the new method is blind without extra side information in detection. The inherent pattern of the image can be served as a non-intrusive watermark for source identification and alteration detection. Therefore pattern selection is crucial in this technology. Although some of the existing methods succeed in reaching a relatively high accuracy, the proposed methods in the survey carried out exhibits limitations and drawbacks which have to be improved. The passive method in collaboration with the active approach may play an important role in the field of image forensics.

Another [15] demonstrates an Open Handwritten Signature Identification System (OHSIS) for offline handwritten signature identification by using conjointly the Curvelet Transform (CT) and the One-Class classifier based on Principal Component Analysis (OCPA). The datasets used are "Grupo de Procesado Digital de Senales" (GPDS) signature dataset and the Center of Excellence for Document Analysis and Recognition (CEDAR) signature dataset. Binarization of acquired signature is done as a pre-processing method. CT is explored for feature generation due to its efficient characterization of curves contained into the local orientations within the signature image. While OC-PCA is used for its effectiveness to absorb the high feature size generated by the CT and allows achieving at the same time an open system new combination approach based on Choquet fuzzy integral is proposed to combine multiple individual OHSISs in order to improve the robustness of the OHSIS. Evaluation is done on the basis of Identification rate which is the number of instances correctly identified to the total number of instances in percentage. The proposed combination of methods is able to cope with a restricted number of writers and reference signatures to design an efficient and parameter independent OHSIS, offers a better improvement and stability for extending new writers. However, this does not take dissimilarity into consideration. The dissimilarity learning approach using OCC ensemble to generate a generic and writer independent handwritten signature identification system can be built in future.

The proposed technique [20] uses digital signatures embedded in the least significant bits of the selected pixels of each row and column. The process maintains a symmetry in the use of pixels for computing and hiding the digital signatures. The pixels in each row and column of an image are divided into two groups. One group contains pixels of a row or column used in the calculation of digital signatures, and the second group of pixels is used for embedding the digital signatures of the respective row or column. The digital signatures are computed using the hash algorithm, e.g., message digest five (MD5) using greyscale Lena Image after modifying its pixels. The proposed technique divides the pixels of each row and column into two parts. One group of pixels is used in the computation of the digital signature, while the second group of pixels is used for embedding the digital signatures. To authenticate image contents and detect any possible modification introduced to the image, the digital signature for each row and column is computed similarly by using the selected pixels. The embedded digital signatures are retrieved from the LSBs of the

selected pixels used for embedding. The digital signatures are computed using the MD5 algorithm and are embedded in LSBs of selected pixels using the LSB substitution method. As each pixel is a part of a row and a column, if a pixel is modified, the corresponding rows and columns will be labeled as unauthentic. Therefore, the forged pixel is located at the point of intersection of the forged row and column. True Positive (TP), True Negative (TN) and accuracy are evaluated for proposed model. The algorithm is capable of detecting rows' or columns' truncation. The technique detects pixel level modification in a single or multiple pixels. 1) This method would mark the complete image as forged if the part of pixels having embedded signatures was modified. This would possibly mark a lossy compressed image as a forged image, e.g., in the case of JPEG compression.

Another novel approach used in [22] consists of three steps. First, an image is partitioned into blocks of size  $16 \times 16$ . Second, image features are extracted from each block using steerable pyramid and SVD transforms. Finally, the extracted features are sorted lexicographically and matched using the KS test. CoMoFoD database is used for this purpose. In the proposed method, an image is partitioned into blocks of size  $16 \times 16$  using a  $16 \times 16$  sliding window which is shifted by one pixel per step. This results in 246, 016 blocks for an image of size  $512 \times 512$ . SVD is applied to each  $2 \times 2$  sub-block to extract a single singular value which is the corresponding feature. The feature vectors are sorted lexicographically so that similar vectors are close which simplifies the search process. The KS test is applied to the sorted feature vectors. Applying the KS test to the corresponding feature vectors may increase the false positive rate. To avoid this problem, a minimum distance between pixels is employed. Accuracy, Precision, Recall and F1 score are used to evaluate the model. The proposed method can detect forgeries at a pixel level and has a minimal false positive rate of less than 4%. This method has a longer computation time compared to other methods.

In this paper [23], a forgery detection technique is proposed which exploits the artifacts originated due to manipulations performed on JPEG encoded images. In JPEG compression technique, an image is divided into non-overlapping blocks of size  $8 \times 8$  pixels and discrete cosine transform (DCT) coefficients are evaluated for each block independently. When a JPEG compressed image is tampered, there is a change in the statistical properties of AC components of block DCT coefficients. To capture this change, they propose to use standard deviation and count of non-zero DCT coefficients corresponding to each of the AC frequency components independently. The images are cropped by removing a few rows and columns from the top left corner and suggested features are evaluated for test image and its cropped version. The extracted feature vector is used with the support vector machine (SVM) for the classification of authentic and forged images. CASIA v1.0 and v2.0 are used as datasets. The steps involved in the algorithm are the key idea is to exploit the variation in statistical properties of AC coefficients of the entire image by computing standard deviation and count of non-zero DCT coefficients corresponding to each AC frequency component independently. The suggested features are evaluated for the test image and its cropped version. The extracted feature vector is then used with the SVM classifier for identifying the modified/unmodified images. The proposed scheme is experimented with various pre- and post-processed forged images available in the CASIA dataset. Receiver Operating Characteristic (ROC) curve and accuracy are performance measures used. This method can deal with splicing as well as copy move forgery at the same time. The proposed method is consistent and can deal correctly with any kind of manipulation. However, there is a decline in accuracy during pre-processing operations when compared with the results of accuracy for post-processing operations.

Another approach [27] proposes a differential excitation component (DEC) of Weber Law descriptor in combination with the gray level co-occurrence matrix (GLCM) approach of texture feature extraction for CMFD. GLCM Texture features are computed in four directions on DEC and this acts as a feature vector for support vector machine classifiers. These texture features are more distinguishable and it is validated through other two proposed methods based on discrete wavelet transform-GLCM (DWT-GLCM) and GLCM using CoMoFoD and CASI datasets. Features are extracted for all the original and forged images in the database. An SVM is trained with these feature vectors and a model is developed. This SVM model is used for classification. Convert each color image to gray image. Perform CMFD using GLCM features, DWT-GLCM features, DEC- GLCM features. Train SVM Model using polynomial kernel. Test the trained SVM model to identify the image as original or forged. Accuracy, sensitivity and specificity are taken as performance measures. The proposed methods work with a 24-dimension feature vector, exhibits resilience against post-processing attacks and is computationally effective, however it concentrates only on the detection of forged images, it doesn't consider localization of forged images.

This paper [55] collated a lot of different types of keypoint based copy-forgery techniques and compared their performance in various categories: method used for feature extraction, strategy for feature matching, pre-processing method, detection region/s, block pattern and accuracy/recall. This paper was a large scale project made to compare and evaluate a lot of different methods that were published around that time. A lot of future papers used this paper to base what algorithm/methodology to work on next to see if any improvement was possible.

Another author [56] proposed a new form of copy-move forgery detection using their “New Interest Point Detector”. They proposed a new interest point detector specifically designed for CMFD. In this new scheme, the entire image, even low contrast regions, is covered adaptively based on a distinctiveness metric. The interest point density can also be automatically adjusted over the image in order to concentrate more on the suspected regions. Finally, an appropriate descriptor is employed for the detected interest points. Interest points are detected and then described using Polar Cosine Transform. After that, an improved version of the adaptive matching is utilized. Next, falsely matched pairs are discarded by an effective filtering algorithm. In order to enhance the result, the whole process can be iterated regarding the prior information. Image Manipulation Dataset (IMD) was used to train the model. Effectiveness of filtering stage and comparison of detection results were used as performance metrics. The method has a very effective filtering stage, coupled with great accuracy and is better than 60% of the models compared to for accuracy.

