Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 170 (2020) 610–617

Procedia Computer Science

www.elsevier.com/locate/procedia

The 3rd International Conference on Emerging Data and Industry 4.0 (EDI40), April 6 - 9, 2020, Warsaw, Poland

# Offline Signature Recognition and Forgery Detection using Deep Learning

Jivesh Poddar[a], Vinanti Parikh[a], Santosh Kumar Bharti[a,*]

[a] *Pandit Deendayal Petroleum University, Gandhinagar, Gujarat, India*

**Abstract**

Authentication plays a very important role to manage security. In the modern era, it is one, in all the priorities. With the appearance of technology, the interaction with machines is turning automatic. Therefore, the need of authentication increases rapidly for various security purposes. Because of this, the biometric-based authentication has gained a drastic momentum. It is a kind of boon over other techniques. However, this event is not a replacement of drawback but varied ways are adopted to verify folks. Signature is one of the first broadly practiced biometric features for the verification of an individual. This paper proposes a method for the pre-processing of signatures to make verification simple. It also proposed a novel method for signature recognition and signature forgery detection with verification using Convolution Neural Network (CNN), Crest-Trough method and SURF algorithm & Harris corner detection algorithm. The proposed system attains an accuracy of 85-89% for forgery detection and 90-94% for signature recognition.



*Keywords:* Signature Verification; Forgery Detection; CNN; Signature Recognition; SURF Algorithm; Harris Algorithm.

## 1. Introduction

A signature is outlined as a uniquely written drawing that a person writes on any document as an indication of identity. An individual uses it on a usual wish to sign a check, a legal instrument, contract, etc. The matter arises when once somebody tries to replicate it. A signature by any individual depicts a picture conveying a particular pattern of pixels that bothers a particular person. Signature verification drawback is plagued with monitoring and checks whether a picked signature refers to an individual or not. Signatures range exceptional case of script during which special characters flourish area unit viable. Signature verification may be a complex pattern identification with a shortcoming as no two genuine signatures of an individual can be precisely similar. If unintentionally it is winning then it will do serious injury to a person. One of the way is to use the biometric features of every individual. In this paper, we tend to specialize in the signature as a biometric feature whereas, we tend to notice that signature depends

* Corresponding author. Tel.: +91-933-826-2742 ; fax: +0-000-000-0000.
*E-mail address:* sbharti1984@gmail.com

1877-0509 
10.1016/j.procs.2020.03.133

on several other factors like state of the person, body position, writing surface, environmental factors, etc. Therefore, it is necessary to get rid of the maximum amount of features as attainable these factors to extend the potency of the system. However, it is hard to include all factors. In this work, we represented a number of ways to discern forgery in signature. Our proposed approach relies on a Convolutional Neural Networks (CNN) [2][4] for signature verification and Crest-Trough [8] for forgery detection. CNN consists of assorted layers wherever inputs labor under and are finally, feed into the classifier. It is one of the most effective methodologies for detective work whether or not the signature is real or solid. In Crest-Trough for forgery detection, the range in every signature and the magnitude relation between consecutive crest and trough remains the same. CNNs are extremely effective system for recognition task because it is way higher at extracting important/relevant data for classification than humans.

The contributions of the paper are as follows:

- Proposed preprocessing method to make verification of signature easier.
- Proposed CNN, Crest-Trough algorithm based model for Signature verification system.
- Proposed Harris, Surf based model for forgery detection in signature.

The rest of the paper is organized as follows: Section 2 explains the literature survey. Proposed scheme is discussed in Section 3. Experimental results are shown in Section 4. Finally, Section 5 drawn the conclusion and future scope.

## 2. Literature Survey

In the recent past, no work is reported for Offline signature verification using deep learning techniques. A very few authors [1][3][5][6][7][9][10][11][12] are working in this direction.

