Deepfakes Signatures Detection in the Handcrafted Features Space

Assia Hamadene
Morsli Abdellah University of Tipaza
Tipaza, Algeria

Abdeldjalil Ouahabi
UMr 1253, iBrain, Inserm, Université de Tours,
Tours, France.

Abdenour Hadid
Sorbonne Center for Artificial Intelligence
Sorbonne University Abu Dhabi, UAE

Abstract

In the Handwritten Signature Verification (HSV) literature, several synthetic databases have been developed for data-augmentation purposes, where new specimens and new identities were generated using bio-inspired algorithms, neuromotor synthesizers, Generative Adversarial Networks (GANs) as well as several deep learning methods. These synthetic databases contain synthetic genuine and forgeries specimens which are used to train and build signature verification systems. Researches on generative data assume that synthetic data are as close as possible to real data, this is why, they are either used for training systems when used for data augmentation tasks or are used to fake systems as synthetic attacks. It is worth, however, to point out the existence of a relationship between the handwritten signature authenticity and human behavior and brain. Indeed, a genuine signature is characterised by specific features that are related to the owner's personality. The fact which makes signature verification and authentication achievable. Handcrafted features had demonstrated a high capacity to capture personal traits for authenticating real static signatures. We, therefore, Propose in this paper, a handcrafted feature based Writer-Independent (WI) signature verification system to detect synthetic writers and signatures through handcrafted features. We also aim to assess how realistic are synthetic signatures as well as their impact on HSV system's performances. Obtained results using 4000 synthetic writers of GPDS synthetic database show that the proposed handcrafted features have considerable ability to detect synthetic signatures vs. two widely used real individuals signatures databases, namely CEDAR and GPDS-300, which reach 98.67% and 94.05% of successful synthetic detection rates respectively.

1. Introduction

Today's security systems have reached high accuracy, effectiveness and protection level. Some biometric tasks related to human behaviour, however, are still to be improved. Human behavior is quite mysterious and unpredictable, it is the most complex aspect to understand and even more to model and to simulate. Not only does it involve brain, consciousness and mind, but it is extremely sensitive to environment and emotional constraints [14] [12] [1]. The paradox between machine and brain is almost the major challenge in scientific research. Actually, fingerprints, faces, palm-prints and other biological biometrics are less constraining because they are stable and specific to each person which makes them more easily differentiated. Conversely, behavioral actions such as handwriting has several facts that make it a highly challenging and complex task. Several psychological and medical studies on handwriting analysis demonstrated that handwriting is controlled by brain, consciousness and behavioral characteristics of one's personality, where the direct linkage between handwriting, human psychology and consciousness has clearly been established in [14] [11].

Nowadays, several handwritten signature verification researches address data-augmentation issue due to the lack of references in the real life, they work on artificially generating new specimens, or synthetic Data [4] [10] [2]. The specificity of the handwritten signature verification as a behavioural issue, however, raises some questions regarding synthetic data, since by definition, a genuine or authentic handwritten signature is one that has been handwritten by an authentic writer. It contains handwriting style characteristics of the author which are specifically related to her/his personality, habits, culture and handwriting manners. Thus, the reason why, we address the issue of considering a synthetic signature as an authentic one to train HSV systems since it is actually an artificial specimen which is not faith-

fully and naturally related to a human identity, especially, when synthetic specimens are resulting from synthetic identities and not duplication of real genuine signatures.

In the scenario considered by Liwicki in handwritten signature competition [9], a particular challenging type called disguised signatures were produced to test the robustness of the HSV systems [9] [8]. This kind of signatures was handwritten by the authentic writer but with the intention to be rejected by the verification system. This is why, we think this particular type of genuine signature is interesting to assess the ability of handcrafted features to capture the handwriting style and behavioral traits of the authentic writer in spite of his goal to fake the verification system.

In the literature of HSV, several synthetic databases have been developed in order to deal with data augmentation issues. For instance, the authors in [4] developed a database containing 4000 synthetic identities with 24 synthetic genuine signatures and 30 synthetic forgeries for each one by tuning 4 parameters of a neuromotor inspired approach. Maruyama et al in [10], created 22 duplicated signatures for each genuine signature in both static images and feature space to train SVM classifier, the duplication method was based on modeling intra-writer variability traits and was tested on standard CEDAR, GPDS 300 and MCYT-75 datasets. A more comprehensive survey that traces recent works on synthetic data generation for biometric applications can be found in [6] [13].