This novel methodology [57] uses a completely different approach. The image is first adaptively divided into non-overlapped regions, using simple linear iterative clustering (SLIC) algorithm. Then, SIFT is used to detect keypoints in the whole image, and based on whether the ratio of keypoints' number to the pixels' number is less than a threshold, a region is classified as a smooth region or keypoints region. Afterwards, a multiple keypoints matching procedure is performed in keypoints regions to decide candidate forgery regions, and RANSAC is used to prune outliers. Finally, if there are more than two smooth regions in the image, Zernike moments are used as block features to detect forgery in smooth regions. The database consists of 48 high-resolution base images. 4 images from MICC-F220 and 4 images from CoMoFoD\_small\_v2 database. The metrics measured were precision, recall and F1. A good level of precision was measured and the second highest level of recall from the 5 other methods compared to. However, the level of precision isn't as good as SURF or SIFT.

Copy-move forgery detection based on scaled ORB was implemented [58]. There are four main steps in the proposed method: identify the pyramid scale space, extract scaled ORB feature, match the feature and remove the false matching. They used a dataset containing 214 images (107 real images and their corresponding tampered images). The real images come from Columbia University natural images library and Internet. To assess the performance of the copy-move forgery detection method, true positive rate (TPR) and false positive rate (FPR) criteria are used, where TPR is the fraction of tampered images correctly identified as such, while FPR is the fraction of original images that are not correctly identified. The proposed method takes less time for both feature extraction and feature matching compared to the SIFT and SURF algorithms. The proposed algorithm is also very robust against images with noise.

## B. Deep Learning Based Algorithms

### 1) Convolutional Neural Networks Based Techniques

This paper [8] implements CNN supervision for forgery detection in compressed pictures. The main aim is to provide a robust and effective framework for camera model identification (CMI) and image forgery detection. They have used a camera identification model based on convolutional neural networks. Their trained CNN is then fed with a mixture of different qualities of compressed and uncompressed images. approaches. In order to better interpret our trained CNN, they have proposed an in-depth supervision by first a visualization of the layer and an experimental analysis of the influence of the learned features. The performance measures used were 1) Accuracy, 2) Receiver operating characteristic (ROC) curves and 3) Area Under the ROC Curve (AUC) on the Dresden dataset.

The merits of this approach are: This method results in a robust and accurate framework for Forgery Detection. Using CNN the system is capable of learning classification features directly from image data.

The only let-down is that this framework has a low test performance (around 40%). Therefore it can only be dedicated to a very specific task and can not be used for other applications.

This paper [9] discussed a method for Forgery Numeral Handwriting Detection using CNN. This paper proposes a method for handwritten forged numeral detection based on convolutional neural networks. They focus on the research of forged numeral detection based on convolutional neural networks, establish a database of handwritten forged numeral samples, and optimize the AlexNet under the Caffe framework in order to promote the application of convolutional neural network in document forgery detection and improve the level of forensic document identification. The dataset was created by allowing 50 volunteers who were recruited to write samples with different pens; 2 samples of each type of handwriting for each combination, and obtain a total of 7,200 samples.

The main plus point of this method is that it solves the problems of relying on the experience and knowledge of the appraisers in the forensic documents identification which is time-consuming and labor-intensive.

The drawback is that this paper only involves the study of adding strokes to a handwriting image under a single background. In actual cases, there is a situation of complex writing background.

Another method of tampering is called Image slicing. This paper [10] proposed a method Image Splicing Forgery Detection Combining Coarse to Refined Convolutional Neural Network and Adaptive Clustering. In the proposed model the differences in the image are found by cascading a coarse CNN and refined CNN (C-CNN and R-CNN respectively). The cascading results in making scales where the image has been tampered finding difference in their properties. The computational complexity of the whole model is reduced by an image-level CNN rather than using a patch level CNN into C2RNet. Since the difference in properties is compared therefore it results in stabilised results. Furthermore, after a preliminary detection of the forged regions by the CNN adaptive clustering is performed to detect the forged regions. The differences in the image are found by cascading a coarse CNN and refined CNN (C-CNN and R-CNN respectively). CNN adaptive clustering is performed to detect the forged regions. The main advantage of this approach is that the proposed method produces better results than the already existent splicing techniques for forgery detection even in conditions of attack. The limitation is that the size of these datasets restricts training and hence optimal results are not yet obtained from this proposed model.

This paper [12] proposes new deep learning techniques, namely Directed Acyclic Graph -Convolutional Neural Network (DAG-CNN) is used for handwritten character recognition. A custom dataset was used for this purpose. Various handwritten cursive alphabets are collected and a dataset is created. The various modules of the system are data acquisition, dataset augmentation, partitioning of training and testing data, pre-processing, model building and training, finally classifying and predicting output. The model is finally passed to softmax module for classification and accuracy prediction. The major advantage of this method is we can use the low, middle and high level features for classification, enabling a holistic consideration of all features. However, preprocessing of images if not done properly can lead to inaccurate results.

This research [14] proposes a handwritten signature verification and recognition using Artificial Neural Network and contour-based features. The dataset included 5600 genuine and 5600 forged offline signatures. This method makes use of two steps, first is Data acquisition and processing and second being Feature extraction and representation. Offline signatures are captured using devices such as scanner and camera and online signatures take acceleration, speed, etc. into account. Feature-based extraction is carried out using the Canny algorithm by applying Gaussian filter and non-suppression techniques. On identification of the contour, it is passed through ANN classifier. The parameters used for evaluation are False Rejection Rate and False Acceptance Rate. FRR and FAR obtained are low comparatively to related methods. Choosing the features appropriately, showing signatures through these features and using these to find a match between the training and test dataset.

Another paper [16] proposes a framework which has mainly three parts: the sample generation (random distortion), CNN models and voting. The datasets worked upon were CASIA and MNIST. Sample generation: since the training of CNN requires a large number of training samples, the sample generation is important to provide enough samples to fully train the CNN model. The sample generation is realized by two different types of random distortion: the local distortion and global distortion. The network structure of the CNN models is designed according to the properties of handwritten characters and several training tricks are also employed for better training. Multiple trained CNN models are used to vote for the final recognition result. The voting can significantly improve the recognition rate which was used as the performance measure. But there is scope of improvement as better sample generation methods, training scheme and network structure of CNN can be added.

In this paper [18], the author proposes a first its of kind of attempt in which an intelligent framework tries to learn the online signatures of a writer using Deep Generative Adversarial Networks (DGANs). Thorough experimental analysis on three widely used datasets MCYT-100, SVC, SUSIG confirms the supremacy of the method and boost confidence in real time deployment of our framework in data centric applications like offline signature verification, forged document detection, etc. Three widely used datasets in this method are MCYT-100, SVC, SUSIG. True Acceptance Rate (TAR), i.e. classification accuracy of real signature samples. False Rejection Rate (FRR), i.e. classification accuracy of fake signature samples are the performance measures taken. OSV model is proposed to address the data scarcity problem of online signature verification, We have evaluated the proposed model, our proposed model achieved best results compared to the current state of the art models. Major advantage of this method is it tries to outspread the proposed model by evaluating it with additional datasets and all possible categories of experimentation.

The paper[21] discusses an offline handwritten signature verification method based on an explainable deep learning method (deep convolutional neural network, DCNN) and unique local feature extraction approach. They use the open-source dataset, Document Analysis and Recognition (ICDAR) 2011 SigComp, to train our system and verify a questioned signature as genuine or a forgery. ICDAR 2011 SigComp dataset is used for training and testing. First, convert image into grayscale image.



Divide into Sub-image blocks by setting a window as a sliding mask to get a sub-image block from the original image. Reduce background texture by brightening the sub-image by 7.5%, and the method is to multiply each RGB pixel values by 1.075 directly. Rotate sub-image blocks and repeat the process until a full 360 degrees rotation is done. Classify valid and invalid samples. CNN system focuses on the rotation-invariant features and reduces the unnecessary influence from different handwriting angles. Accuracy and False Rejection Rate (FRR) are taken as performance measures. This method is currently used to solve binary classification problems. Under conditions of small sample size, there is a relatively low accuracy rate.

