Online Signature Profiling Using Generative Adversarial Networks

Chandra Sekhar Vorugunti
IIIT SriCity
Chittoor-Dt, 517 646
Andhra Pradesh, India
Chandrasekhar.v@iiits.in

Prerana Mukherjee
IIIT SriCity
Chittoor-Dt, 517 646
Andhra Pradesh, India.
prerana.m@iiits.ac.in

Viswanath Pulabaigari
IIIT SriCity
Chittoor-Dt, 517 646
Andhra Pradesh, India.
viswanath.p@iiits.ac.in

Abstract— **A signature is an ability learned by humans from an elementary age. The skill to generate one's own exclusive signature along with imitating another writer's signature is a challenging and complex task. In real time scenarios like E-Commerce and M-Commerce payments, user verification based on online signatures constrain the verification framework needs to be trained extensively with huge samples, which unfeasible to obtain. Hence, as a solution, in this paper, we propose 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.**

Keywords—GAN, Online Signature Verification, User Profiling

I. INTRODUCTION

Biometric technology is extensively used as a security tool in a variety of real time deployments to classify the user trying to login into the system as genuine or forged. Specialized devices like Wacom signature pads are used to capture the user signatures. The device returns spatial coordinates (x, y) and dynamic features (pressure, velocity, azimuthal angle, etc.) at each point of writer's signature [1,2]. The biometric based real time online signature verification systems require huge amount of training on online signatures. Capturing the vast number of online signatures specific to each user is impractical. The frameworks trained with lesser samples will have a downgrade performance on the classification accuracies of user test signatures. To address the challenge of shortfall in amount of real time signatures of writers, we have proposed an intelligent framework tries to artificially synthesize writer specific online signatures using a fully connected network based Generative Adversarial Networks (GANs).

In literature very few works are proposed based on artificial synthesize of writer specific online signatures. Galbally et al [1] put forward an Online Signature Framework (OSV) based on a single real signature sample, synthetic samples are generated using HMM models. Diaz et al [2] put forward a novel OSV model in which a random noise is induced into the into the genuine signature of a user, which injects distortion in the signature. Based on these distortions, the synthetics samples are generated. The subsequent contribution is by Diaz et al [3], in which using one signature sample, duplicate set of signature samples are generated by extracting sigma-lognormal parameters build on the kinematic theory of fast hand movements. The framework reaches out an Equal Error rate (EER) of 13.56%. Very recently, Diaz et al [4] put forward an OSV framework in which fake signature samples are produced based on simulating the architecture of realarm and forearm movements using virtual skeletal arm (VSA) model which outputs anthropomorphic features, which used for fake signature generation.

All these models are based on neuro muscular and kinematic theory of rapid hand movements. The neuro movements are not constant and varies with respect to the mood of the writer and doesn't reflect the writer characteristics effectively. All these above models are based on six Sigma-Lognormal parameters [3] $P_i = (D_i, t_{o,} \mu_i, \sigma_i, \theta_s, \theta_{ei})$, computed at each stroke point of the signature. Hence, these modes are highly computational, which makes them inefficient for real time deployments. In addition to the above, all these frameworks are supervised, which requires labelling for the signatures. Therefore, as a solution to the above pitfalls, we are proposing 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) in an unsupervised manner. In our proposed framework, an online signature is represented as 1*3 vector.

II. PROPSOED ONLINE SIGNATURE GENERATION MODEL

As depicted in Fig 1 and Fig 2, the proposed Online Signature Generation framework is a combination of two sub-models: a generator and discriminator. The generator, a fully connected model with three hidden layers, takes a fixed-length random vector of size 3, drawn randomly from a Gaussian distribution as a seed or source of noise. On inputting the noise vector, the generator generates the new synthetic signature samples from the problem domain (dataset) by automatically discovering and learning the regularities or patterns of user signature. The discriminator model takes an input signature either from the problem domain (real) or from the generator (fake) and classifies the genuineness of the input signature. The discriminator model efforts to lessen the 'binary cross-entropy' loss function, and the 'Adam' is used as an optimizer. Based on the resultant error of the discriminator, the weights of a generator are updated. The architecture specifics of generator and discriminator are specified in the table below.

