JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

HANDWRITTEN OFFLINE SIGNATURE VERIFICATION AND FORGERY DETECTION

Dr. Kusuma Kumari B.M

Assistant Professor, University College of Science, Tumkur University
Tumakuru, Karnataka- 572103,India
kusuma.kuku@gmil.com
http://tumkuruniversity.ac.in

Prof. Ramakanth Kumar .P

Professor, Department of Computer Science and Engineering, R.V. College of Engineering, Bangalore, Karnataka, India
ramakanthkp@rvce.edu.in
https://www.rvce.edu.in

Abstract

Handwritten signatures are very useful in many applications. Such as in the field of bank-cheque processing, document authentication, ATM access, etc. Simultaneous signature verification and forgery detection are also important to avoid misuse and prove the identity of the person signing the document. In this paper, we discuss how the problem has been tackled over the past few decades and analysing the latest progress in this field.

***Keywords*: offline signature; genuine; forgery; dataset; feature extraction.**

1. Introduction

For a wide variety of security applications, biometric technology is used. Recognize a person using physiological or behavioural characters is the main aim of such systems. At first, the recognition of a person based on fingerprints, face, iris, etc. is the measurement of biological qualities. Next, it is concerned with voice and the handwritten signature which belongs to behavioural characteristics [4].

Our identity is the most expensive and valuable asset in our life. With our identity, we can introduce ourselves and access our assets. For all official and legal activities, it is required to prove our identity. To confirm our identity we are producing different identity tokens like PAN cards, Aadhar Card, passports, etc., and sometimes it is required to remember passwords and some secrete PIN numbers. It is some time creates a problem, because we have lost the card or someone has stolen or duplicated the card details. Many a time we have forgotten or shared our password knowingly or unknowing. An insight solution to these problems is biometrics. All human beings are biologically unique. Thus It has made, possible to distinguish ourselves from others. Our identity is possible through some of our biological attributes and these attributes are called biometrics.

The word biometrics comes from geek words “bio” means life and “metriks” means measures. In biometrics, the person or individuals are identified through measurements of their biological attributes [4][14].
A signature is a handwritten representation of someone's name to identify a person as proof on some documents. Each person's signature is visually distinguished from others. For validating and authenticating any documents or any agreements person signatures are the standard practice [6][26].

Signature verification is a technique it is used to compare the original signatures with others sample signatures. It is used to check whether the signature under test is of the same person or not. The signature verification is done by using some kind of characteristics studies or analysis [2][5].
Signature forgery is nothing but the act of deceptively replicating another person signature. There are three types of signature forgery. They are **Random forgery, Unskilled forgery, and Skilled forgery.**

- **Random Forgery:** Random forgery signatures are less difficult to produce and the easiest forgery to detect. In this forgery, the person is going to forge but does not know the name of the original signature. The person who claims to be another signature just writes something to generate the forged signature.

- **Unskilled Forgery:** The signer forges the signature in his own style without knowing any prior experience. The signer observing the signature closely once or twice and does not have any previous experience.

Skilled Forgery: in this type, the forger copying a signature with good practice over it. The signer accesses the original signature and reproduces the forged signature after accurately practicing it. Therefore skilled forgery signatures are most difficult to detect.

2. Challenges

Offline signature verification can be said to be more challenging than online signature verification. The differences in user signatures and ease of use forgery signatures can be challenging in both cases, as dynamic information available on online signatures makes signatures more unique and more difficult to forge.

In particular, simulating both the shape and dynamic information of online signatures seems to be more difficult than simple signatures. In contrast, in some real-life situations, a fraudster can detect real offline signatures and obtain high-quality counterfeit. In addition, the availability of the signature path makes it easier for online verification systems to attach two signatures and find differences.

3. Datasets

Much research has been done on automated signature verification with private datasets and this makes it difficult to compare related work, Improvements in classification performance can be attributed to a better method or a cleaner or simpler database. Some of the offline signature databases available publicly for the research community are as shown in table 1. The process of obtaining signature images follows similar steps for most public datasets. But they all contain a limited number of signature samples, which according to researchers is not enough to develop an efficient signature verification system. The quality database of offline signatures is still required in the Offline Signature Verification field.

Forgeries storage follows a different process: users receive samples from actual signatures and are asked to simulate the signature one or more times. It is important to note that users who provide duplicates are not skilled at producing duplicates. After collecting forms, they are scanned (often at 300 dpi or 600 dpi) and pre-processed.

