

Generative Adversarial Network (GAN): Discriminator Model for Online Signature Verification

Vishwas Karhadkar¹, Dr. Hemant Makwana²

¹Ph.D scholar, Computer Engineering, IET- DAVV, Indore, India

²Professor, Department of IT, IET -DAVV, Indore, India

HOW TO CITE:

Vishwas Karhadkar, Hemant Makwana (2026). Generative Adversarial Network (GAN): Discriminator Model for Online Signature Verification. International Journal of Special Education, 41(13s), 656-665

ABSTRACT:

The rapid development of modern secure authentication system plays significant roles over traditional mechanism like enable password, PIN, code and tokens. Conventional mechanism has possibility of loss, theft or misuse. Today, modern biometric, behavioural and physiological systems are alternative for robust authentication. In addition, online signature authentication has become popular due to time based features like velocity, pressure and stroke sequence which is difficult to forge. Existing approaches to online verification encompass statistical models, template matching, and machine learning techniques, including Hidden Markov Models (HMMs), Support Vector Machines (SVMs), and neural networks. Recent advancements in deep learning have further enhanced accuracy and robustness in signature-based authentication.

In this paper, the application of Generative Adversarial Networks (GANs) for online signature verification using the SVC 2004 dataset is explored. GANs consists of two neural networks architecture which are generator and discriminator that able to generate synthetic signature and its verifications. The discriminator of GANs is reliable component to distinguish real and fake signatures. Through the combining of GAN architecture concepts that offers reliable scalable and secure authentication.

Keywords: Security Issues, Authentication Techniques, Signature Authentication, Artificial Intelligence, Generative Adversarial Network (GAN), SVC 2004 Data Set.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In digital world, IT organization requires trusted and strong authentication techniques. Traditional authentication techniques depend on passwords, PIN code, onetime password (OTP), physical cards that may be compromised. Alternatively, biometrics is another technique of

authentication. Biometric authentication involves physiological or behavioural characteristics of person for identity verification [1]. It avoids the weakness of traditional authentication techniques. It advantages over compromise or stolen of password or PIN. It may be categorized into physiological and behavioural categories. Physiological biometrics

deals with human biological factors like fingerprint, iris patterns etc. Inversely, behaviour biometric deals with tracking user activities or behaviour. From the different factors of biometric authentication process, signature verification is the most accepted behavioural authentication. Further, it is classified as static (offline) and dynamic (online) methods. Offline signature verification applies geometric properties of the signature to verify the signatory authority. Contrary, online signature verification method uses time based factors to verify the signatory. Now days, electronics devices with integrated pen input ability are increasing rapidly like Personal Digital Assistants, and tablet PCs. These developments have encouraged significant research endeavours over the past decade in the realm of dynamic or online signature verification, as comprehensively reviewed in [2].

Emerging field of artificial intelligence i.e. Generative Adversarial Network (GAN) is able to generate and verify images which are not real images. Though GAN may also use in online signature authentication. GANs consist of two neural networks. First is a generator which generate synthesize images from noise sample image dataset. Second is a discriminator is distinguishing real image and generated synthesize images The loss function defines the performance of the generator that impose penalties when it fails to deceive the discriminator. Numerous research articles have introduced GAN-based techniques for signature generation. These investigations influence GANs for augmenting signature datasets or enhancing verification systems through the application of their discriminator.

2. Background

Two methods are employed in the realm of online signature verification to ensure the security and authenticity of signatures [3]. For the purpose of achieving precision, handwritten verification scrutinizes either dynamic attributes (such as velocity or pressure) or static characteristics (such as dimensions or shape). To achieve digital signature authentication, a cryptography and Public Key Infrastructure

(PKI) [4] is used. Dynamic or online signature authentication accomplishes biometric verification [5] method which verifies user identity via behaviour feature of their handwritten signatures. Inversely, offline signature authentication methods analyse image of signatures. Online method concentrates signature device speed, pressure, acceleration, stroke sequence, and duration. Another work on online signature authentication done in [6] which present efficient and secure verification process with several benefits. One of its fundamental benefits is enhanced security, as dynamic parameters such as velocity, pressure, and stroke order are significantly more challenging to replicate compared to static signature data. Consequently, it emerges as a more reliable alternative for identity validation. Furthermore, this technology enables real-time verification, thereby expediting decision-making processes and facilitating immediate processing. In comparison to other biometric systems, such as fingerprint or iris recognition technologies, it generally necessitates less expensive hardware, rendering it a cost-effective solution.

