

State of Art Survey Signature Verification Techniques 2019

Mitesh Parmar¹, Nupur Puranik², Dhruva Joshi³, Sonal Malpani⁴, Bhushan Thakare⁵,

Computer Department, Sinhgad Academy Of Engineering, Maharashtra, Pune, India

[1mitesh2798.mp@gmail.com](mailto:mitesh2798.mp@gmail.com) [2nupurpuranik2406@gmail.com](mailto:nupurpuranik2406@gmail.com) [3dhruvajoshi88@gmail.com](mailto:dhruvajoshi88@gmail.com)

[4sonalmalpani@gmail.com](mailto:sonalmalpani@gmail.com) [5bhushan.thakare86@gmail.com](mailto:bhushan.thakare86@gmail.com)

Abstract— Currently a lot of time is needed for the verification of signature manually. The need of developing an automated checking system is felt because of signature forgery in various transactions. The dynamic signature is a biometric trait which is used in identification. The aim of the model is identifying correct signature for reducing fraudulent transactions. The idea is to duplicate a given signature a number of times and train the verifier with each of the resulting signatures. Automatic signature verification is an application of image processing. Signature Verification can be 1) Online (Dynamic) 2) Offline (Static). For duplication of signature one approach is using the Cognitive Inspired Model. The approach for creating human like signatures can be done by introducing Intra-Component and Inter-Component variability. This system, with a single reference signature, is capable of achieving a similar performance to standard verifiers trained with up to five signature specimens. For classification classifiers like SVM, CNN can be used.

Keywords: SRSS, Cognitive Inspired Model, Signature Duplication

1. Introduction

Verifying the identity of people with their signature is an important goal in biometrics. Even in the age of iris and fingerprint detection, at some stages, signatures are needed. The need of signatures is for culturally acceptance of personal identification in wills, contracts and other important documents like cheque. The signatures of the same individual may vary little at times. So the repetition of signature from the same writer doesn't have an identical appearance. This is known as intrapersonal variability. The main limitation of current systems is that it does not have enough training sets so as to improve accuracy. The effectiveness of biometric verification is determined mainly by difference of attributes used.

For verifying signatures database of signatures with intrapersonal variability is required. This becomes difficult as it is to feasible to collect variations of a single signature. To introduce Intrapersonal Variability Cognitive Inspired Model is used. This model is inspired by working of human

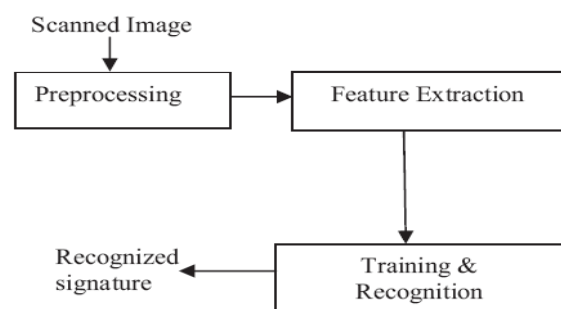
cognition. It embeds more realistic variations for signature duplication. This can be achieved by human model behaviour of signature kinematics. These parameters are useful for a design of Single Reference Signature System (SRSS) which enables the replication of signatures based on one real signature. For duplication of signatures a five step architecture is used:

- 1) Signature Segmentation
- 2) Intra-Component Variability
- 3) Component Labelling
- 4) Inter-Component Variability
- 5) Signature Inclination.

The results obtained using this method are significantly used for verification. Support Vector Machine can be used for classification, if the signature is forged or authorized.

2. Motivation

The need for signature authentication is necessary due to increased rates in forgery. As the use of cashless transactions is increasing in banking sector it is the need of the hour to increase security by authenticating the process. A lot of discovery is in process in this field. The use of Image Processing for verification can be made better with increasing accuracy which can be helpful to reduce forgery transactions.