Database	Resolution (in dpi)	No. of sets)	Genuine Samples	Forged samples	References
GPDS-39	75	40	24	30	[11]
GPDS-100	600	100	24	24	[12]
GPDS-160	300	160	24	30	[13]
GPDS-960	300	960	24	30	[14]
MCYT-75	600	75	15	15	[15]
CEDER	600	55	24	24	[16]
4NSigComp2010	600	6	2	2	[17]

Table. 1 some available offline signature databases.

4. Pre Processing

First, collect the signatures and then perform the next step of enhancing the images of the captured signatures and preparing them for later processing. Scanned images need to be pre-processed before they can be processed. The pre-processing is done using signal processing algorithms. Pre-processing can greatly help improve feature extraction and classification performance. This reduces computational cost in classification[21][25].

According to the signature model, pre-processing operations are determined, depending on the quality of the signature image and the classification techniques to be used. It should be kept in mind that during pre-processing, information from images should not be discarded. Loss of the information in pre-processing affects the overall accuracy of the signature verification system.

Pre-processing plays an important role in signature verification. Signature images can present differences in terms of pen thickness, scale, rotation, etc., even between the official signatures of the individual.

4.1. *Noise Removal*

The scanned signature image may contain noise. The noise in the image deteriorates the feature extraction and its sequential processes. Therefore, filtering of noise is an inevitable preprocessing step in pattern recognition. It has been observed that scanned images are usually affected by salt-pepper noise. The median filter effectively removes such noise that preserves the edges of the images.

4.2. *Image Conversion*

In the case of offline signature verification, the input given to the system is a scanned signature, a form of the digital image. The first step in the given procedure is to convert this obtained RGB image into a greyscale image and again a grayscale image into a binary image. This is done to reduce the complexity and execution time of the system. The system is easier to work with binary images than RGB images.

4.3. *Image Cropping*

When scanned, the signature image contains the signature and some white unsigned areas. Cutting the image to the bounding rectangle of the signature portion removes those non-overlapping parts. The crop is the pre-processing step required for all types of classification techniques.

4.4. *Alignment*

Pairing is a common technique in online signature verification, but is not widely applicable to the offline context. Yilmaz [20] proposes to assemble signatures for training by applying rotation, scaling, and translation. Calera et al. [19] Proposed a method for generalizing rotation using the first and second-order moments of the signature image.

4.5. *Resizing*

Signature lengths are different for different signers. The lengths of a person's signature are also not equal. But when a grid-based signature verification method is used, signatures are projected onto the same size grid. Therefore, all signatures must be the same size. So in that case, resizing the signature becomes important [15]. However, resizing is not a mandatory pre-processing step for all signature verification methods.

4.6. *Edge Detection*

The purpose of detecting sharp changes in image brightness is to capture important events and changes in image characteristics. In the ideal case, the result of applying an edge detector to the image results in a set of connected curves that indicates the boundaries of the objects, the boundaries of the surface markers, and the curves corresponding to the discontinuities in the surface orientation. Therefore, applying the edge detection algorithm to the image significantly reduces the amount of data that needs to be processed and therefore filters out less relevant information while maintaining the key structural characteristics of the image. So far the canny edge detector has been found to yield good results, so canny is used in this method for edge detection.

5. Feature Extraction

Offline signature verification has been studied from many perspectives, offering many alternatives for feature extraction. At this point, a variety of features are extracted to detect the counterfeit. This step is an essential part of the computation ahead of the classification stage. It aims to extract valuable information from input images related to areas of interest.

Features extracted from an offline signature are basically classified into two categories [9], [24], [1].

- **Local Features:** Local features are extracted from a small area of a signature region. Critical, distinct parts with unique features are chosen for this. Local features are very noise-sensitive. Local feature extraction is considerably more expensive.
- **Global Features:** Global features are extracted by considering the entire signature image as a whole. Global features are easy to extract and these features are at least sensitive to noise. But global features are influenced by position alignment and are more susceptible to signature differences.

Some methods rely on learning feature representations directly from signed images. They are as follows:-

5.1. *Geometric Features*

It includes basic descriptions such as the signature's height, width, aspect ratio, and signature area. A more complex description includes counting endpoints and closed loops. In addition to using global descriptions, several authors also create local geometric

features by dividing the signature into a grid and counting the features from each cell. For example, using pixel density within grids.

5.2. *Statistical Features*

In many methods of offline signature verification, researchers have used the statistical features of the signature. They originate from the distribution of pixels in the signature image. Some of the statistical features extracted from offline signatures are, on average, the center of gravity of the signature image, the global maximum, the local maximum, and the moments. Statistical features can tolerate slight differences in signature style and ambiguity.