TABLE I. ARCHITECTURE DETAILS OF GENERATOR (G) AND DISCRIMINATOR (D)

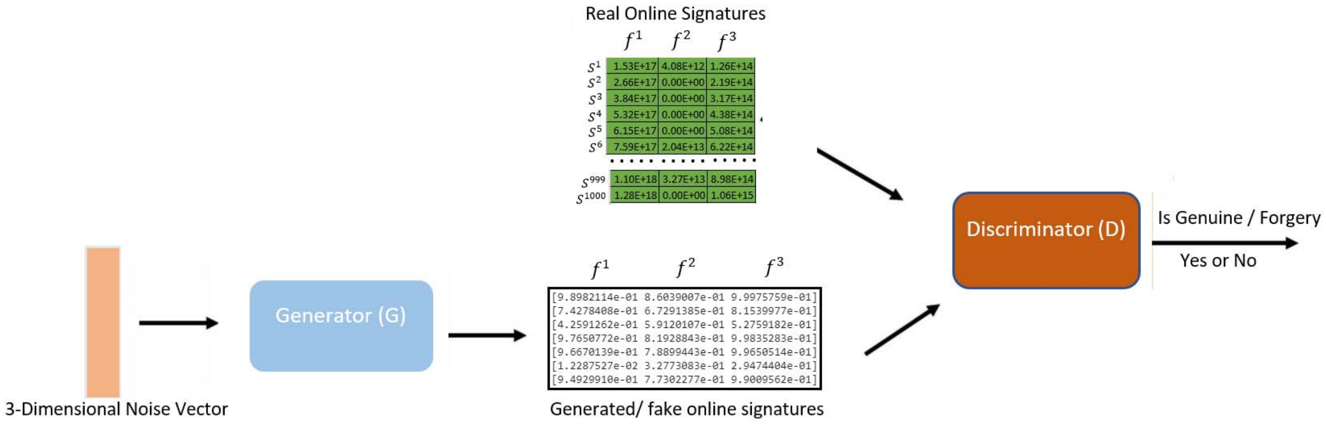
Layer Number	Number of Nodes	Activation Function	Kernel and Bias Iniializer
1 (Input)	25	Leaky Relu (0.01)	he_uniform
2	15	Leaky Relu (0.01)	he_uniform
3	10	Leaky Relu (0.01)	he_uniform
4	5	Leaky Relu (0.01)	he_uniform
5 (Output)	G = 3, D=1	Sigmoid	

As depicted in Fig 2, the generator and discriminator models are stacked such that, the random points in the latent space forms an input to the generator, which outputs fake signature samples of size 3. The fake samples form an input to the

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

978-1-7281-3187-0/20/$31.00 ©2020 IEEE

discriminator for classification. Accordingly, the weights of a generator are updated.



	f^1	f^2	f^3
s^1	1.53E+17	4.08E+12	1.26E+14
s^2	2.66E+17	0.00E+00	2.19E+14
s^3	3.84E+17	0.00E+00	3.17E+14
s^4	5.32E+17	0.00E+00	4.38E+14
s^5	6.15E+17	0.00E+00	5.08E+14
s^6	7.59E+17	2.04E+13	6.22E+14
s^{999}	1.10E+18	3.27E+13	8.98E+14
s^{1000}	1.28E+18	0.00E+00	1.06E+15

f^1 f^2 f^3

```
[9.8982114e-01 8.6039007e-01 9.9975759e-01]
[7.4278408e-01 6.7291385e-01 8.1539977e-01]
[4.2591262e-01 5.9120107e-01 5.2759182e-01]
[9.7650772e-01 8.1928843e-01 9.9835283e-01]
[9.6670139e-01 7.8899443e-01 9.9650514e-01]
[1.2287527e-02 3.2773083e-01 2.9474404e-01]
[9.4929910e-01 7.7302277e-01 9.9009562e-01]
```

Figure 1. General architecture of the proposed GAN based framework for generating duplicated signature samples.