Authors	Main Features	Database	Approach	Results/Conclusions
Moises Diaz et al[1]	Neuromuscular Model, Sigma-Lognormal Model	SUSIG-Visual Sub-corpus, SUSIG-Blind Sub-corpus, SVC-Task1 Sub-corpus, SVC-Task2 Sub-corpus, MCYT100 Sub-corpus, SG-NOTE Database	Dynamic Time Warping(DTW), Manhattan Distance Based Verifier, Hidden Markov Model(HMM)	False Rejection Rate(FRR):2.15 False Acceptance Rate(FAR):2.10
Kamlesh Kumari , et al[10]	Discrete Cosine Transform, Linear discriminant analysis, SURF	Region Based Signature Database	Neural Networks, HMM	Dynamic features cannot be extracted.
Moises Diaz et al[9]	Cognitive Inspired Model, Intra component and inter component variability	GPDS-300, MYCT-75	Support Vector Machine(SVM), HMM	FRR: 1.9%
Moises Diaz et al[8]	Cognitive inspired duplicate model, Bresenham Line drawing algorithm, Local Binary pattern, Local Derivative pattern.	MCYT	HMM	Improves the accuracy
Anastasia Beresneva et al[7]	Discrete Wavelet Transform, Discrete Fourier Transform	Local database	HMM	K-Nearest Neighbour (KNN) performs better.
Miguel A. Ferrer et al[3]	Cognitive Model, Neuromotor Model	Synthesizer Data Set, MCYT330,NISDCC, SVC2004, SUSIG BLIND, SUSIG VISUAL	HMM,SVM,DTW	HMM performs better.

Mohsen Fayyaz et al[14]	Broyden–Fletcher–Goldfarb–Shannoalgorithm, Autoencoder	SVC2004, SVS2004	SVM	Equal Error Rate(EER) is reduced.
Syed Khaleel Ahmed et al[11]	Dynamic Feature Extraction, Self Organization Map(SOM)	Local Database	NN	FAR: 5.17% FRR: 31.33%
Napa Sae Bae et al[15]	Histogram Feature Extraction, User Template Generation, Manhattan Distance	MCYT-100, SUSIG	HMM	FAR: 4.66%
B.S Thakare, H.R Deshmukh[15]	SIFT,LBP for feature extraction, Computer Vision	GPDS-300	Markov Random Model	FRR: 16.62% FAR: 14.33
Bhushan S. Thakare,Dr. H.R. Deshmukh[12]	Simulated annealing	CPDS & CEDAR	SVM	FRR: 17%
Zhihua Xia et al [2]	Two step verification	SGNOTE, MCYT-100	K-Nearest Neighbour (KNN)	2 step verification improves the accuracy
Luiz G. Hafemann et al. [16]	LBP gradient, Simulated annealing. FGM - Fast gradient method, CNN Signet for feature extraction	MCYT,CEDAR, GPDS-160	SVM	FAR: 4.5 % FRR: 4.36%

Taraggy. M. Ghanim et al.[17]	HOG,Random Classifier, Bagging Tree Classifier	Local Database	SVM	FRR: 6%
YasmineSerdouk et al.[18]	Conventional Artificial Immune Recognition System for classification, Gradient local binary pattern for signature characterization	CEDAR, GPDS-300	SVM classifier	CEDAR: FAR:19.60% FRR:8% GPDS-300: FAR:30.69% FRR:9.16%
Victor K.S.L. Melo1 et al[19]	Leaky rectified linear units as activation function	IRONOFF-300	Full Convolutionary Neural Network(CNN)	
Songxuan Lai et al.[20]	1. DTW 2. Gated Auto Regressive Units (GARU)	MYCT-100	Recurrent Neural Network (RNN)	
BiswajitKar et al.[6]	1. Skeleton tree matching. 2. Dynamic time warping. 3. Gaussian mixture model.	MCYT -100 for skilled forgery	SVM	1.0% EER

3. CONCLUSION

Automatic Signature Verification is a very advancing field and has huge scope in real world. With the continuous growth of Internet online verification systems are in dire need. Even though features of iris detection, fingerprints are used for verification, signatures still play a vital role in case of legal documents, cheques, contracts. Physical biometrics doesn't require active involvement as it does in the process of signing. Authentication is required of the signatures being real. Thus this increases security level. Online signature

verification has important applications in online banking, monetary transactions, and retail POS. Offline signature verification applications mainly concern the authentication of bank checks, contracts, ID personal cards, administrative forms, formal agreements. Considering the intrapersonal variability the minute changes are observed in signatures of the same person. This needs to be evaluated and a real signature must not be considered are forged. Also, it isn't feasible to collect multiple real signatures. This needs a

solution which is it can be duplicated on One Real Time Signature. The purpose is to detect forge signatures which is of utmost importance in online as well as offline transactions. As research is continuously in process, the need of development of the most optimal model is required.