For the best of our knowledge, most of synthetic handwritten signatures are used in the literature for data-augmentation purposes, where synthetic genuine and synthetic forgeries are used to train verification systems. More recently, the authors in [2] [3] investigated the reliability of writer-independent (WI) static signature verification systems when being attempted to be fooled by artificial signatures which were generated by robots and GANs.

Thus, we propose in this paper, a synthetic signature detection system using WI concept using a handcrafted feature space to characterize synthetic signatures, their similarities with respect to real specimens in terms of intra-writers variability, inter-writers variability as well as statistical distributions.

1.1. Comparative concept through Handcrafted Feature space

In a context of assessing the realism degree and representativeness of synthetic signatures for off-line signature verification, one could assume the hypothesis that artificially generating two categories of data implies that we do create the separability between both categories, especially when new identities are produced rather than being duplicated from real specimens of real writers.

In some scenarios, the generated signature are used for both training and testing stages. Therefore, one could consider the risk of biased verification results even when high verification efficiency is obtained. That is to say, the obtained efficiency can be related to the voluntary created separability during data generation. Consequently, in such a scenario, the system could be non-consistent if it is attacked by real human signatures. Hence, we propose to analysis synthetic signatures in the handcrafted feature space and using simple thresholding as a base-line for both synthetic and real signature databases.

The Directional Codes Cooccurrence Matrix (DCCM) handcrafted features [5] have demonstrated good performances for offline signatures using dissimilarities thresholding on standard real signature databases and allows visually explainable separability through dissimilarity distribution curves. This is why, we propose a combination of the DCCM feature generation method with Local Binary Pattern encoding Principle as described below.

1.2. Proposed Handcrafted Feature generation Method

The proposed local Directional Coded Patterns (LDCP) feature generation method is based on combination of DCCM method proposed in [5] and Local Binary Patterns (LBP) encoding principle to allow capturing more textural structures than each method alone. The concept encodes a neighborhood from two to eight pixels surrounding each pixel of interest according to a chosen template. The encoding method is LBP encoding method using the directional indexes rather than gray level classically used in LBP method. Each resulting LDCP code is unique for a specific directional structure contained into signature contours segments. Then, the histogram of LDCP codes is computed as a resulting feature vector to characterize the whole quantitative and directional textures of local structures contained into the signature contour segments. The different stages of the feature generation method are depicted as follows:

First, Contourlet Transform (CT) is performed on the signature image, carrying out directional sub-bands at the first resolution. The resulting CT coefficients describe the importance of each contour segment according to its direction. Then, a directional map is constructed by assigning a code corresponding to the dominant CT coefficient selected through directional sub-bands for each location . This framework means that for each considered location, the carried directional sub-bands are compared in terms of coefficients' importance in order to assign the directional code of the dominant one. The feature vector is then generated according to the following steps:

The first step involves the selection of the dominant direction of the contour segment according to the dominant CT coefficient amplitude for each location. Let consider the dominant CT coefficient computed by taking the absolute maximum value of all directional CT coefficients as fol-

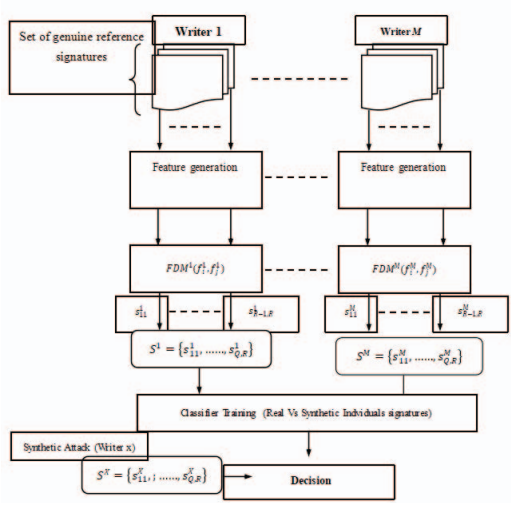

Figure 1. Scheme of Writer-Independent Synthetic Signatures Detection

lows:

$$S_j(n,m) = Max\left\{|C_{jk}(n,m)|\right\}_{k=0}^{K_j-1} \tag{1}$$

The directional map associated with the selected dominant CT coefficient is then generated as:

$$D_j(n,m) = K \tag{2}$$

Thus, the index of the according direction is associated with the dominant contourlet coefficient:

$$LDCP_j(p_i) = \sum_{p=1}^{p} D_j(n,m) \times 2^n \tag{3}$$

$$\sum_{p=1}^{p} D_j(n,m)\times 2^n = \left(D_j(n,m) \times 2^0\right) + ... + \left(D_j(n,m) \times 2^n\right) \tag{4}$$

Finally, the histogram of the obtained LDCP codes of the entire image will represent the final feature vector.