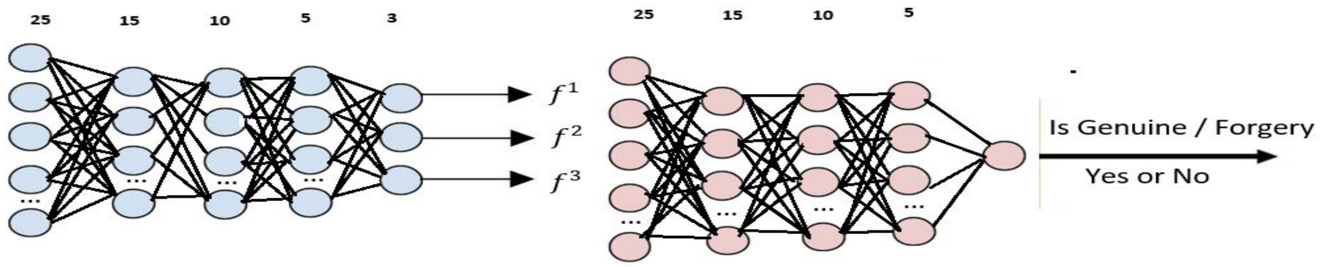


Figure 2. The Fully Connected Layered based Generator and Discriminator networks of the proposed GAN based framework.

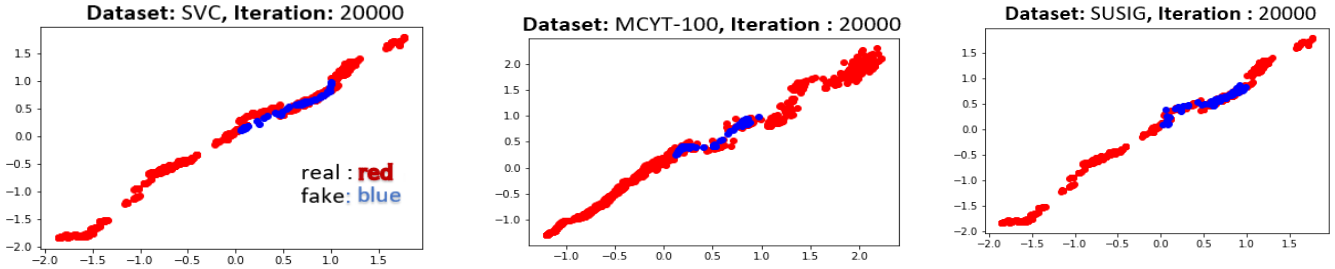
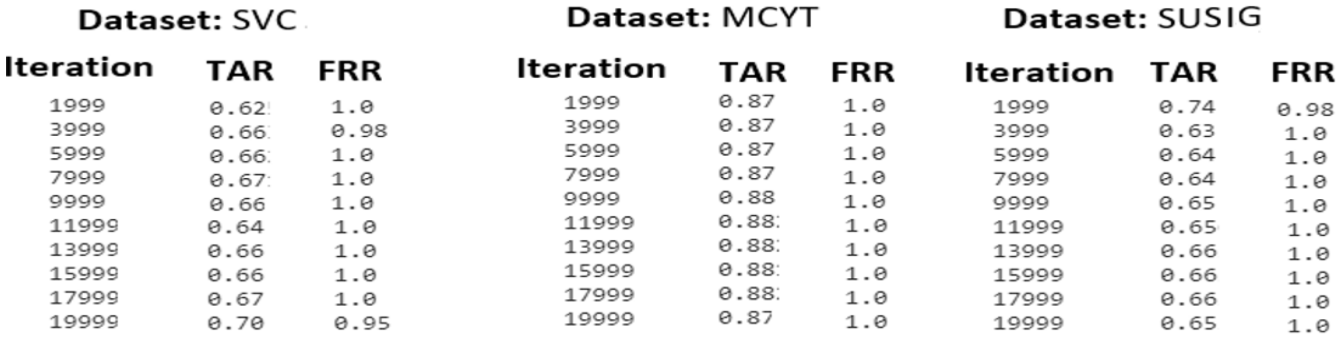


Figure 3. The performance of the discriminator of the proposed framework at 20000th iteration.