Table 1. Summary of previous relevant studies on signature verification.

| Studies | Key Features and Dataset | Implementation method | Results and Conclusion |
|---|---|---|---|
| Shahane et al. [1] | Noise removal, pre-processing, feature extraction, learning and verification modules. | Different thresholds used for matching to boost the general potency of the system. It additionally includes the verification of the account range and quantity on the cheque using OCR and finds out if the cheque is cleared or bounced. | The edge values used here weren't acceptable for all kinds of signatures because the values dissent from signature to signature of various persons. |
| Fahmy [3] | Supported separate wave remodel discrete wavelet transform (DWT) feature extraction and uses a feed-forward backpropagation error neural network for recognition. | It's enforced on information of two hundred signature having twenty real and twenty sure-handed forgery signatures of 5 folks. | Accuracy obtained is ninety-fifth for real signature. Here the dataset used for terribly little and overfitting prospects was high. |
| Zhu et al. [9] | It has a supervised learning framework for combining complementary form data from totally different unsimilarity metrics via LDA. | Nursing approach to conjointly notice that signatures from document image can be extracted by structure study detection across image scales. | It is a complicated structural framework. |

## 3. Preliminaries

To extract and procure correct feature results from the images, equipped images should have an exact form, size, and alignment to strike a comparison amongst all. Hence, numerous pre-processing techniques are applied as shown in Fig. 1 to realize the specified exactness within feature detection.

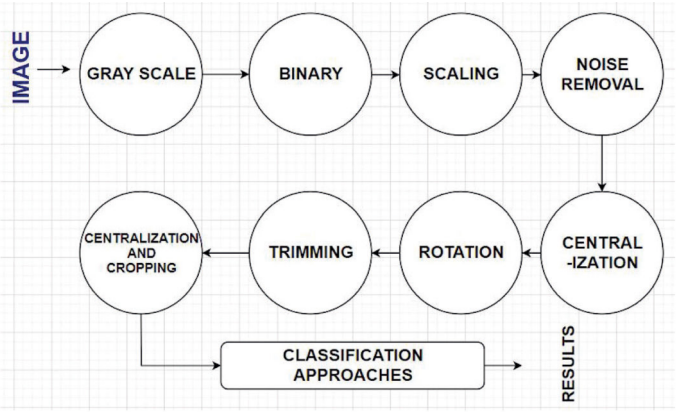


Fig. 1. Data Pre-Processing.

### *3.1. Preprocessing Algorithms On CNN*

#### *3.1.1. Noise Removal*

With each image that carries vital knowledge, additionally comes the noise pixels that aren't a part of the image. Now, since the project is bothered with written signatures, most of the noise points area unit is like small dark spots on paper that keep once the image is reborn to binary. To make freed of those points, the picture was examined by running a frame of size 5x5 with each component however the sting points are at the center of the window. If the magnitude relation of black pixels within the same is 0.3 then that center constituent was reborn to white. Thus, noise removal leaves the image with simply the pen or pencil points. A sample noise removal process is shown in Fig. 2, where part (a) shows original and part (b) shows noise less signature.

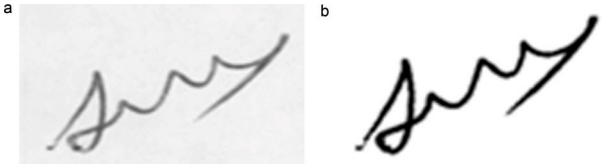


Fig. 2. (a) Original Image; (b) Transformed Image.

#### *3.1.2. Scaling*

The signature within the image will generally be of a larger length and will be covering most of the image, which can build rotation tough as therefore a part of the signature is often lost whereas doing so. To beat a similar, every constituent of the signature is scaled to a smaller length to scale back the general space of the image. The scaling of the image is completed by an element of 1/(sqrt(2)) if the length of the signature exceeds by a substantial quantity. A sample signature scaling process is shown in Fig. 3, where part (a) shows original and part (b) shows scaled image.