The first two approaches mentioned in the paper[24] are “on-demand” generators and they can be used during the training stage to produce a potentially infinite number of synthetic signatures. In their approach, they have initially trained Siamese Neural Networks using signatures from GAVAB dataset and different combinations of synthetic data. GAVAB for training and preliminary tests and GDPS Synthetic (training), MCYT75, SigComp11, CEDAR are the datasets used. The algorithm includes preprocessing the signature image dataset, partitioning the samples into disjoint training, validation and test subsets, Generating the signature pairs using four different schemes to produce samples (Original GAVAB training set, augmented GAVAB training set, their proposed synthetic signatures and GPDS Synthetic dataset), training the model using a Siamese Neural Network and testing the trained model. 1) Area under the ROC (Receiver operating characteristic) Curve and Equal Error Rate (EER) are taken as the evaluation measures. This method works best when the test sample includes a combination of original signatures, augmented signatures and synthetic signatures. The Equal Error Rate (EER) is low for varied datasets.1) This method doesn't perform well for original or data augmented signatures when compared to synthetic signatures.

Another work [26] presents an approach for copy-move forgery detection based on block processing and feature extraction from the transforms of the blocks. In addition, a Convolutional Neural Network (CNN) is used for forgery detection. The feature extraction is implemented with serial pairs of convolution and pooling layers, and then classification between the original and tampered images is performed with and without transforms. A comparison study between different trigonometric transforms in 1D and 2D is presented for detecting the tampered parts in the image using MICC-F220 dataset.1) The proposed forgery detection algorithm depends on three phases: the pre-processing phase, the feature extraction phase, and the classification phase. In the data pre-processing phase, a trigonometric transform is carried out on the input images, and then they are resized to a unified size specified in the input layer. The feature extraction stage consists of a set of layers that encloses neurons arranged in 4 dimensions: the number of samples, the width and height of the input image, as well as the number of filters used in each CNN layer.3) After these layers, a Global Average Pooling (GAP) layer exists, and after that the fully-connected layer. Finally, a dense layer deciding between two classes (original or tampered) is used for the classification phase. Completeness rate and Accuracy are used for evaluation. The main advantage of this detection algorithm is the small feature vector, where a block of size  $(8 \times 8)$  is represented by a  $1 \times 4$  feature vector. However, the Completion rate is relatively low when 2DDFT (2D Discrete Fourier Transform) is applied on each block.

This author [29] proposes to use recurrent neural networks (RNN) for representation learning in the dynamic time warping framework. An RNN variant-gated auto regressive units-is proposed and shows a better generalization performance in our framework. Furthermore, we interpret the online signature verification problem as a meta-learning problem: one client is considered as one task, therefore, different clients compose the task space using MCYT-100, Mobisig, and e-BioSign datasets. The selection criterion was skilled forgery EER .Metric-based loss functions were designed to explicitly minimize the intra-individual variability and enhance the inter-individual variability, and guide the RNN network in learning discriminative representations for online signatures. However, when there are no available skilled forgeries in the adaptation stage, it is currently unable to adapt the RANs model. Moreover the main formula used in the method works well in training, as it has no direct relationship with DTW. Further search needs to answer this question and improve the metric.

This author [30] proposes an end-to-end learning method based on statistical features extracted on set-of-samples level as a step toward solving the writer verification problem which is about deciding whether two handwriting sources are identical given handwriting samples from the two sources. The dataset come from cropped out word-level images from the CEDAR-LETTER database. Human engineered (GSC features) single sample features and automatically learned features using convolutional neural networks(CNN). Accuracy of the model is calculated to measure its performance. CNN feature extraction, when trained with data augmentation, performs better on “and” data than human-engineered features on both one-to-one and many-to-many comparisons but not necessarily so on the much smaller “th” dataset. The statistical features worked on sets of samples gives better result than K-S test based on distance space and end-to-end fine-tuning can improve a pretrained model's performance in some cases.

In this approach [33] the authors proposed a preprocessing way to make verification of signatures simpler. They proposed CNN, Crest-Trough algorithm based approach for Signature verification solution. The also implemented a Harris-Surf based model for forgery detection in signature.



The planned system was massively economical in finding and sleuthing the counterfeits at runtime and therefore the responsibility of the model can be improved by training the drawn features on the Artificial Neural Networks by saving the extracted features. Minor mis-classification or error is required in such sensitive applications.

This paper [34] deals with a hybrid method using CNN and LSTM where an time saving dimensionality reduction approach, to reduce the number of attributes is implemented and a state-of-the-art CNN-LSTM based hybrid system for online signature verification is proposed. The main advantage of the proposed model is that it achieves high accuracy and the proposed model is thoroughly tested on numerous datasets and satisfied its efficiency with lessened error rates.

Another method [35] proposes an online signature verification by long-term recurrent convolutional network (LRCN) which guarantees extracting distinguishable attributes between genuine and false signature. In this method, CNN and time interval embedding are applied for feature extraction of signature patterns and LSTM is used for modeling long-term temporal behaviours of stroke flow. In the comparisons with the other methods, this method outperformed other methods when considering both random forgery and skilled forgery.

This approach [39] investigates whether prototype selection (PS) preprocessing can be used in the space resulting from the dichotomy transformation without degrading the performance of the classifier. Furthermore, an investigation is also performed to examine the use of a WI classifier in a transfer learning scenario, i.e., where the classifier is trained in one dataset, and is used to verify signatures in other datasets. The experiments were carried out using the GPDS, BRAZIL- IAN, MCYT and CEDAR datasets. The performance evaluation of the classification methods is based on the Equal Error Rate (EER) metric, using user thresholds

The method proposed by the authors in this paper [41] uses two LSTM RNN networks to extract different features. The first one extracts the features of the strokes and the latter extracts the global features of the whole signatures. The results on the BiosecureID dataset demonstrate that the authors' proposed method can reduce the EER by 33.05%, from 5.6% to 3.75% with fewer features and less training samples. The BiosecureID [29], MCYT-100 [30], SCUT-MMSIG [31] and MOBISIG [32] datasets are used to verify the performance of the proposed network. In this paper, The Equal error rate (EER) is used to measure the accuracy of signature verification.

In this paper [42] the author proposes a framework which has mainly three parts: the sample generation (random distortion), CNN models and voting. Sample generation: since the training of CNN requires a large number of training samples, the sample generation is important to provide enough samples to fully train the CNN model. The sample generation is realized by two different types of random distortion: the local distortion and global distortion. •CNN models: the network structure of the CNN models is designed according to the properties of handwritten characters and several training tricks are also employed for better training. •Voting: multiple trained CNN models are used to vote for the final recognition result. The voting can significantly improve the recognition rate. The model performs beyond human performance on both MNIST and CASIA datasets. But Better sample generation methods, training scheme and network structure of CNN can be done

The approach used in paper [45] proposed signature verification system comprises the feature extraction using CNN and classification using SVM. The architecture of CNN consists of a number of layers such that each layer performs a simple computation starting at the raw image pixels and feeds the result to the next layer. The features are tapped from an experimentally selected layer. The database used is the GPDS960 which contains 960 signatures which vary significantly in shape ranging from small signatures of size 153x258 to large signatures of size 819x1137 pixels. We have 24 genuine signatures for each individual, plus 30 forgeries of his/her signature. The 24 genuine samples of each signer are collected in a single-day writing session.

A deep learning approach using a custom model [61]. They first converted the image into a YCrCb color space. Then segmented the image into 32 by 32 patches. Finally, they applied a 3 Level 2D Daubechies Wavelet decomposition to each YCrCb component of the patches. They then obtained the standard deviation, mean, and the sum for each of the approximation, horizontal, vertical and diagonal coefficients to obtain 90 features. In addition, they applied Daubechies orthogonal wavelets D2-D5 to obtain a total of 450 basic features. They manually labelled 1000 images randomly selected from the CASIA 1 and 2 databases. For the task of labelling the ground truth, they referred to their published instructions. In the first layer, features were learnt using a SAE with 3 hidden layers. Hence, the network's input is 450 dimensions and the number of neurons in the SAE's remaining layers are 500-256-128-2. At the second layer which integrates ontexual features, the average of the MLP values of the 3 half-overlapped neighbouring patches are further used to calculate the final prediction value. The accuracy is greater than other models. The proposed method also supports both jpeg and tiff images. However, overall accuracy for TIFF images is still only 80% which leaves a lot to be desired.