REFERENCES:

- 1) Moises Diaz, Andreas Fischer, Miguel A. Ferrer, and Réjean Plamondon, Dynamic Signature Verification System Based on One Real Signature”, 2168-2267 _c 2016 IEEE
- 2) Zhihua Xia, Tuanjia Shi , Neal N. Xiong, Xingmuing Sun, Byeungwoo Jeun, “A Privacy-preserving handwritten signature verification method using combinational features and secure KNN”
- 3) Miguel A. Ferrer, Moises Diaz, Cristina Carmona-Duarte and Aythami Morales “A Behavioral Handwriting Model for Static and Dynamic Signature Synthesis” 0162-8828 (c) 2016 IEEE.
- 4) Andreas Fischer, Member, IEEE, and R´ejean Plamondon, Fellow, IEEE “Signature Verification Based on the Kinematic Theory of Rapid Human Movements” 2168-2291 © 2016 IEEE.
- 5) Moises Diaz, Andreas Fischertt, Rejean Plamondon and Miguel A. Ferrer “Towards an Automatic On-Line Signature Verifier Using Only One Reference Per Signer” 2015 13th International Conference on Document Analysis and Recognition (ICDAR).
- 6) Biswajit Kar, Anirban Mukherjee , and Pranab K. Dutta “Stroke Point Wrapping-Based Reference Selection and Verification of Online Signature” 0018-9456 © 2017 IEEE.
- 7) Anastasia Beresneva, Anna Epishkina, Darina Shingalova “Handwritten Signature Attributes for its Verification” 978-1-5386-4340-2/18/\$31.00©2018 IEEE .
- 8) Moises Diaz-Cabrera, Miguel A. Ferrer, Aythami Morales “Cognitive Inspired Model to Generate Duplicated Static Signature Images” 2167-6445/14 \$31.00 © 2014 IEEE.
- 9) Moises Diaz, Miguel A. Ferrer, Eskander, Robert Saburin “Generation of Duplicated Offline Signature Images for Verification Systems” 0162-8828© 2016 IEEE.
- 10) Kamlesh Kumariand, V.K.Shrivastava “Factors Affecting The Accuracy of Automatic Sugnature Verification” 978-9-3805-4421-2/16/\$31.00 ©2016IEEE
- 11) Syed Khaleel Ahmed, Member IEEE; Agileswari K. Ramasamy; Anis Salwa Mohd. Khairuddin and Jamaludin Omar, Member IEEE “Automatic Online Signature Verification: A Prototype Using Neural Networks” 978–1–4244–4547–9/09/\$26.00© 2009 IEEE.
- 12) Bhushan S. Thakare, Dr. Hemant R. Deshmukh “A Novel End-To-End Approach For Offline Signature Verification System” 978-1-5386-4273-3/18/\$31.00 ©2018 IEEE
- 13) Mohsen Fayyaz, Mohammad HajizadehSaffar, MohammadSabokrou, M. Hoseini and M. Fathy “Online Signature Verification Based on Feature Representation” 978-4799-8818-1/15/\$31.00 ©2015 IEEE.
- 14) Napa Sae-Bae and NasirMemon, Fellow, IEEE “Online Signature Verification on Mobile Devices” 1556-6013 © 2014 IEEE.
- 15) Bhushan S. Thakare, Dr. Hemant R. Deshmukh “A combined feature extraction model using SIFT and LBP for offline signature verification system” 978-1-5386-4273-3/18/\$31.00 ©2018 IEEE
- 16) Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira “Characterising and Evaluating adversarial examples for Offline Handwritten Signature Verification”.
- 17) Taraggy M. Ghanim,Ayman M. Nabil “Offline Signature Verification and Forgery Detection Approach” 978-1-5386-5111-7/18/\$31.00 ©2018 IEEE.
- 18) YashmineSerdouk, HassibaNemmourand YoucefChibani “An Improved Artificial Immune Recognition System for Off-line Handwritten

Signature Verification” 978-1-4799-1805-8/15/\$31.00(c) 2015 IEEE.

- 19) Victor K.S.L Melo, Byron LeiteDantasBezerra, DonatoImpedovo,GiuseppaPirlo ,Antonio Lundgren “Deep Learning Approach to Generate Offline Handwritten Signatures based on Online samples” IET Biom., 2019, Vol. 8 Iss. 3, pp. 215-220.
- 20) Songxuan Lai, LianwenJin “Recurrent Adaption Networks for Online Signature Verification” 1556-6013 (c) 2018 IEEE