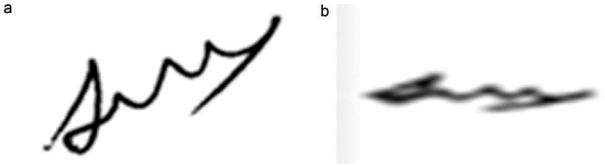


Fig. 3. (a) Original Image; (b) Transformed Image.

#### *3.1.3. Centralization*

The signature thanks to scaling will shift to the corner by varying amounts, to equalize a similarly the signature is delivered to the center of the image by shifting the pixels from an element of Manhattan distance from the middle

of the image. A sample signature centralization process is shown in Fig. 4, where part (a) shows original and part (b) shows centralized image.

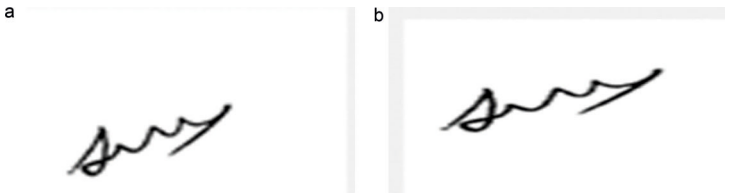


Fig. 4. (a) Original Image; (b) Transformed Image.

*3.1.4. Rotation*

The image obtained once centralization contains signature within the middle. Thanks to the signature being done at numerous potential angles, still the matter of angle of signature persists, thence to form every signature horizontal, rotation is performed on the signature. For rotation, the angle of the road change of integrity bottom-most left purpose and therefore the bottom-most right purpose with a surface is measured and then revolved by the angle obtained. The obtained image is the image with a horizontal signature with zero degree tilt. For accuracy improvement the angle between the left and right points of a signature is taken into account. A sample signature rotation process is shown in Fig. 5, where part (a) shows original and part (b) shows rotated image.

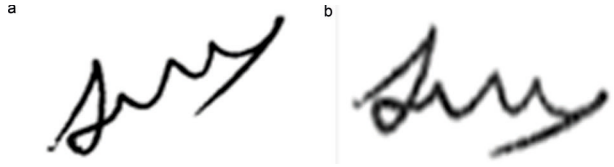


Fig. 5. (a) Original Image; (b) Transformed Image.

*3.2. Preprocessing Algorithms on Crest-Trough Method*

*3.2.1. Length to space Ratio*

The length of the signature is measured by finding the gap between the left and therefore the right constituents that are then divided by the issue of space.

*3.2.2. Width to space Ratio*

The dimension of the signature is obtained by finding the distance between the top and therefore the bottom-most constituent of the signature that is then divided by the issue of space.

*3.2.3. Crest-Trough Parameter*

This is often the foremost necessary parameter of the feature extraction because it takes note of all the contours of the signature. The crest and trough points for every signature contains a definite pattern. Lets contemplate a 3x3 matrix of black constituents and therefore the top-right Associate in Nursing top-left corner black constituent can have the adjacent "Black pixel: White pixel" quantitative relation five: 3 and solely the particular set of neighbours would be white et al black in eight neighbour theory. These points mark the curve corners of a crest within the signature once the rotation. The bottom-left and bottom-right corner black pixel area unit denoted as trough points. The relative distance between these consecutive crest and trough points yields the total that then divided by the realm of the signature returns a novel variety that's relative to simply that signature. Hence, the forgery detection will be done by extracting the features from the associated person's original signature and it will be compared with the signature given for comparison.

When the signature is known on that person it belongs, the image that was tested and therefore the set containing all signature pictures of the known subject is extracted. If all the 3 options extracted consist of the calculated varies the signature is assessed originally else it's thought of cast.

## 4. Proposed Scheme

In this paper, we proposed a novel method for signature recognition and forgery detection. The proposed system architecture is shown in Fig. 6, where, test signature is recognized with the given input training set using both CNN and Crest-Trough method. Then forgery detection algorithms (Harris Algorithmic followed by Surf Algorithm) are enforced on this classified image.