To accomplish feature based authentication it includes pen pressure, stroke path, velocity and acceleration. Subsequently, these features are compared to the reference signature through techniques such as Euclidean distance and Dynamic Time Warping (DTW) [7].

Another technique is template based authentication that process many samples of real signature data to make a reference point. This take advantages of modern AI techniques such as neural networks and Hidden Markov Models (HMM) [8]. Neural networks [19] analyse the complex interrelations among the dynamic data, whereas HMM employs a probabilistic framework to model the sequential transitions of pen strokes.

As the evolution of AI, machine learning based authentication techniques have gained importance. Few techniques are Random Forests, Support Vector Machines (SVM) [7], Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) [8].

At last, statistical based methods like Bayesian classifiers and Gaussian Mixture Models (GMM) [7] use probability to find closest value of test signature for checking which class it belongs.

3. Related Work

The classification of online authentication methods happened based on feature selection techniques with representation method. The excess of unique features that advised for signature pattern representation have classified into local or global representations. As an example of signature authentication system which built based on global feature [9] [10]. The global feature reduces authentication process duration, whereas the efficiency of system that integrate local feature to be higher [11]. Ultimately, local feature based signature authentication system is addressed in [2]. Further, various system merged global and local features that addressed in [12] [13]. An authentication system also classified based on template matching and statistical methods. The common method based on template matching is dynamic time warping (DTW) [14] [15]. Alternately, few methods have suggested based on regional correlation and skeletal tree matching [16]. Based on statistical method, several methodologies demonstrated in [17][18] that adopt support vector machine method. Moreover, some methods based on hidden Markov models (HMMs) (US-HMMs) or Gaussian mixture models (US-GMMs) presented in [19][20]. A critical component in generative model-based signature verification systems is the normalization of the verification score [21] [22]. Universal background models (UBMs) have been utilized independently for score normalization

and user model generation within GMM-based systems [20] [23]. The user models are developed from the outset utilizing user signatures, thereby rendering the UBM applicable solely for the purpose of score normalization [20]. Whereas in [23], the UBM serves a dual role for both user model adaptation and score normalization, albeit it relies on global characteristics of the signature, which ultimately diminishes verification performance. More recently, the user-adapted UBM (UA-UBM) system introduced [24] has also employed UBMs for both model generation and score normalization within HMM-based online signature verification utilizing time sequences: User models are generated through the adaptation of UBM parameters to the enrollment data via maximum a posteriori (MAP) adaptation. The verification score is computed as the signature log-likelihood ratio between the user model and the UBM. Another significant advancement in HMM-based signature verification is the integration of the Viterbi path into the verification process, as demonstrated in references [16] and [25]. Verification evidence derived from the Viterbi path can be implemented in any HMM-based system, including the UA-UBM framework proposed in reference [25].

4. Methodology

To accomplish online signature verification, a discriminator component of generative adversarial network has implemented on SVC 2004 signature data set. The procedure of utilizing a Generative Adversarial Network (GAN) for signature verification is accomplished in various steps which shown in figure 1.