In this paper [66] the authors propose the combination of 'Faster RCNN with Caffee deep learning library and YOLOv2 which were considered for the experiments. The Caffee-based pre-trained models are publicly available for most of the object detectors. There are fewer numbers of document images in the dataset for a deep learning system to learn from scratch. Hence, in order to take full

advantage of network architectures, a transfer learning technique from ImageNet was used to fine-tune our models. The fine-tuning process helps our system to converge faster and perform better. Various network architectures such as ZF, VGG16 and VGG CNN M 1024 were used to train the system and evaluate the performance on the dataset.

This author [71] decided to experiment on having an intensive preprocessing component. The proposed method involves the following steps: Data Acquisition, Pre-processing, Noise Removal, Grayscale to Bitmap, Resizing, File Management, and then finally training the model. The dataset which has been used in this research work is a collection of 6000 signatures with 1000 genuine and 1000 forged signatures per subject. In this work the signature images are pre-processed in a batch by batch manner and split them into training and test sets based on a split ratio (which is chosen) This is done in Matlab, with functions from the image processing toolbox After these signatures preprocessed, it is stored in a file directory structure which the keras python library can work with Then the CNN has been implemented in python using the Kerswith the TensorFlow backend to learn the patterns associated with the signatures. Then the model derived has been verified using accuracy and loss metrics to see how well the model has fit the data. In the end result, the training and validation accuracy for each split is between 97% and 98% which is extremely high. However, the model does take a long time to train.

### C. Machine Learning based Algorithms

A novel method [11] examines that a signature verification is a popular way of performing biometric (i.e. using methods to identify a person through his individualities or traits) verification. With a booming area of interest and application such as banking , e-business etc. it has huge scope for research. This paper uses the idea of feature selection to carry out the task of signature verification of offline signatures. The datasets used in the model are CEDAR, MCYT and GPDS. There are 4 steps involved in the given process : namely pre-processing , feature extraction , feature selection and finally feature verification. The aspect ratio, a signature is, pure width and height, normalised signature height etc are few global features that are used for the given task. It also uses local features such as angle, slope, centroid and distance. Genetic algorithms are used in feature selection which then feeds them into a support vector machine (SVM) for the process of classification. The method was evaluated using FAR, FRR and AER accuracy measures. Results reveal improved performance of proposed work in comparison with existing approaches as far as average accuracy is concerned. However, incorrect image processing operations might lead to less reliable systems.

In this paper the author [13] proposes techniques for automatic signature verification which must be created to avoid forgeries. The forgeries in handwritten signatures have been categorized based on their characteristic features. The three major types of forgeries are: Random Forgery, Unskilled Forgery and Skilled Forgery. From the signature image, we use the Harris corner detection method to find an interesting point. Then orientation is assigned. For each key-point, we calculate the feature vector based on gradient features. A custom dataset was used. A number of signatures from 20 different persons. For each of the person 6 signatures are used, 5 of them are genuine and the rest one is forged. Out of those 5 genuine signatures only 3 are used for training the system. Online data tracks the motion of the stylus when the signature is produced, and includes location, and possibly velocity, acceleration and pen pressure, as a function of time. These characteristics are specific to each individual and are stable as well as repetitive for the individual. Off-line data is a 2-D image of the signature. For signature verification, a number of techniques are suggested. Some of the methods use global features which are calculated keeping in mind the whole image. Some of them use local features which are estimated based on some interest points but these methods are unable to ensure overcoming all the difficulties, especially when the same threshold is taken for different persons which often lead to error and affect accuracy. In this paper, the system suggests a statistical method that extracts features on the basis of local gradient values. From the signature image, we use the Harris corner detection method to find an interesting point. Then orientation is assigned. For each key-point, we calculate the feature vector based on gradient features. Accuracy( $N_s/N$ )e  $N_s$  is the number of correctly classified signatures and  $N$  is the total number of test cases is used as a performance measure. It works fine with any rotation of the training or test signature. It can learn from a comparatively lesser amount of training data thus making it suitable for usage in practical scenarios. Noise removal is necessary otherwise leads to inaccurate results.

This paper [19]proposes a method to compensate the lack of dynamic information from static signature images through the use of discrete Radon transform(DRT), principal component analysis(PCA) and probabilistic neural network(PNN). Dataset used is available offline consisting of handwritten signature database, which is the MYCT subset -a total of 2250 offline handwritten signature images, consisting of 15 genuine signatures and 15 skilled forgeries from 75 signers respectively. Probabilistic neural network (PNN) instead of similarity matching concept. A PNN has three layers –pattern layer which has one neuron for each input layer vectorin the trainingset, summation layer which has one neuron for each user class and an output layer which holds the maximum value of summation of neurons to produce the probability score.

Performance measures include Cosine angle distance, and the L1(Manhattan), L2(Euclidean) distance measures. High accuracy and speed of PNN was obtained. However, the method is not reliable. Future works include using a large database of signatures with forgeries and a powerful specification of PC support to obtain a more reliable system.

The paper[25] proposes a signature verification method based on circlet transform and the statistical properties of the circlet coefficients is presented. The datasets used are GPDS-synthetic, MCYT-75 and UTSig. A signature verification system includes three main steps: preprocessing, feature extraction, and classification. Some preprocessing tasks have been conducted including conversion of image into binary format using Otsu's algorithm. Feature extraction step has been conducted based on the circlet transform. The statistical properties of circlet coefficients have been computed using the Gray Level Co-occurrence Matrices (GLCM) of the circlet coefficients. Finally, in order to classify the signature images in the space of extracted feature vectors, two classifiers: Support Vector Machine (SVM) with Radial Basis Function (RBF) kernel and polynomial kernel, and k-Nearest Neighbor (k-NN) classifier have been considered. Performance measure used are False Rejection Rate (FRR), False Acceptance Rate (FAR) and Equal Error Rate (EER).<sup>1</sup> This method provides an effective use of circlet transform in signature verification system. The extracted features are rotation dependent, so the performance of the presented system can be relatively low if the signatures are not in the right angle.

Another author [28] proposed a feature that is called Local Difference Feature (LDF) is a LBP-like texture descriptor. LDF calculates differences between a central pixel and eight neighbors taken on a specific neighborhood radius. Differences are coded into binary thresholded values before evaluating the histogram of codes. The verification step is achieved by SVM classifier trained on genuine signatures. Furthermore, the test stage is performed on both genuine signatures and skilled forgeries conducted on GPDS and CEDAR datasets. Machine learning algorithms such as Local Difference Feature (LDF) and SVM classifier are used. False Acceptance Rate (FAR): It is the percentage of forgeries that are accepted as genuine by the system. False Rejection Rate (FRR) which is the percentage of genuine signatures that are considered as forgeries by the system and Average Error Rate (AER) which is the mean of FAR and FRR are taken as performance measures. Usage of LDF has two main advantages, it is simple to calculate, and second, it gives a feature vector with a small size. Therefore, it makes an interesting tradeoff between accuracy and feature size. Further tests can be done to evaluate the usefulness of the multi-scale computation for LDF.

This paper [30] uses Support Vector Machine logic for offline signature verification. A group of signature test cases are taken from individuals and these signature values are scanned in a grayscale format. These scanned signature pictures are then computed to a number of image enhancement tasks like complementation, binarization, filtering, trimming and edge detection. By these pre-processed signatures, attributes such as centroid, centre of force, calculation of amount of loops, horizontal and vertical profile and normalized area are taken out and stored in a database individually. The results from the database are put into the support vector machine which makes a hyperplane and categorizes the signature as original or fake based on a certain feature value.

A novel approach [31] that suggests that it is viable to verify handwritten signatures precisely by analyzing movement data obtained from hand-worn gadgets. This was initially a hypothesis based on the presumption that most persons adopt a specific signing design over the years that is distinct and very difficult for anyone else to copy, and this uniqueness can be recorded enough using the motion sensors of a hand-worn product. This technique had high accuracy and also worked extremely well provided one had the hardware needed to track the movement of hands.

In this approach [40] the authors have adopted a dynamic time warping (DTW) barycenter averaging to obtain an effective mean template while preserving intra-user variability between all references. Then, by using the mean template, the authors proceed to calculate multi-distance measures: The multiple DTW from each feature with independent warping and the single DTW from all features with dependent warping. To boost the discriminative power, the authors have applied a weighting scheme using gradient boosting to efficiently combine the multi-distance measures. The model performance is evaluated by EER. The experimental results confirm the effectiveness of the proposed method.