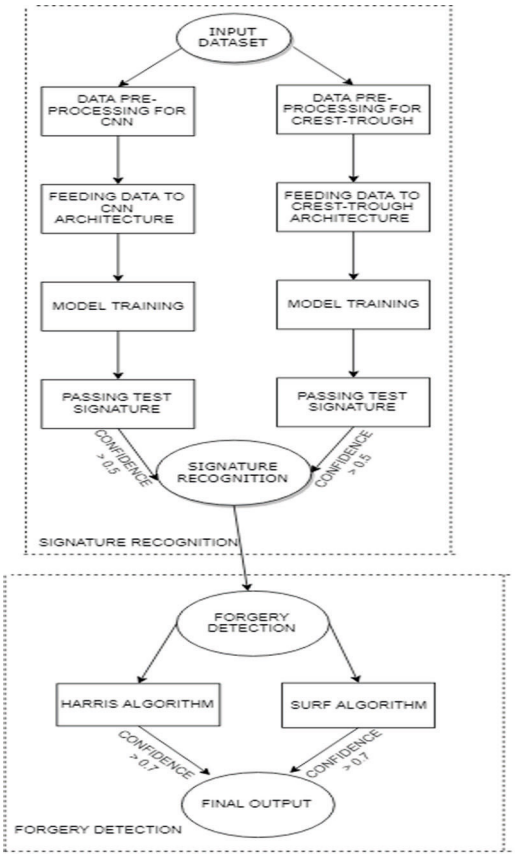


Fig. 6. Proposed system architecture for signature recognition and forgery detection.

### *4.1. Signature Recognition*

Convolutional Neural Networks (CNNs)[4] have tested no-hit in recent years at an outsized variety of image processing-based machine learning tasks. Several different strategies of playacting such tasks as shown in Fig. 7 revolve around a method of feature extraction, during which hand-chosen options extracted from a picture fed into a classifier to make a classification call. Such processes solely as sturdy because of the chosen options, which regularly take giant amounts of care and energy to construct. Against this, in CNN, the options fed into the ultimate linear classifier all learned from the dataset. A CNN consists of a variety of layers as shown in Fig. 7, beginning at the raw image pixels, that each performs an easy computation and feeds the result to the successive layer, with the ultimate result being fed to a linear classifier.

The layers computation area unit supports a variety of parameters that learned through the method of backpropagation, during which for every parameter, the gradient of the classification loss with relation to that parameter is computed and therefore the parameter is updated to minimize the loss perform. The look of any signature verification system typically needs the answer of 5 sub-issues: data retrieval, pre-processing, feature extraction, identification method, and performance analysis. Off-line signature verification just deals with pictures non-heritable by a scanner or a photographic camera. In associate degree off-line signature verification system, a signature is non-heritable as a picture. This picture depicts a private sort of human. The method needs neither be too sensitive nor too rough. It

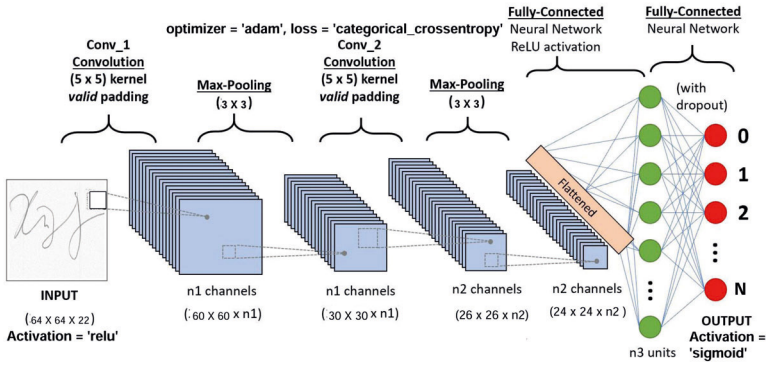


Fig. 7. CNN Architecture.

should have a proper balance between an occasional False Acceptance Rate (FAR) and an occasional False Rejection Rate (FRR).