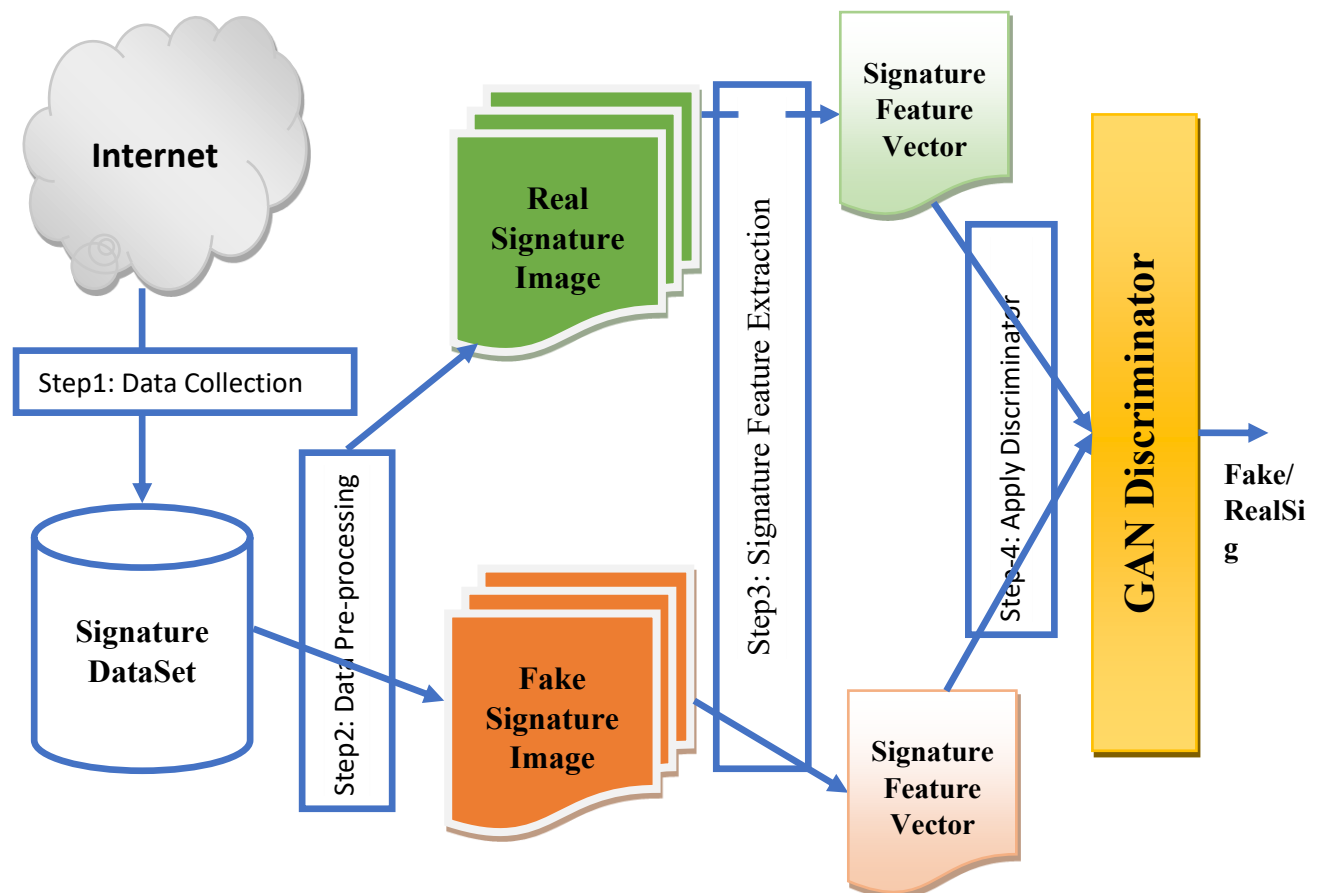


Figure-1: Methodology workflow

Step-1: Data Collection- The data set of authentic and falsified signatures i.e. SVC 2004 extracted.

Step-2: Data pre-processing: Data pre-processing involves data cleaning process to improve data quality that leads model accuracy.

Step-3: Feature extraction- Model is trained using selection of feature extraction.

Step-4: GAN Discriminator: For the detection of real or fake signature, discriminator is implemented.

Step-5: Signature Matching- To verify authenticity, the characteristics of real signature is evaluated.

Step-6: Analyse Model: To make sure the GAN is effective, use metrics to measure its performance.

Step-7: Deploy System: For automatic signature verification, implement the trained GAN in a real-time system.

5. Implementation

The GAN is implements on SVC 2004 signature data set. Experiment is accomplished using Google colab GPU and python 3.13 version. The data set comprises of feature vector of signature images. The sample data of SVC 2004 shows as:

Line	Col	Character
170	1	h70
2280	7111	75748770 0 1310 680 244
2252	7058	75748780 1 1320 650 247
2207	6996	75748790 1 1300 630 247
2185	6857	75748800 1 1310 610 245
2178	6662	75748810 1 1290 600 287
2173	6429	75748820 1 1280 580 344
2173	6121	75748830 1 1280 570 425
2173	5747	75748840 1 1260 560 485
2178	5328	75748850 1 1250 550 515
2190	4901	75748860 1 1240 540 537
2206	4574	75748870 1 1220 540 554
2227	4314	75748880 1 1200 540 562
2252	4106	75748890 1 1170 550 568
2276	3984	75748900 1 1160 550 562
2290	3920	75748910 1 1130 560 565
2296	3920	75748920 1 1120 560 565
2286	3974	75748930 1 1100 560 548
2259	4070	75748940 1 1070 570 522
2220	4302	75748950 1 1060 570 504
2185	4615	75748960 1 1040 570 496
2156	4981	75748970 1 1030 570 490
2156	5417	75748980 1 1030 570 490
2177	5814	75748990 1 1030 570 490
2229	6186	75749000 1 1020 560 486
2307	6514	75749010 1 1020 560 449
2401	6762	75749020 1 1040 560 438
2507	6957	75749030 1 1050 560 440
2616	7082	75749040 1 1080 560 441
2727	7146	75749050 1 1110 550 441
2826	7170	75749060 1 1130 560 448
2927	7133	75749070 1 1150 550 448
3031	7019	75749080 1 1170 550 464
3134	6853	75749090 1 1190 540 496
3203	6662	75749100 1 1220 540 515