This author [59] decided to use an unsupervised learning method. In order to provide a mean for the representation of the reference signatures they re-entered a groundbreaking unsupervised learning method named archetypal analysis, which is connected to effective data analysis approaches such as sparse coding. Due to the fact that until recently there was no efficient implementation publicly available, archetypal analysis had only a few cases of use. Recently, a fast optimization scheme using an active set strategy was presented and an efficient open-source implementation interface has been also provided to facilitate computations. The CEDAR and MCYT75 signature datasets were used to train the model. During the first phase of the learning stage-enrollment, a population of Ngen-reference genuine signature samples is enrolled. Then, the union of the signature pixels of all reference images forms the matrix.



In the second phase of the learning stage, which includes training, for each of the genuine reference input signatures along with a number of random forgeries i.e. other writers genuine signatures, similar data matrices are formed, and analyzed into the corresponding matrices by keeping another matrix fixed while solving the equation. Average pooling across the rows of the A matrices creates the signature features with dimensionality proportional to the value of  $p$ . Next a binary SVM classifier is built with the genuine reference features as the positive class and the random forgeries features as the negative class. This approach ended up being more accurate than both state-of-the-art model and sparse coding model. It was faster than more than 50% of the models compared to and it required less training data to become accurate. However it was less accurate than the top end models.

Grey level occurrence matching [60]. In TF-GLCM, texture features are extracted from the input image to identify whether it is authentic or tampered. The textural features are calculated based on BDCT which is capable of decomposing an image into several blocks and GLCM which can exhibit good features of image textures. The input color image is converted into YCbCr color model, and chrominance components of the image pixel array are divided into a set of non-overlapping  $n \times n$  blocks. The 2-D DCT is applied to each block, and the corresponding DCT coefficient array is obtained. The Difference BDCT arrays in the four directions are calculated. For each of the differences in the BDCT array, the four GLCM with the different combinations of  $d$  and  $\theta$  are calculated. And six types of textural features are extracted based on the four GLCM. The Me and SD of each type of textural features are calculated in the four directions and they are used as elements in feature vectors to distinguish authentic and spliced images with SVM as the classifier. The proposed method has the highest accuracy compared to the five leading other methods. The dimensionality and as a result the number of feature vectors required by the proposed method are much lower. The proposed method is robust against noise.

Another approach [62] used the CASIA Tampered Image Detection Evaluation Database version 1.0 (CASIA TIDE v1.0) and version 2.0 (CASIA TIDE v2.0) or (CASIA 2010) and Columbia Image Splicing Detection Evaluation Dataset (Columbia) for their model. Image tampering (copy-move or splicing) is done simply by copying and pasting. The pasting operation introduces structural changes in the host image. The micro-texture patterns inside and along the boundary of the pasted region become different, and discontinuity is introduced along its edges. In this way, local frequency distribution is changed and there is no more correlation between image pixels in the region. Capturing these structural changes is a key step to successful detection of tampering. The algorithm goes as follows: Pre-processing - color conversion; Feature extraction - Block division, LBP, DCT; Classification - Training, testing; Evaluation. Combining LBT and DCT has led to over 90% accuracy rate, which is extremely high. This method has more accuracy than every method proposed prior to its year of release. Unfortunately, it's drastically more computationally expensive to train the model.

#### *D. Other Novel Techniques*

##### *1) GPU Based Methodology*

In this paper [36] the authors present a GPU based offline signature verification system that has been implemented using Hidden Markov Model (HMM) for both training and verification of the signatures. It was discovered that this version of offline signature verification system achieves a speedup of approximately 5 times more over the serial implementation. This gives a positive sign for the way to be useful at several time constrained situations.

##### *2) Discrete Cosine Transform Approach*

This method [37] uses DCT and local binary design to implement Image tampering (copy-move or splicing) which is done simply by copying and pasting. The pasting operation involves structural changes in the original image. The micro-texture patterns inside and among the boundary of the pasted region turns into different, and discontinuity is introduced near its edges. In this manner, local binary distribution is changed and there is no more correlation among image pixels in the region. Capturing these structural values is a key step to successful identification of tampering.

##### *3) Histogram of Oriented Gradients Approach*

This paper [38] proposes an approach that aims to complement existing efforts in this field by employing Histogram of Oriented Gradients (HOGs) as a feature extraction mechanism that feeds into a template matching exercise based on Normalized Cross Correlation (NCC). The scale at which HOGs are applied is controlled in order to investigate the trade-off between granularity and verification effectiveness. Accuracies of 78% and 70% are obtained on the SVC2004 dataset for complete and half signature coverage respectively. It highlights the importance of global context when using real time features, since it appears that useful information is lost when using separate HOGs for the first and second half of an online signature.

The two false outcomes are formally quantified through the False Acceptance Rate (FAR) and False Rejection Rate (FRR) metrics. FAR measures the rate at which forged signatures are incorrectly verified as genuine while FRR measures the rate at which genuine signatures are incorrectly verified as forged signatures. Of these two error types, false acceptance is considered as the less desirable error in biometric security since it grants system access to unauthorized users.

#### 4) *DTW-based Algorithm Approach*

In this paper [43] the author proposes a methodology for evaluating the robustness of handwritten signature biometrics against forgeries. A particular emphasis has been applied in considering the viability of the attacks under operational environments. In order to carry out this work, not only a methodology but a toolbox has been developed. Such a toolbox stores data, not only from a signing pad connected to a computer, but also from touch-screen devices such as smartphones and tablets. The proposed methodology has been tested by performing a robustness evaluation of a DTW-based algorithm, and with a database of genuine signatures acquired using a STU-500 pad as an input for the evaluation toolbox. The improvement on the number of successful attacks when training with only static information leads to the conclusion that the algorithm may be more sensible to the static information than the dynamic. This technique however produces different results with different algorithms, especially Presentation Attack detection (PAD) mechanisms.

#### 5) *Motion Data Analysis Algorithm Approach*

The paper [63] set out to see if motion detection hardware could be capable of detecting forgery. They hypothesized that it is possible to verify handwritten signatures accurately by analyzing motion data (i.e., accelerometer and gyroscope measurements) collected from hand-worn devices. They based their hypothesis on the assumption that most people adopt a specific signing pattern over the years that is unique and very difficult for others to imitate, and this uniqueness can be captured adequately using the motion sensors of a hand-worn device. The algorithm goes as follows: reference signature and forged signature are inputs, both are normalized, applying DCT function to transform both sets of data to frequency domain, feature extraction using DTW, model is trained using those features. This resulted in a model that works extremely well provided you have the hardware required to motion track hands and provides high accuracy. However, this approach can't be used in a real world setting to classify a real vs forged signature as motion data is required from the forger. It also requires expensive hardware.

#### 6) *Time Causal Information Theory Quantifiers*

A novel approach [64] experimented with a completely unique kind of detection using time causal information. The procedure exploits only the temporal information present in the signature coordinates and, thus, can be termed quasi-offline. Data acquisition and pre-processing, they performed quasi-offline recognition, as they only employ information about coordinates and do not require pressure, speed or pen-up movements data. For feature extraction, they tackled the problem with parameter features: signatures are characterized as a six-dimensional vector extracted from the original data. Finally, for classification, their approach is related to distance-based classifiers, as they made decisions based on the similarity of the features extracted from the test signature to a description of an ensemble of genuine signatures. They pre-processed each time series as follows: a) the coordinates were re-scaled into the unit square  $[0, 1] \times [0, 1]$ ; b) the original total number of data for each time series is expanded to  $M = 5000$  points using a cubic Hermite polynomial. In this way, for each subject  $k$  ( $k = 1, \dots, 100$ ) and associated signatures  $j$  ( $j = 1, \dots, 25$ ) they analyzed two time series, in which the supra-index  $\alpha = G, F$  denotes genuine and forgery signature, and  $x_{\sim}$  and  $y_{\sim}$  are the interpolated values, respectively. With as few as five examples it surpasses the performance of recent successful techniques. The error exponentially decreases when the number of samples increases. The main weakness is that this model can only be used for scanned signatures.