### *4.2. Signature Forgery Detection*

When the image is finally classified into one among the present classes of the topics. The henceforward system proposes a technique for the detection of the forgery within the same by checking the chosen options against the on the market set of pictures for the signature and produces a binary result if it's cast or not. Here two Algorithms are used for Forgery Detection.

#### *4.2.1. Harris Algorithm*

Avoid hyphenation at the end of a line. Symbols denoting vectors and matrices should be indicated in bold type. Scalar variable names should normally be expressed using italics. Weights and measures should be expressed in SI units. All non-standard abbreviations or symbols must be defined when first mentioned, or a glossary provided [13]. The Harris corner detection algorithm is based on formula shown in Eq. 1.[13]

$$E(v,u) = \sum_{x,y} w(x,y)[I(x+u,y+v) - I(x,y)]^2 \quad (1)$$

Where:

- E is the separation between the first and affected window.
- u, v is the displacement of the frame within the x-direction and y-direction respectively.
- w(x, y) is the frame at point (x, y). This acts sort of a mask which assures that solely the marked window is working.
- I is that the intensity of the image at a point (x, y).
- I(x+u, y+v) is the intensity of the considered frame.
- I(x, y) is the intensity of the first.

Features:

- Corner points detected from training and take a look at knowledge.
- Corner points extracted from training and take a look at knowledge.
- Take a look at knowledge compared with each training knowledge.

#### *4.2.2. Surf Algorithm*

Speeded up robust features (SURF) [14] uses square-shaped filters for approximation of Gaussian smoothing. (The SIFT approach uses cascaded filters to observe scale-invariant characteristic points, wherever the Difference of

Gaussians (DoG) is calculated on rescaled pictures more and more.) Filtering the image with a sq. is far quicker if the integral image is used. The SURF algorithm is based on formula shown in Eq. 2.[14]

$$S(x,y) = \sum_{i=0}^{x} \sum_{j=0}^{y} I(i,j) \tag{2}$$

Features:

- Index points detected from training and take a look at knowledge.
- Index points extracted from training and take a look at knowledge.
- Take a look at points compared with each training knowledge.

## 5. Experimental Results

Firstly, the test signature is recognized with the given input training set using both CNN and Crest-Trough method. Then forgery detection algorithms (Harris Algorithmic followed by Surf Algorithm) are enforced on this classified image. The Results from each the algorithms are then compared as shown in Fig. 8 and Fig. 9 respectively. The popularity associated with identification with neural networks yields an accuracy of 94%. The latter planned forgery detection works with associate accuracy of 85-89%. The sole skilled and closely solid signatures typically don't seem to be captured, else it properly identifies all the forgeries within the signature. A sample result of proposed approach is shown in Fig. 8 and Fig. 9.


Fig. 8. Forgery Detection Using Harris Algorithm.

## 6. Conclusion and Future Scope

The system successfully recognizes and identifies the signature holder accurately with the forgery issue gift in it. The popularity pattern is trained on Convolutional Neural Networks that works well with the dataset of 1320 pictures and therefore the forgery detection is trained on the whole image set of the individual that is around twenty-five pictures and every time the calculations are runtime that minimizes the likelihood of error in classification. A robust and reliable signature recognition and verification system with maximum accuracy possible is very important for many purposes like enforcement, security management, and lots of business processes. It can be used as an intermediate tool to authenticate several documents like cheques, legal records, certificates, etc.The model gave encouraging results. Entirely different threshold values are used for feature matching on testing and training vectors, which helped to boost the overall performance and efficiency of the system.