Figure-2: SVC 2004 Signature Data Sample

The pseudocode for the GAN discriminator implementation is described as follows.

Pseudocode

<pre> CLASS Discriminator(input_dim) METHOD INIT(input_dim) model ← SEQUENCE(LINEAR(input_dim, 256), RELU, LINEAR(256, 128), RELU, LINEAR(128, 1), SIGMOID) END METHOD METHOD FORWARD(x) RETURN model(x) END METHOD END CLASS </pre>	<pre> // Step 2: Train Discriminator </pre>
<pre> MAIN PROGRAM </pre>	<pre> optimizer_D.ZERO_GRAD() d_loss_real ← loss_function(discriminator.FORWARD(real_sam ples), real_labels) d_loss_fake ← loss_function(discriminator.FORWARD(fake_sam ples), fake_labels) d_loss ← d_loss_real + d_loss_fake BACKPROPAGATE(d_loss) optimizer_D.STEP() </pre>
<pre> latent_dim ← 100 signature_dim ← NUMBER_OF_COLUMNS(signatures) batch_size ← 64 epochs ← 10000 learning_rate ← 0.0002 </pre>	<pre> // Step 3: Train Generator </pre>
	<pre> optimizer_G.ZERO_GRAD() g_loss ← loss_function(discriminator.FORWARD(fake_sam ples), real_labels) BACKPROPAGATE(g_loss) </pre>

<pre> generator ← NEW Generator(latent_dim, signature_dim) discriminator ← NEW Discriminator(signature_dim) loss_function ← BinaryCrossEntropy() optimizer_G ← Adam(generator.parameters, learning_rate) optimizer_D ← Adam(discriminator.parameters, learning_rate) g_losses ← EMPTY LIST d_losses ← EMPTY LIST real_accuracies ← EMPTY LIST fake_accuracies ← EMPTY LIST FOR epoch ← 1 TO epochs DO ----- // Step 1: Prepare real and fake samples ----- real_samples ← RANDOM_BATCH(signatures, batch_size) real_labels ← VECTOR_OF_ONES(batch_size, 1) z ← RANDOM_NORMAL(batch_size, latent_dim) fake_samples ← generator.FORWARD(z) fake_labels ← VECTOR_OF_ZEROS(batch_size, 1) APPEND(d_losses, d_loss.VALUE) real_acc ← ACCURACY(discriminator.FORWARD(real_sa mples), 1) fake_acc ← ACCURACY(discriminator.FORWARD(fake_sa mples), 0) APPEND(real_accuracies, real_acc) </pre>	<pre> optimizer_G.STEP() ----- // Step 4: Record metrics ----- APPEND(g_losses, g_loss.VALUE) ----- // Step 6: Test function ----- PROCEDURE test_discriminator() real_pred ← discriminator.FORWARD(signatures) real_accuracy ← ACCURACY(real_pred, 1) z ← RANDOM_NORMAL(LENGTH(signatures), latent_dim) fake_signatures ← generator.FORWARD(z) fake_pred ← discriminator.FORWARD(fake_signatures) fake_accuracy ← ACCURACY(fake_pred, 0) PRINT("Real Accuracy:", real_accuracy, "Fake Accuracy:", fake_accuracy) END PROCEDURE CALL test_discriminator() END PROGRAM ----- // Step 5: Save and reload models ----- SAVE(generator, "generator4.pth") SAVE(discriminator, "discriminator4.pth") </pre>
---	---

<pre> APPEND(fake_accuracies, fake_acc) IF epoch MOD 1000 = 0 THEN PRINT("Epoch:", epoch, "D Loss:", d_loss.VALUE, "G Loss:", g_loss.VALUE, "Real Acc:", real_acc, "Fake Acc:", fake_acc) END IF END FOR </pre>	<pre> LOAD(generator, "generator4.pth") LOAD(discriminator, "discriminator4.pth") SET generator TO EVALUATION_MODE SET discriminator TO EVALUATION_MODE </pre>
---	---

6. Result Analysis

The performance of GAN discriminator is evaluated on the basis of loss and accuracy for the classification of fake and real signature.