#### 7) *Additive Fuzzy Modelling*

This paper [68] proposed a model based on additive fuzzy modelling. The handwritten signatures images are pre-processed and angle features extracted from them via a novel grid method. These features are then modelled using the Takagi-Sugeno fuzzy model, which involves two structural parameters in its exponential membership function. Each angle feature yields a fuzzy set when its values are gathered from all samples because of the variations in handwritten signatures. Two cases are considered. In the first case, the coefficients of the consequent part of the rule are fixed so as to yield a simple form of TS model and in the second case the coefficients are adapted. In this formulation, each rule is constituted by a single feature. In the second formulation, we consider only one rule encompassing all the features.

### 8) Adaptive Over-Segmentation and Feature Point Matching

This author [68] conducted multiple experiments to evaluate the effectiveness and robustness of the proposed image forgery detection scheme using adaptive over-segmentation and feature point matching. proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over-Segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. Subsequently, to detect the more accurate forgery regions, we propose the Forgery Region Extraction algorithm, in which the labeled feature points are replaced with small superpixels as feature blocks, and the neighboring feature blocks with local color features that are similar to the feature blocks are merged to generate the merged regions. Next, the morphological operation is applied to the merged regions to generate the detected forgery regions.

In [69], the authors proposed a system which uses Feature Extraction and Matching for online signature verification which deals with both forgeries and disguised signatures. This system extracts several features of the signatures and compares them at the histogram level and the signal level.

Several classifiers have been tested for combining these features, with neural networks and random forests generally preferred.

### 9) Pseudo- Bacterial Genetic Algorithm (PBGA)

In [70], the main thrust here is to establish the genuineness of the signature thereby detecting the forgeries, we go in for fuzzy modeling of angle features. For the purpose of signature verification and detection of forgeries, they employed the Takagi-Sugeno model for considering each feature as forming a fuzzy set over large samples. This is because the same feature exhibits variation in different samples giving rise to a fuzzy set. So, their attempt was to model the uncertainty through a fuzzy model such as the TS model.

### 10) Bayesian Learning of Finite Generalized Inverted Dirichlet Mixtures

In [52] using Bayesian alternatives to both Gaussian and the inverted Dirichlet mixtures when dealing with positive data, a proposed algorithm based on the generalized inverted Dirichlet distribution which offers high flexibility and ease of use. The proposed mixture model is subjected to a fully Bayesian analysis based on Markov Chain Monte Carlo (MCMC) simulation methods namely Gibbs sampling and Metropolis–Hastings used to compute the posterior distribution of the parameters, and on Bayesian information criterion (BIC) used for model selection.

### 11) KAZE Features via Fisher Encoder

In [48] a new method using KAZE features based on the recent Fisher vector (FV) encoding is proposed. The adoption of a probabilistic visual vocabulary and higher-order statistics, both of which can encode detailed information about the distribution of KAZE features, provides us with a more precise spatial distribution of the characteristics for a writer. The experimental results on the public MCYT-75 dataset

## III. PROPOSED METHODOLOGY

In order to address the constraint of the current CNN algorithms which results in about false positives and cuts down the real world accuracy of the program that will be utilized in a professional field of work, we propose a novel strategy that makes use of ResNet (Residual Neural Network), a type of neural network, which simplifies the problem by essentially taking a few shortcuts across certain steps or processes involved which thus permits the gradient to be directly backtracked thereby lessening the odds that it will rapidly fall to a very small value.

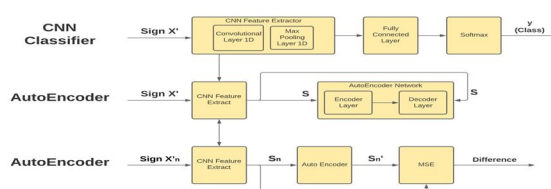


Figure 1: Working of Forgery Detection of Handwritten signatures based on CNN



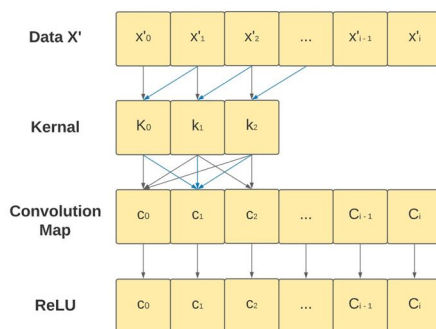


Figure 2: Working of ResNet (Residual Neural Network)

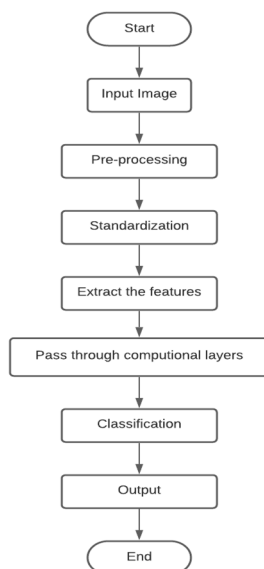


Figure 2: Flowchart of our proposed algorithm

```

TRAIN TEST(train_features, test features unlabeled features
Returns test results of the deep classifier.

ResNet ← load()
Incep ← load()
Xcep ← load()

res_features ← ResNet(train_features, test_features, unlabeled_features)
incep_features ← Incep(train_features, test_features, unlabeled_features)
xcep_features ← Xcep(train_features, test_features, unlabeled_features)
all_features ← concatres features, inc features, xep features
if save_features=True then
    save (all features)
end if
model ← create_model()
if training = True then
    fitted_model ← model.fit(all_features train), labels)
if pseudo = True then
    newly_labeled ← pseudo labeling (fitted_model, all_features[unlabeled])
    fitted_model ← fitted_model.file(newly_labeled, labels)
end if
model ← fitted_model
end if
if testing =True then
    results ← fitted_model(all_features[test])
end if
return results
end

```

Figure 3 : Proposed Algorithm

- 1) *Input Image*: The images to be tested will be provided to the system as an input.
- 2) *Pre-processing*: The picture will be modified into a NumPy series for further processing. Data alteration will be done; here the pictures are randomized so as to prepare the model to be able to create proficient and accurate outcomes.
- 3) *Standardization*: Standardization will make the data similar to each other and provides them a mutual belief to chip away at. It involves rescaling of the data.
- 4) *Passing through Computational Layers*: Each stage wise, the dataset will be passed through the numerous layers available in the deep neural network. These layers are the convolutional block and the ResNet.
- 5) *Extract the Features*: The CNN is applied in such a manner as to find particular features and patterns available in images. We effectively find trends in that portion of the image as we pass over an image. This works due to filters which are groups of weights depicted as a vector and are multiplied by the numbers that are as output by the convolution. The pooling layer divides the input picture into a set of rectangles and for each such sub-part it outputs a value. The result is that the precise location of a feature is not as significant as its approximate location with regard to other features. Hence, CNN is trained with a dataset and has the capacity to smartly identify certain features for a test picture.
- 6) *Classification*: Two classes have been designed for classification. One class is called the “forged” and the other class is called the “original”. The test picture will be classified under one of these two classes.
- 7) *Output*: The output/result of the system will be displayed here. The image input’s shape and the class prediction vector will be shown in order to identify if the signature is fake or original.

In our project, we assume that if a CNN is programmed to classify between counterfeit and original signatures, the trained model can take out effective attributes to help differentiate behavior features of forgery, such as hesitation and delay before calculating the complex portions of a signature. The advantage of deep networks is that it depicts multiple complex methods and learns features at various levels of abstraction, leaving to complex features that are present in the lowermost of the layers from the borders which are a part of the much lower layers in general. But a large barrier while implementing deep networks is that the gradient reduces exponentially and rapidly to zero as we back trace back from the final layer, back to the initial layer. In very rare cases it might rapidly increase or grow into very large values, spontaneously and quickly.

This is more problematic during the handling of an image dataset which has signatures because of the fact that they are containing many areas with very clear lines and small marks in the pictures that can in affect the final output and that last result is modified many times due to this limitation of the CNN framework. This mostly results in false positives and brings down the real world accuracy of the program that will be used in a professional capacity.

To overcome this, we use the ResNet (Residual Neural Network) which carries the weight of the matrix from the initial to the last without actually traversing through the layers in between.