5.3. *Graphometric Features*

To find the authenticity and to detect forgery, the graphometry concept is used through inspecting handwriting. Some system uses graphometric features like the aspect ratio of the image, proportion, symmetry of the signature, alignment to baseline, the angular displacement to a horizontal baseline and spacing for automated signature verification.

5.4. *Extra Features*

Additional geometric features examined in this research are normalized signature area with respect to bounding box gives information about the signature density, The ratio of signature width to signature height of a cropped signature, Horizontal and Vertical center of the signature, Horizontal and Vertical Histograms, Signature height It is the height of a signature image, after width normalization, the center of Gravity or Centroid, Slope of the line obtained from curve fitting of the center of gravity of each column, center of Gravities of the vertically divided images, Skew Angle, Slope of Centre of Gravity of two equal halves of the signature image, Baseline shift or Orientation of signature.

6. Classifiers

The main purpose of comparing the performance of classifiers in the absence of targeted forgeries in the training process is to see how the involvement of targeted duplicates in the training process affects the verification accuracy.

Classifiers for signature verification can be broadly divided into two groups: writer dependent and writer-independent. First, it is more common in the literature, where a model is trained for each user, using the real signature of the user, and by using random signature duplicate real signatures from other users. At the operational stage, a trained model for claim identification is used to classify question signatures as true or forged. On the other hand, the writer-independent method involves only one classification for all users. In this case, the system learns to compare the query signature with the reference. During the test phase, the query is compared to a quote with actual samples from the person claiming to determine the signature. Some system use a combination of both approaches.

The following are the main models used for the signature verification:-

6.1. *Hidden Markov Models*

Some systems use hidden Markov models for signature verification. Hidden Markov Model (HMM) is a stochastic model matching technique that is able to absorb both the difference and the similarity between signature models. HMM has been incorporated to develop a combination of Discrete Cosine Transformation [DCT]signature features and a visual modelling framework and signature classification algorithm used by Adebayo Daramola et al [23]. The space sequence is considered in dividing the signature image into four states, regardless of the length of each signature, and the 4L-R HMM is used to model each user's signature. In the work of Justino [11], Olivera [18], and Batista [16], the signatures are divided into grids. Each column of the grid is used as an HMM view, and features are extracted from different cells within each column and subsequently standardized in the codebook.

6.2. *Support Vector Machine*

Another method for verifying signatures is based on the Support Vector Machine (SVM). The support vector machine is a new type of learning machine for model recognition and regression problems, which builds on its solution in terms of a subset of training data. Support vector machines (SVMs) have bSeen very popular for few years. They provide good results for various pattern recognition problems. SVM is mainly used in classification and regression problems. In classification, this involves assessing the decision task using a set of training data with labels that correctly classify unseen test examples. Meanwhile, for the regression, it is an approximation of real-value functions, similar to the case of model identification.

Both writer-dependent and writer-independent classification [12], [10], [7], [22], [20], [17], support vector machines are widely used for signature verification, practically one of the most efficient classifiers for the task.

6.3. *Neural Networks and Deep Learning*

The deep learning method is used for offline signature verification. Convolutional Neural Network (CNN) temporal models have been used as a deep learning method. Convolutional neural networks used are individually trained using two formats:- Writer Dependent and Writer Independent.

More recently, Solaimani et al. [3] proposed a Deep Multitask Metric Learning (DMML) system for signature verification. In this method, the system learns to compare two signatures, the distance metric between them. Signatures are processed using the Feedforward Neural Network, where the bottom layers are shared among all users (ie, the same weight is used), and the last layer is specific to each person and specializes in the individual. In the work of Rantz et al. [13], the metric learning classifier is learned, jointly learns feature representation, and the writer is independent.

6.4. *Naïve Baers Classifiers*

In the naive Bayes classification, the distribution of the two features vector distances cannot be determined. Here, each pair of bits in the test and training feature vectors is assigned as random variables. Another is that in Naive Bayes, pairs in different positions in the feature vector are equally distributed and are independent.

In the proposed system, three classifiers, i.e., one unsupervised, viz. Fuzzy C-Means (FCM) and two supervised classifiers, viz. Naive Bayes (NB) and Support Vector Machine (SVM) are used as base classifiers[8].