III. Experimental Analysis

To evaluate the proposed GAN based signature generation framework, we ran our preliminary experiments on three widely used datasets i.e. MCYT-100 [4], SVC [1,5], SUSIG [1,4]. The reader is requested to refer Sekhar et al [9] for more information on about the individual dataset. We have experimented our proposed signature framework in an Ubuntu based GTX1080 GPU machine with 120GB memory. The code is written by using keras API deep learning platform with Python 3.3 version. We have trained the model for 20000 epochs, in each epoch we have trained the model with 64 real signature samples from the corresponding dataset and 64 fake samples generated by the generator. For a set of real signature samples, we have taken 1000 random samples, each of size 1*3 from corresponding datasets and fed to a generator. The Generator outputs a synthetic signature samples of size 1*3. The synthetic signature samples form an input to the discriminator, which outputs the classification result i.e. real or fake. After 2000 epochs, we plotted the curves which are illustrated in fig 3-5. The x-axis and y-axis represent the input domain. The input domain is of two types positive and negative. Fig 3 illustrates that, in all the three datasets, there is overlapping of fake images with real images, which confirms the efficiency of the generator model in generating synthetic samples. Fig 4, illustrates the efficiency of discriminator in detecting the genuine and forgery signatures. The column 1 signifies the iteration count, the second column signifies the True Acceptance Rate (TAR), i.e. classification accuracy of real signature samples. The third column signifies the False Rejection Rate (FRR), i.e. classification accuracy of fake signature samples. In all the three datasets, discriminator remains very stable in classifying the signatures. In case of MCYT and SUSIG, the discriminator achieved 100% accuracy and 95% with respect to SVC in detecting the fake



Dataset: SVC			Dataset: MCYT			Dataset: SUSIG		
Iteration	TAR	FRR	Iteration	TAR	FRR	Iteration	TAR	FRR
1999	0.62	1.0	1999	0.87	1.0	1999	0.74	0.98
3999	0.66	0.98	3999	0.87	1.0	3999	0.63	1.0
5999	0.66	1.0	5999	0.87	1.0	5999	0.64	1.0
7999	0.67	1.0	7999	0.87	1.0	7999	0.64	1.0
9999	0.66	1.0	9999	0.88	1.0	9999	0.65	1.0
11999	0.64	1.0	11999	0.88	1.0	11999	0.65	1.0
13999	0.66	1.0	13999	0.88	1.0	13999	0.66	1.0
15999	0.66	1.0	15999	0.88	1.0	15999	0.66	1.0
17999	0.67	1.0	17999	0.88	1.0	17999	0.66	1.0
19999	0.70	0.95	19999	0.87	1.0	19999	0.65	1.0

Figure 4. The TAR and FAR performance of the discriminator of the proposed framework.

signatures. In case of MCYT, the discriminator achieved an accuracy of 88% in detecting the genuine signatures. In case of SVC, the discriminator achieved a very decent accuracy of 70% in detecting the real signature samples

IV. Comparision Study

The proposed GAN based online signature verification framework is a first of its kind work, hence, no comparison work in online signature is available, for brevity we compare the proposed work with latest OSV frameworks.

TABLE II. COMPARISION OF EER (%) VALUES WITH RECENT OSV FRAMEWORKS.