#### IV. EVALUATION

We have used Python and its libraries, in conjunction with a solution based on Convolutional Neural Network (CNN) for detecting forgery in handwritten signatures. A working desktop/laptop with Windows 10 operating system is needed to run this program for detecting forgery in handwritten signatures. A minimum of 4GB of RAM, with at least an intel I3 intel processor. A Nvidia graphics card would be preferred for more efficient training.

#### REFERENCES

- [1] Meena, K. B., & Tyagi, V. (2020). A copy-move image forgery detection technique based on tetrolet transform. *Journal of Information Security and Applications*, 52, 102481.
- [2] Badr, A., Youssif, A., & Wafi, M. (2020, June). A Robust Copy-Move Forgery Detection In Digital Image Forensics Using SURF. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
- [3] Hegazi, A., Taha, A., & Selim, M. M. (2020). Copy-Move Forgery Detection Based on Automatic Threshold Estimation. *International Journal of Sociotechnology and Knowledge Development (IJSKD)*, 12(1), 1-23.
- [4] Devanshi Chauhan, Dipali Kasat, Sanjeev Jain, Vilas Thakare, Survey on Keypoint Based Copy-move Forgery Detection Methods on Image, *Procedia Computer Science*, Volume 85, 2016, Pages 206-212, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2016.05.213>.
- [5] Zandi, M., Mahmoudi-Aznaveh, A., & Talebpour, A. (2016). Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector. *IEEE Transactions on Information Forensics and Security*, 11(11), 2499–2512. doi:10.1109/tifs.2016.2585118.
- [6] Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., & Yang, H. (2016). Fusion of block and keypoints based approaches for effective copy-move image forgery detection. *Multidimensional Systems and Signal Processing*, 27(4), 989–1005.
- [7] Zhu, Y., Shen, X., & Chen, H. (2015). Copy-move forgery detection based on scaled ORB. *Multimedia Tools and Applications*, 75(6), 3221–3233.
- [8] Diallo, B., Urruty, T., Bourdon, P., & Fernandez-Maloigne, C. (2020). Robust Forgery Detection for Compressed Images using CNN Supervision. *Forensic Science International: Reports*, 100112.

- [9] Chen, Y., & Gao, S. (2020, June). Forgery Numeral Handwriting Detection based on Convolutional Neural Network. In 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC) (pp. 201-205). IEEE.
- [10] Xiao, Bin, et al. "Image Splicing Forgery Detection Combining Coarse to Refined Convolutional Neural Network and Adaptive Clustering." *Information Sciences*, vol.511, 2020, pp. 172-191.
- [11] Sharif, M., Khan, M. A., Faisal, M., Yasmin, M., & Fernandes, S. L. (2018). A framework for offline signature verification system: Best features selection approach. *Pattern Recognition Letters*.
- [12] P. V. Bhagyasree, A. James and C. Saravanan, "A Proposed Framework for Recognition of Handwritten Cursive English Characters using DAG-CNN," 2019 1st International Conference on Innovations in Information and Communication Technology (ICICT), CHENNAI, India, 2019, pp. 1-4
- [13] B. M. A. Rahman, G. Mostaeen and M. H. Kabir, "A statistical approach for offline signature verification using local gradient features," 2016 2nd International Conference on Electrical, Computer & Telecommunication Engineering (ICECTE), Rajshahi, 2016, pp. 1-4
- [14] Aravinda C.V; Lin Meng; Uday Kumar Reddy K.R," An approach for signature recognition using contours based technique ", 2019 International Conference on Advanced Mechatronic Systems (ICAMechS),doi: 10.1109/ICAMechS.2019.8861516
- [15] Bilal Hadjadji, Youcef Chibani, Hassiba Nemmour; Neurocomputing," An efficient open system for offline handwritten signature identification based on curvelet transform and oneclass principal component analysis" Volume 265, 22 November 2017,p66-67
- [16] L. Chen, S. Wang, W. Fan, J. Sun and S. Naoi, "Beyond human recognition: A CNN-based framework for handwritten character recognition," 2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR), Kuala Lumpur, 2015, pp. 695-699.
- [17] A. Abdel Raouf and D. Salama, "Handwritten Signature Verification using Haar Cascade Classifier Approach," 2018 13th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 2018, pp. 319-326
- [18] C. S. Vorugunti, P. Mukherjee and V. Pulabaigari, "Online Signature Profiling using Generative Adversarial Networks," 2020 International Conference on COMMunication Systems & NETworkS (COMSNETS), Bengaluru, India, 2020, pp. 894-896, doi: 10.1109/COMSNETS48256.2020.9027369.
- [19] Shih Yin Ooi, Andrew Beng JinTeoh, Ying HanPang, Bee YanHiew ,,"Image-based handwritten signature verification using hybrid methods of discrete Radon transform, principal component analysis and probabilistic neural network",*Applied Soft Computing*, Volume 40, March 2016,pp 274-282
- [20] Khan, S., Khan, K., Ali, F., & Kwak, K. S. (2020). Forgery Detection and Localization of Modifications at the Pixel Level. *Symmetry*, 12(1), 137.
- [21] Kao, H. H., & Wen, C. Y. (2020). An Offline Signature Verification and Forgery Detection Method Based on a Single Known Sample and an Explainable Deep Learning Approach. *Applied Sciences*, 10(11), 3716.
- [22] Ahmed, B., & Gulliver, T. A. (2020). Blind copy-move forgery detection using SVD and KS test. *SN Applied Sciences*, 2(8), 1-12.
- [23] Image forgery detection based on statistical features of [23] Dua, S., Singh, J., & Parthasarathy, H. (2020). block DCT coefficients. *Procedia Computer Science*, 171, 369-378.
- [24] Ruiz, V., Linares, I., Sanchez, A., & Velez, J. F. (2020). Off-line handwritten signature verification using compositional synthetic generation of signatures and Siamese Neural Networks. *Neurocomputing*, 374, 30-41.
- [25] Foroozandeh, A., Hemmat, A. A., & Rabbani, H. (2020, February). Offline Handwritten Signature Verification Based on Circlet Transform and Statistical Features. In 2020 International Conference on Machine Vision and Image Processing (MVIP) (pp. 1-5). IEEE.
- [26] Al\_Azrak, F. M., Sedik, A., Dessowky, M. I., El Banby, G. M., Khalaf, A. A., Elkorany, A. S., & El-Samie, F. E. A. (2020). An efficient method for image forgery detection based on trigonometric transforms and deep learning. *Multimedia Tools and Applications*, 1-23.
- [27] Suresh, G., & Rao, C. S. (2020). Copy Move Forgery Detection Through Differential Excitation Component-Based Texture Features. *International Journal of Digital Crime and Forensics (IJDCF)*, 12(3), 27-44.
- [28] N. Arab, H. Nemmour and Y. Chibani, "New Local Difference Feature for Off-Line Handwritten Signature Verification," 2019 International Conference on Advanced Electrical Engineering (ICAEE), Algiers, Algeria, 2019, pp. 1-5, doi: 10.1109/ICAEE47123.2019.9014828.
- [29] S. Lai and L. Jin, "Recurrent Adaptation Networks for Online Signature Verification," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1624-1637, June 2019, doi: 10.1109/TIFS.2018.2883152.
- [30] Chu, Jun & Shaikh, Mohammad Abuzar & Chauhan, Mihir & Meng, Lu & Srihari, Sargur. (2018). Writer Verification using CNN Feature Extraction.
- [31] Kruthi, C., & Shet, D. C. (2014, January). Offline signature verification using a support vector machine. In 2014 Fifth International Conference on Signal and Image Processing (pp. 3-8). IEEE.
- [32] Ben Nassi, Alona Levy, Yuval Elovici, & Erez Shmueli. (2016). Handwritten Signature Verification Using Hand-Worn Devices.
- [33] Poddar, J., Parikh, V., & Bharti, S. K. (2020). Offline Signature Recognition and Forgery Detection using Deep Learning. *Procedia Computer Science*, 170, 610-617.
- [34] Doctor, Anoushka, Prerana Mukherjee, and Viswanath Pulabaigiri. "A Light weight and Hybrid Deep Learning Model based Online Signature Verification." *arXiv preprint arXiv:1907.04061* (2019).
- [35] C. Park, H. Kim and H. Choi, "Robust Online Signature Verification Using Long-term Recurrent Convolutional Network," 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, pp. 1-6, doi: 10.1109/ICCE.2019.8662005.
- [36] A. K. Kar, S. Kumar Chandra and M. Kumar Bajpai, "Parallel Gpu Based Offline Signature Verification Model," 2019 IEEE 16th India Council International Conference (INDICON), Rajkot, India, 2019, pp. 1-4.
- [37] Alahmadi, A., Hussain, M., Aboalsamh, H. et al. Passive detection of image forgery using DCT and local binary pattern. *SIViP* 11, 81-88 (2017).
- [38] M. Mshengu and M. V. Gwetu, "Online Signature Verification through Scaled Histogram of Oriented Gradients," 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Winterton, South Africa, 2019, pp. 1-5, doi: 10.1109/ICABCD.2019.8851050.
- [39] V. L. F. Souza, A. L. I. Oliveira, R. M. O. Cruz and R. Sabourin, "On Dissimilarity Representation and Transfer Learning for Offline Handwritten Signature Verification," 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 2019, pp. 1-9, doi: 10.1109/IJCNN.2019.8852130.
- [40] M. Okawa, "Online Signature Verification Using Multi-Distance Measures and Weighting with Gradient Boosting," 2019 IEEE 1st Global Conference on Life Sciences and Technologies (LifeTech), Osaka, Japan, 2019, pp. 277-278, doi: 10.1109/LifeTech.2019.8884008.
- [41] C. Li et al., "A Stroke-Based RNN for Writer-Independent Online Signature Verification," 2019 International Conference on Document Analysis and Recognition (ICDAR), Sydney, Australia, 2019, pp. 526-532, doi: 10.1109/ICDAR.2019.00090.