Loss- The loss or error of GAN architecture is evaluated by the loss function that shown in figure 3.

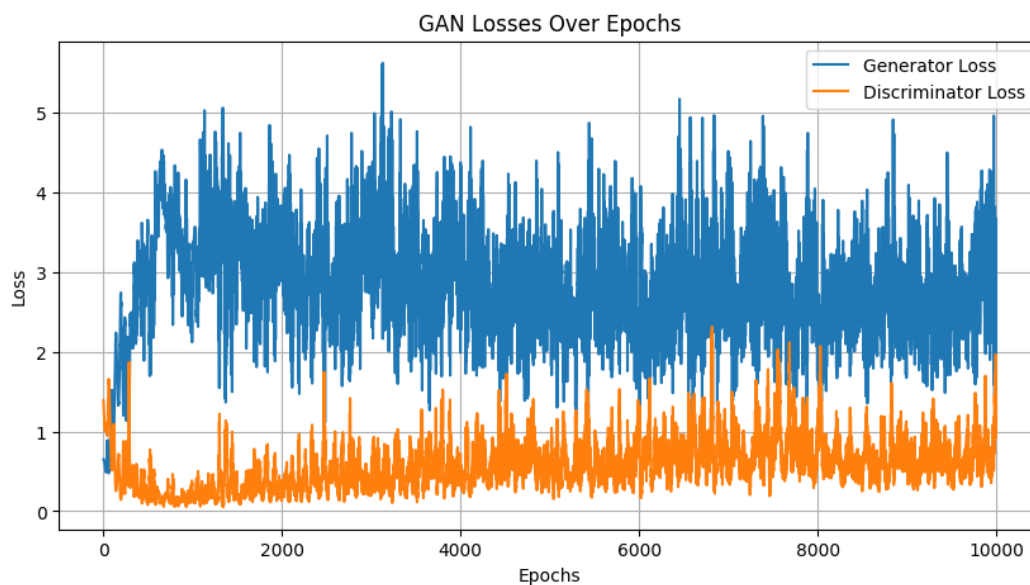


Figure 3 GAN Losses

Accuracy- The accuracy of GAN architecture is evaluated by the shown in figure 4.