6.5. *Decision tree*

Decision tree is a decision support tool used in the classification of a decision analysis model or a strategy used to determine the goal. Structurally, it resembles a tree with its various decision paths or branches. Therefore, the decision tree provides intuitive visual help for gathering and analyzing data input. No prior knowledge or parameter tuning is required in the decision tree. It is more suitable for investigative knowledge discovery.

To construct the decision tree, 3 algorithms were used namely C4.5, CART, and Random Forest.

7. Future Enhancement

- To verify the signature for security, integrity, and authentication.
- Account holders signature mismatch
- To avoid proxy signature.
- To avoid forgery signatures.
- The Xerox copy signatures may not be valid(legal, financial, and Government orders). A solution can be found by generating an OTP for the all above-said problems. To avoid the above-said problems – a single source OTP can solve all.

The following problems may occur due to offline signature mismatch.

- To verify the account holder’s signature and to authenticate the bearer of the cheque, an OTP has to be generated by the software, which should be acknowledged by the account holder.
- This will double ensure the misuse of signature and some third party misusing the cheque when the cheque is misplaced or lost by the bearer.
- This will ensure if there is any slight mismatch with the original signature.
- To a great extent, the relationship between the account holder and the customer/third party will remain intact [there will be no embarrassment].
- Over a period of time, the account holder have changed the signature which leads mismatch.
- The signature may have changed due to physical conditions (overage, tension, and physical disorders (tremor)).
- To authenticate the signature sometimes thumb impressions are taken which is very cumbersome to identify and authenticate.
- When the signature mismatch, the cheque cannot be honoured.
- A known person can proxy the signature when it is simple.

- The offline signature may be forged when it is simple and if the document is misplaced or lost.
- To avoid such forgery signatures and to catch hold of the culprit,
- Such forgery will discourage such illegal activities and the finder may honestly return the document to the authority.

8. Conclusion

Researchers have proposed a variety of methods for offline signature verification. While the separation of actual signatures and skilled forgeries remains a challenging task, the error rate have declined significantly over the past few years.in this paper we have discussed about challenges, dataset used, pre-processing techniques, feature extraction and classifiers used for offline signature verification and forgery detection.

References

[1] A Aarti. Chugh, C Charu. Jain, P Priti. Singh and P Preeti. Rana, "Learning Approach for Offline Signature Verification Using Vector Quantization Technique," In the proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Emerging ICT for Bridging the Future, , 2014, vol. 1, pp. 337-344, https://doi.org/10.1007/978-3-319-13728-5_38

[2] A. J. Mauceri, "Feasibility studies of person identification by signature verification," Report No. SID 65 24 RADC TR 65 33, Space and Information System Division, North American Aviation Co., Anaheim, USA, 1965. https://apps.dtic.mil/sti/citations/AD0617615

[3] Amir Soleimani, Babak N. Araabi, and Kazim Fouladi. Deep Multitask Metric Learning for Offline Signature Verification. Pattern Recognition Letters, 80:84–90, 2016. https://doi.org/10.1016/j.patrec.2016.05.023

[4] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4–20, 2004. **DOI:** 10.1109/TCSVT.2003.818349

[5] Ankita Wadhawan and Dinesh Kumar, "Design and Analysis of Online Punjabi Signature Verification System Using Grid Optimization," In Proceedings of Second International Symposium on Security in Computing and Communications, , 2014. pp 250-262, https://doi.org/10.1007/978-3-662-44966-0_24

[6] David Fillingham, "A comparison of digital and handwritten signatures," Ethics and Law on the Electronic Frontier, vol. 6, Fall 1997. http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/fillingham-sig.html

[7] D. Bertolini, L. S. Oliveira, E. Justino, and R. Sabourin. Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. Pattern Recognition, 43(1), 2010. P- 387-396. https://doi.org/10.1016/j.patcog.2009.05.009

[8]Deka, A., and Mahanta, L. B. (2020). An Ensemble Based Offline Handwritten Signature Verification System. Statistics, Optimization & Information Computing, 8(4), 902-914. https://doi.org/10.19139/soic-2310-5070-447

[9] Donato Impedovo, and Giuseppe Pirlo, "Automatic Signature Verification: The State of the Art," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 38, no. 5, pp. 609-635, September 2008. **DOI:** 10.1109/TSMCC.2008.923866

[10] Edson J. R. Justino, Flavio Bortolozzi, and Robert Sabourin. A comparison of SVM and HMM classifiers in the off-line signature verification. Pattern Recognition Letters, 26(9):1377–1385, July 2005. https://doi.org/10.1016/j.patrec.2004.11.015