MCYT-100	
Method	**RF-EER**
Histogram+Manhattan [3]	1.15%
Duplicated + DTW [4]	6.60%
□**Λ** + DTW [5]	1.01%
Symbolic Rep [6]	2.40%
VSAr + DTW [8]	0.75%
VSA + DTW [8]	0.80%
Proposed: GAN+OSV	**0.0%**

SUSIG	
Method	**RF-EER**
Fuzzy modelling [2]	4.57%
Histogram+Manhattan [3]	2.91%
Duplicated + DTW [4]	6.60%
□**Λ** + DTW [5]	1.48%
VSAr + DTW [8]	0.78%
VSA + DTW [8]	0.78%
Proposed: GAN+OSV	**0.0%**

The above Tables confirm that the proposed GAN based online signature verification model surpassed the latest OSV frameworks. We have compared our model with other frameworks in Random Forgeries [9] and the point at which the False Acceptance Rate and False Rejection Rate is computed (Equal Error Rate-EER). The outcomes confirm the potential of the framework in classifying the real and fake signature samples. In future work, we try to outspread the proposed model by evaluating it with additional datasets and all possible categories of experimentation.

V. Conclusion

Our OSV model is proposed to address the data scarcity problem of online signature verification. To generate synthetic signature samples, we have used a Generative Adversial Networks, in which a generator model learns to generate the fake samples from the resultant error of discriminator. Finally, the experimental analysis proved that, GANs attain human-like behaviour in complex activities like online signature verification. The model achieved higher classification accuracies in discriminating the real and fake samples. We have evaluated the proposed model, our proposed model achieved best results compared to the current state of the art models.

Acknowledgements. The work reported in this paper is partly funded by a DIC funded project with reference DIC Proj14 PV. Partly from IIIT SriCity seed grant on writer recognition.

References

[1] J. Galbally, J. Fiérrez, M. Diaz, and J. O.Garcia, “Improving the enrollment in dynamic signature verfication with synthetic samples,” in Int Conf on Doc Anal. Recognit. (ICDAR), pp. 1295–1299, Barcelona, Spain, 2009.

[2] A. Ansari, M. Hanmandlu, J. Kour, and A. Singh, “Online signature verification using segment-level fuzzy modelling,” IET Biometrics, vol. 3, no. 3, pp. 113–127, 2014.

[3] N. Sae-Bae and N. Memon, “Online signature verification on mobile devices,” IEEE Trans. on Information Forensics and Security, vol. 9, no. 6, pp. 933–947, 2014.

[4] M. Diaz, A. Fischer, R. Plamondon, and M. A. Ferrer, “Towards an automatic on-line signature verifier using only one reference per signer,” in Int. Conf. Document Anal. Recognit. (ICDAR), Tunis, Tunisia, pp. 631–635, 2015.

[5] A. Fischer and R. Plamondon, “Signature verification based on the kinematic theory of rapid human movements,” IEEE Trans. On Human-Machine Systems, vol. 47, no. 2, pp. 169–180, April 2017.

[6] D. Guru, K. Manjunatha, S. Manjunath, and M. Somashekara, “Interval valued symbolic representation of writer dependent features for online signature verification,” Expert Systems with Applications, vol. 80, pp. 232–243, 2017.

[7] M.Diaz, A.Fischer, M. A. Ferrer and R.Plamondon, Dynamic Signature Verification System Based on One Real Signature, IEEE Trasactions On Cybernetics, vol 48, Jan 2018.

[8] M.Diaz, M.A. Ferrer and J.J.Quintana, Anthropomorphic features for On-line Signatures, IEEE Transactions on Pattern Anaysis and Machine Intelligence, pp:2807 - 2819.,vol 41, Dec 2019.

[9] V.C.Sekhar, P.Mukherjee, D. S. Guru, V.Pulabaigari, Online Signature Verification Based on Writer Specific Feature Selection and Fuzzy Similarity Measure, WORKSHOP ON MEDIA FORENSICS, CVPR, PP:88-96, 2019.