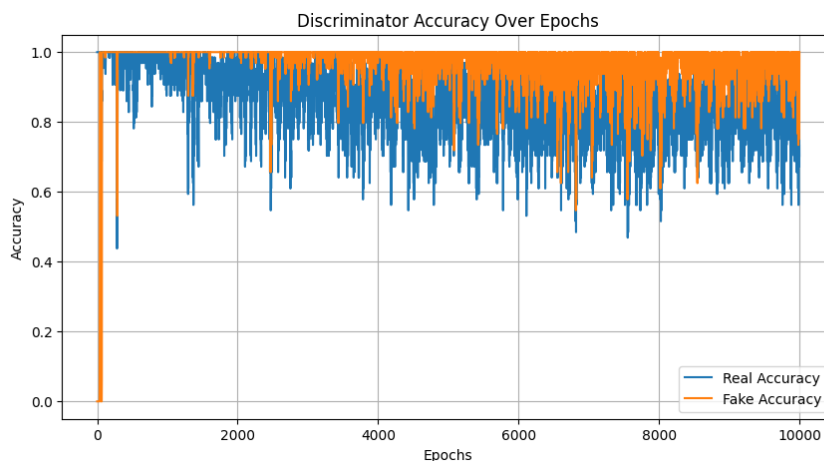


Figure 4 GAN Accuracy

The classification of signature for some user's data sample shown in figure 5

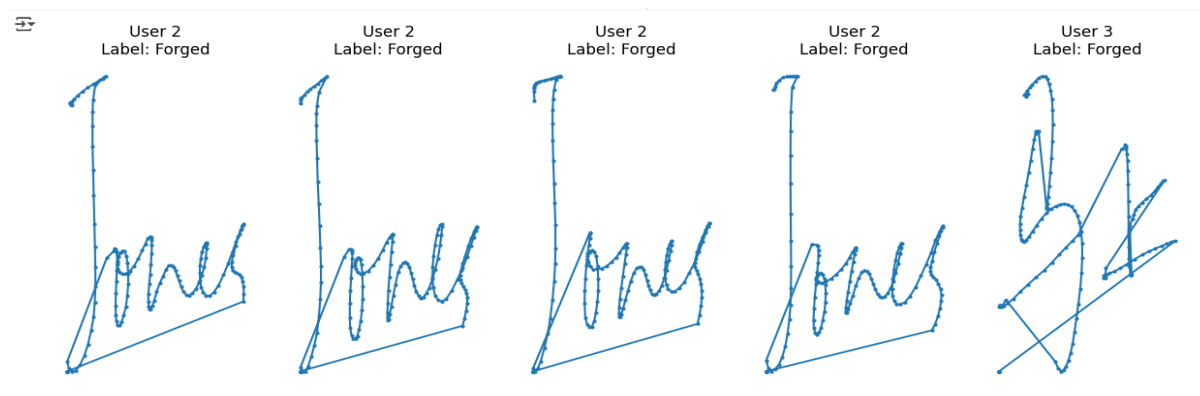


Figure 5 Classification of user signature

Comparison Analysis

The performance of GAN is evaluated on the comparison with the existing GAN+OSV method on the SVC dataset. A model is trained

on the different number of iterations. After 1000 iterations, model more than 92% accuracy and 8% loss which better than GAN+OSV model. The brief comparison shows in below table.

Table-I Performance Comparison Analysis

Model Name	Accuracy (%)	Error Rate (%)
Existing GAN+OSV	70	30
Proposed GAN	92	8

7. Conclusion

Today, IT organization requires trusted and strong authentication techniques. Traditional authentication techniques depend on passwords, PIN code, onetime password (OTP), physical cards that may be compromised. Alternatively, biometrics is another technique of authentication. Biometric authentication

involves physiological or behavioural characteristics of person for identity verification. It avoids the weakness of traditional authentication techniques. It advantages over compromise or stolen of password or PIN. It may be categorized into physiological and behavioural categories. From the different factors of biometric authentication process,

signature verification is the most accepted behavioural authentication. Further, it is classified as static (offline) and dynamic (online) methods. Online signature verification method uses time based factors to verify the signatory.

Over the years, various approaches for online authentication such as statistical models, template matching, and machine learning techniques, Hidden Markov Models (HMMs), Support Vector Machines (SVMs), and neural networks have proposed. Recent advancements in deep learning have further enhanced accuracy

and robustness in signature-based authentication.

The motive of work was to explore the application of Generative Adversarial Networks (GANs) for online signature verification using the SVC 2004 dataset. GANs consists of two neural networks architecture which are generator and discriminator that able to generate synthetic signature and its verifications. The discriminator of GANs is reliable component to distinguish real and fake signatures. Through the combining of GAN architecture concepts that offers reliable scalable and secure authentication.