- [42] L. Chen, S. Wang, W. Fan, J. Sun and S. Naoi, "Beyond human recognition: A CNN-based framework for handwritten character recognition," 2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR), Kuala Lumpur, 2015, pp. 695-699.
- [43] R. Sanchez-Reillo, H. C. Quiros-Sandoval, J. Liu-Jimenez and I. Goicoechea-Telleria, "Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries," 2015 International Carnahan Conference on Security Technology (ICCST), Taipei, 2015, pp. 373-378
- [44] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks [Abstract]. Pattern Recognition, 70, 163-176. doi:10.1016/j.patcog.2017.05.012
- [45] Hanmandlu, M., Sronothara, A. B., & Vasikarla, S. (2018). Deep Learning based Offline Signature Verification. 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). doi:10.1109/uemcon.2018.8796678
- [46] Nedjah, N., Mourelle, L. D., Buarque, F., & Wang, C. (2017). New trends for pattern recognition: Theory and applications. Neurocomputing, 265, 1-3. doi:10.1016/j.neucom.2017.05.080
- [47] Bunk, J., Bappy, J. H., Mohammed, T. M., Nataraj, L., Flenner, A., Manjunath, B., . . . Peterson, L. (2017). Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning. 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). doi:10.1109/cvprw.2017.235
- [48] Okawa, M. (2017). KAZE features via fisher vector encoding for offline signature verification. 2017 IEEE International Joint Conference on Biometrics (IJCB). doi:10.1109/btas.2017.8272676
- [49] G. S. Prakash and S. Sharma (2017) Computer vision & fuzzy logic based offline signature verification and forgery detection. 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2014, pp. 1-6, doi: 10.1109/ICCIC.2014.7238363.
- [50] D. Cozzolino, D. Gragnaniello and L. Verdoliva (2014) Image forgery detection through residual-based local descriptors and block-matching. 2014 IEEE International Conference on Image Processing (ICIP), Paris, 2014, pp. 5297-5301, doi: 10.1109/ICIP.2014.7026072.
- [51] Kruthi, C., & Shet, D. C. (2014). Offline Signature Verification Using Support Vector Machine. 2014 Fifth International Conference on Signal and Image Processing. doi:10.1109/icsip.2014.5
- [52] Bourouis, S., Mashrgy, M. A., & Bouguila, N. (2014). Bayesian learning of finite generalized inverted Dirichlet mixtures: Application to object classification and forgery detection. Expert Systems with Applications, 41(5), 2329-2336. doi:10.1016/j.eswa.2013.09.030
- [53] Carvalho, T. J., Riess, C., Angelopoulou, E., Pedrini, H., & Rocha, A. D. (2013). Exposing Digital Image Forgeries by Illumination Color Classification. IEEE Transactions on Information Forensics and Security, 8(7), 1182-1194. doi:10.1109/tifs.2013.2265677
- [54] Lakshmi, K. V., & Nayak, S. (2013). Off-line signature verification using Neural Networks. 2013 3rd IEEE International Advance Computing Conference (IACC). doi:10.1109/iadcc.2013.6514374
- [55] Chauhan, D., Kasat, D., Jain, S., & Thakare, V. (2016). Survey on keypoint based copy-move forgery detection methods on image. Procedia Computer Science, 85, 206-212
- [56] Zandi, M., Mahmoudi-Aznavah, A., & Talebpour, A. (2016). Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector. IEEE Transactions on Information Forensics and Security, 11(11), 2499-2512. doi:10.1109/tifs.2016.2585118
- [57] Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., & Yang, H. (2016). Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidimensional Systems and Signal Processing, 27(4), 989-1005. doi:10.1007/s11045-016-0416-1
- [58] Zhu, Y., Shen, X., & Chen, H. (2015). Copy-move forgery detection based on scaled ORB. Multimedia Tools and Applications, 75(6), 3221-3233. doi:10.1007/s11042-014-2431-2
- [59] Elias N. Zois, Ilias Theodorakopoulos, George Economou; Proceedings of the IEEE International Conference on Computer Vision (ICCV), 2017, pp. 5514-5523
- [60] Shen, X., Shi, Z., & Chen, H. (2017). Splicing image forgery detection using textural features based on the grey level co-occurrence matrices. IET Image Processing, 11(1), 44-53. doi:10.1049/iet-ipr.2016.0238
- [61] Zhang, Y., Goh, J., Win, L.L., & Thing, V.L. (2016). Image Region Forgery Detection: A Deep Learning Approach. SG-CRC.
- [62] Alahmadi, A., Hussain, M., Aboalsamh, H. et al. Passive detection of image forgery using DCT and local binary pattern. SIVIP 11, 81-88 (2017).
- [63] Ben Nassi, Alona Levy, Yuval Elovici, & Erez Shmueli. (2016). Handwritten Signature Verification Using Hand-Worn Devices.
- [64] Rosso OA, Ospina R, Frery AC (2016) Classification and Verification of Handwritten Signatures with Time Causal Information Theory Quantifiers. PLOS ONE 11(12): e0166868.
- [65] Brian C. Lovell & Vamsi Krishna Madasu (2018) An Automatic Offline Signature Verification and Forgery Detection System.
- [66] Nabin Sharma, Ranju Mandal , Rabi Sharma, Umпада Pal (2018) Signature and Logo Detection using Deep CNN for Document Image Retrieval.
- [67] Basavarajappa, Shwetha B & Sathyanarayana, S.. (2016). Digital image forgery detection techniques: a survey. ACCENTS Transactions on Information Security. 2. 22-31. 10.19101/TIS.2017.25003.
- [68] Pun, Chi-Man & Yuan, Xiaochen & Bi, Xiu-Li. (2015). Image Forgery Detection Using Adaptive Over-Segmentation and Feature Points Matching. IEEE Transactions on Information Forensics and Security. 10. 1-1. 10.1109/TIFS.2015.2423261.
- [69] Hassaine, Abdelâali & Al-ma'adeed, Somaya. (2012). An Online Signature Verification System for Forgery and Disguise Detection. 7666. 10.1007/978-3-642-34478-7\_67.
- [70] Mohd Yusof, Mohd Hafizuddin & Madasu, Vamsi. (2003). Signature Verification and Forgery Detection System. 9 - 14. 10.1109/SCORED.2003.1459654.
- [71] Gideon, S. J., Kandulna, A., Kujur, A. A., Diana, A., & Raimond, K. (2018). Handwritten signature forgery detection using convolutional neural networks. Procedia computer science, 143, 978-987.



10.22214/IJRASET



45.98



IMPACT FACTOR:  
7.129



IMPACT FACTOR:  
7.429



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24\*7 Support on Whatsapp)