[11] Edson J. R. Justino, Abdenain El Yacoubi, Flavio Bortolozzi, and Robert Sabourin. An off-line signature verification system using HMM and graphometric features. In Fourth IAPR International Workshop on Document Analysis Systems (DAS), Rio de, pages 211–222, 2000. https://en.etsmtl.ca/ETS/media/ImagesETS/Labo/LIVIA/Publications/2000/JustinoDAS.pdf

[12] Emre Ozgunduz, TulinSenturk, and M. ElifKarsligil. Off-line signature verification and recognition by support vector machine. In European signal processing conference, , 2005. https://ieeexplore.ieee.org/abstract/document/7078479

[13] HHannes. Rantzsch, HHaojin. Yang, and CChristoph. Meinel. Signature embedding: Writer independent offline signature verification with deep metric learning. In Advances in Visual Computing. 2016. pp 616-625. https://doi.org/10.1007/978-3-319-50832-0_60

[14] K Kevin. W. Boyer, V Venu. Govindaraju and N Nalini . K. Ratha, "Introduction to the Special Issue onRecent Advances in Biometric Systems," IEEE Transaction on Systems, Man, and Cybernetics, part Biometric (Cybernetics), vol. 37, no.5, pp. 1091-1095, 2007. **DOI:** 10.1109/TSMCB.2007.903196

[15] K. N. Pushpalatha, Aravind Kumar Gautham, D. R.Shashikumar, K. B. ShivaKumar and Rupam Das, "Offline Signature Verification with Random and Skilled Forgery Detection Using Polar Domain Features and Multi Stage Classification-Regression Model," International Journal of Advanced Science and Technology, vol.59, pp. 27-40, 2013. https://www.earticle.net/Article/A205309

[16] Luana Batista, Eric Granger, and Robert Sabourin. Dynamic selection of generative–discriminative ensembles for off-line signature verification. Pattern Recognition, 45(4):1326–1340, April 2012. https://doi.org/10.1016/j.patcog.2011.10.011

[17] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira. Learning features for offline handwritten signature verification using deep convolutional neural networks. Pattern Recognition, 70:163–176, 2017. https://doi.org/10.1016/j.patcog.2017.05.012

[18] Luiz S. Oliveira, Edson Justino, Cinthia Freitas, and Robert Sabourin. The graphology applied to signature verification. In 12th Conference of the International Graphonomics Society, pages 286–290, 2005. https://www.inf.ufpr.br/lesoliveira/download/IGS2005.pdf

[19] Meenakshi K. Kalera, Sargur Srihari, and Aihua Xu. Offline signature verification and identification using distance statistics. International Journal of Pattern Recognition and Artificial Intelligence. 18(07):1339–1360, 2004. https://doi.org/10.1142/S0218001404003630

[20] Mustafa Berkay Yilmaz and BerrinYanikoglu. Score level fusion of classifiers in off-line signature verification. Information Fusion, 32, Part B:109–119, 2016. https://doi.org/10.1016/j.inffus.2016.02.003

[21] Rafael C. Gonzalez, and Richard E. Woods, Digital Image Processing (2e), Prentice Hall, 2002. https://www.abebooks.com/9780201180756/Digital-Image-Processing-2nd-Edition-0201180758/plp

[22] Rajesh Kumar, J. D. Sharma, and Bhabatosh Chanda. Writerindependent off-line signature verification using surroundedness feature. Pattern Recognition Letters, 33(3):301–308, 2012. https://doi.org/10.1016/j.patrec.2011.10.009

[23] S. Adebayo Daramola, and . T. Samuel Ibiyemi "Offline Signature Recognition using Hidden Markov Model (HMM)" International Journal of Computer Applications (0975 – 8887) Volume 10– No.2, 2010 http://eprints.covenantuniversity.edu.ng/id/eprint/6341

[24] The-Anh Pham, Hong-Ha Le and Do Nang-Toan, "Offline handwritten signature verification using local and global features," Annals of Mathematics and Artificial Intelligence, vol. 75, no.1-2, pp. 231-247, 2015. https://doi.org/10.1007/s10472-014-9427-5

[25] V. A Vinayak Ashok. Bharadi and H Hemant . B. Kekre, "Off-Line Signature Recognition Systems", International Journal of Computer Applications, vol. 1, no. 27, pp. 975-980, 2010. DOI:10.5120/499-815

[26] Warwick Ford and Michael Baum, Secure Electronic Commerce, Prentice Hall, Upper Saddle River, NJ, 1997, page 42.