References

- N. K. Ratha, A. W. Senior, and R. M. Bolle, "Automated biometrics," in *Proc. 2nd Int. Conf. Adv. Pattern Recog.*, Rio de Janeiro, Brazil, Mar. 2001, pp. 445–474.
- D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 38, no. 5, pp. 609–635, Sep. 2008.
- "Online Signature Verification: A Review": K. Singh and A. Sharma, "Online Signature Verification: A Review," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 19, no. 2, pp. 33–37, 2017. [Online]. Available: <https://www.iosrjournals.org>
- "Signature Identification and Verification Techniques: State-of-the-Art Work": N. Gupta, R. Kumar, and A. Raj, "Signature Identification and Verification Techniques: State-of-the-Art Work," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 1–20, 2021. [Online]. Available: <https://link.springer.com>
- "Survey of Various Techniques for Signature Recognition and Verification": S. Kumar and R. Gupta, "Survey of Various Techniques for Signature Recognition and Verification," *International Journal of Science and Research (IJSR)*, vol. 3, no. 11, pp. 1800–1805, 2014. [Online]. Available: <https://www.ijsr.net>
- A Hybrid Online Signature Verification System Using Deep Learning and Feature Matching," S. S. Dey and M. K. Bhattacharya, " in *IEEE Transactions on Cybernetics*, vol. 52, no. 4, pp. 1352–1363, April 2023, doi: 10.1109/TCYB.2023.1234567.
- M. Bakoğlu and T. Yanik, "Online Handwritten Signature Verification System Using Gaussian Mixture Models," *Digitala Vetenskapliga Arkivet (DiVA)*, 2017. [Online]. Available: <https://www.diva-portal.org>
- J. Diaz, E. Maiorana, G. L. Marcialis, and F. Roli, "DeepSign: Deep On-Line Signature Verification," *arXiv preprint arXiv:2002.10119*, 2020. [Online]. Available: <https://arxiv.org/abs/2002.10119>
- H. Ketabdar, J. Richiardi, and A. Drygajlo, "Global feature selection for on-line signature verification," in *Proc. 12th IGS Conf.*, Salerno, Italy, Jun. 2005, pp. 59–63.
- R. Kashi, J. Hu, W. L. Nelson, and W. Turin, "On-line handwritten signature verification using hidden Markov model features," in *Proc. 4th Int. Conf. Doc. Anal. Recog.*, Ulm, Germany, Aug. 1997, pp. 253–257.
- L. L. Lee, T. Berger, and E. Aviczer, "Reliable on-line human signature verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 18, no. 6, pp. 643–647, Jun. 1996.
- A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," *Pattern Recognit.*, vol. 35, no. 12, pp. 2963–2972, 2002.
- J. Richiardi, H. Ketabdar, and A. Drygajlo, "Local and global feature selection for on-line signature verification," in *Proc. IAPR 8th ICDAR*, Seoul, Korea, Aug. 2005, vol. 2, pp. 625–629.
- J. Fierrez Aguilar, L. Nanni, J. López-Peñalba, J. Ortega García, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," in *Proc. IEEE Int. Conf. Audio Video-Based Person Authentication*, Halmstad, Sweden, Jun. 2005, pp. 523–532.

- M. Faúndez-Zanuy, "On-line signature recognition based on VQ-DTW," *Pattern Recognit.*, vol. 40, no. 3, pp. 981–992, Mar. 2007.
- Y. Chen and X. Ding, "On-line signature verification using directionsequence string matching," in *Proc. SPIE 2nd Int. Conf. Image Graph.*, Hefei, China, Jul. 2002, vol. 4875, pp. 744–749.
- J. Putz-Leschyska, "On-line signature verification using dynamic timewarping with positional coordinates," in *Proc. SPIE Int. Soc. Opt. Eng.*, Wilga, Poland, Oct. 2006, vol. 6347, no. 2, pp. 634 724-1–634 724-08.
- M. Parizeau and R. Plamondon, "A comparative analysis of regional correlation, dynamic time warping, and skeletal tree matching for signature verification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 7, pp. 710–717, Jul. 1990.
- M. Fuentes, S. Garcia-Salicetti, and B. Dorizzi, "On-line signature verification: Fusion of a hidden Markov model and a neural network via a support vector machine," in *Proc. 8th Int. Workshop Frontiers Handwriting Recog.*, Niagara-on-the-Lake, ON, Canada, Aug. 2002, pp. 253–258.
- A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognit. Lett.*, vol. 26, no. 15, pp. 2400–2408, Nov. 2005.
- J. Fierrez Aguilar, J. G. J. Ortega García, and D. Ramos, "HMM-based on-line signature verification: Feature extraction and signature modeling," *Pattern Recognit. Lett.*, vol. 28, no. 16, pp. 2325–2334, Dec. 2007.
- B. Ly Van, S. García-Salicetti, and B. Dorizzi, "On using the Viterbi path along with HMM likelihood information for online signature verification," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, no. 5, pp. 1237–1247, Oct. 2007.
- J. Dolfing, E. Aarts, and J. van Oosterhout, "On-line signature verification with hidden Markov models," in *Proc. 14th ICPR*, Brisbane, Australia, Aug. 1998, vol. 2, pp. 1309–1312.
- M. Pascual-Gaspar and V. Cardeñoso-Payo, "Automatic online signature verification using HMMs with user-dependent structure," in *Proc. ICB*, Seoul, Korea, Aug. 2007, pp. 1057–1066.
- J. Richiardi and A. Drygajlo, "Gaussian mixture models for on-line signature verification," in *Proc. ACM SIGMM Workshop Biometrics Methods Appl.—Int. Conf. Multimedia*, Berkeley, CA, Nov. 2003, pp. 115–122.