The planned system is highly economical in recognizing and sleuthing the forgeries at runtime and therefore the responsibility of the system can be magnified by training the extracted features on the Artificial Neural Networks by

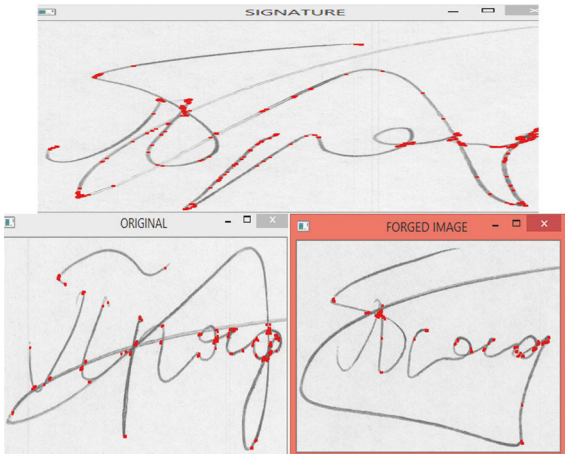


Fig. 9. Forgery Detection Using Surf Algorithm.

storing the extracted features. Negligible misclassification or error is required in such sensitive applications although it's at the cost of a High Recognition Rate (HRR). Different aim is that the probability chance of forgery signature as if it's a real one is zero. As a future work, we may also aim at increasing the resultant system accuracy by trying new and better parameter coefficients that increases the deviation between real and forged signatures.

## References

[1] Shahane P.R., Choukade A.S., & Diyewar A.N. (2015) "Online biometric authentication mistreatment Matlab." *International Journal Of Innovative analysis in Electrical, Physics, Instrumentation, and management Engineering*

[2] Zagoruyko, S., & Komodakis, N. (2015). "Learning to compare image patches via convolutional neural networks." *In Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 4353-4361).

[3] Fahmy, M. M. (2010). "Online handwritten signature verification system based on DWT features extraction and neural network classification." *Ain Shams Engineering Journal*, **1**(1), 59–70.

[4] Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). "Imagenet classification with deep convolutional neural networks." *In Advances in neural information processing systems* (pp. 1097-1105).

[5] Khalajzadeh, H., Mansouri, M., & Teshnehlab, M. (2012). "Persian signature verification using convolutional neural networks." *International Journal of Engineering Research and Technology*, **1**(2), 7-12.

[6] Batista, L., Granger, E., & Sabourin, R. (2012). "Dynamic selection of generativediscriminative ensembles for off-line signature verification." *Pattern Recognition*, **45**(4), 1326-1340.

[7] Liwicki, M., Malik, M. I., Van Den Heuvel, C. E., Chen, X., Berger, C., Stoel, R., ... & Found, B. (2011). "Signature verification competition for online and offline skilled forgeries (sigcomp2011)". *In 2011 International Conference on Document Analysis and Recognition* (pp. 1480-1484). IEEE.

[8] Arena, F., & Soares, C. G. (2009)." Nonlinear crest, trough, and wave height distributions in sea states with double-peaked spectra." *Journal of Offshore Mechanics and Arctic Engineering*, **131**(4), 041105.

[9] Zhu, G., Zheng, Y., Doermann, D., & Jaeger, S. (2008). "Signature detection and matching for document image retrieval." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **31**(11), 2015-2031.

[10] zgndz, E., Åentrk, T., & Karslgil, M. E. (2005). "Off-line signature verification and recognition by support vector machine." *In 2005 13th European Signal Processing Conference* (pp. 1-4). IEEE.

[11] Baltzakis, H., & Papamarkos, N. (2001). "A new signature verification technique based on a two-stage neural network classifier." *Engineering applications of Artificial intelligence*, **14**(1), 95-103.

[12] Justino, E. J., El Yacoubi, A., Bortolozzi, F., & Sabourin, R. (2000). "An off-line signature verification system using HMM and graphometric features." *In Proc. of the 4th international workshop on document analysis systems* (pp. 211-222).

[13] Hsiao, P. Y., Lu, C. L., & Fu, L. C. (2010). "Multilayered image processing for multiscale Harris corner detection in digital realization." *IEEE Transactions on Industrial Electronics*, **57**(5), 1799-1805.

[14] Pang, Y., Li, W., Yuan, Y., & Pan, J. (2012). "Fully affine invariant SURF for image matching." *Neurocomputing*, **85**, 6-10.