1.3. Proposed WI Detection Scheme

The WI signature verification is allowed through diatomic transformation where by moving from feature domain to dissimilarities domain. Usually, the differences between each pair of feature vectors are computed to generate new dissimilarities vectors which are used for training and testing WI classifiers. We propose to perform our WI verification using Feature dissimilarities measures which provide dissimilarities scores between a questioned signature with a set of references signatures of the same writer. The proposed WI scheme is depicted in Figure 1.

1.4. Deepfakes Detection Results

We conduct the experiments through four different datasets, the first three datasets contain real signatures of real individuals and the fourth one contains synthetic signatures of synthetic individuals. The first dataset named CEDAR contains real signatures of 55 individuals with 24 genuine signatures and 24 skilled forgeries [7] the second dataset contains real signatures of real persons. This dataset is called GPDS [15] which is extensively used in the literature and contains highly skilled forgeries. The GPDS dataset have different versions with different numbers of writers, the most widely used in the literature is GPDS-300 which contains 300 writers. The third dataset is a real one proposed for the Forensic competition in [9], this dataset contains three types of real signatures; Genuine, Forgeries and Disguised signatures. The concept of disguised signatures have been proposed by the same authors in 4Nsigcomp12 competitions in [5] The fourth dataset is GPDS-Synthetic, which contains signatures of 4000 writers with 24 genuines and 30 forgeries per writer. All signatures in this database have been generated by tuning four parameters of a neuromotor. these signature are note duplication of real signatures and were generated n a completely artificial manner and are not produced by real humans [4].

The experiments consider three possible scenarios for deep fakes signatures detection:

1.5. Scenario 1

In the first scenario, the system is trained to separate real writers genuine signatures and synthetic genuine writers signature. Then, the system is tested using other remaining writers' signatures of the same databases (real and synthetic). The results of scenario1 are reported in table 1 and 2 for different writers numbers experiments.

1.6. Scenario 2

In the second scenario, the system is trained to separate real writers genuine signatures and synthetic genuine writers signature. while, the system is tested using Writers from other databases (real and synthetic). The results of scenario1 are reported in table 3 for different writers numbers experiments.

1.7. Scenario 3

The third scenario aim to be more challenging and more realistic, it assumes that the systems is a classical verification system which did not learned synthetic data, then, it is attacked with synthetic genuine specimens. thus, the training stage is performed using Genuine and forgeries signatures of real writers. Then, it is testes by Synthetic Genuine. that id to say that the verification system trained on only to separate real genuine vs real skilled forgeries, then,

Training writers	FAR(%)	FRR(%)	AER(%)
20 Real Vs 20 Synthetic	02.40	2.25	02.33
30 Real Vs 30 Synthetic	00.42	01.68	01.05
40 Real Vs 40 Synthetic	00.35	01.40	00.87

Table 1. Deepfakes detection Using writers of CEDAR Database (Scenario 1)

Training writers	FAR(%)	FRR(%)	AER(%)
20 Real Vs 20 Synthetic	03.81	08.10	05.95
50 Real Vs 50 Synthetic	05.38	02.92	04.15
80 Real Vs 30 Synthetic	05.88	02.24	04.06

Table 2. Deepfakes detection Using writers of GPDS-300 Database (Scenario 1)

Training writers	Test Writers	AER(%)
20 CEDAR vs 20 Synth	300 GPDS vs 300 synth	06.90
20 GPDS vs 20 Synth	55 CEDAR vs 55 synth	02.10
55 CEDAR vs 55 Synth	300 GPDS vs 300 synth	06.80
55 GPDS vs 55 Synth	55 CEDAR vs 55 synth	03.92

Table 3. Deepfakes detection Using writers of mixed database (Scenario 2)

Training on real writers	Attack with synth and real Writers	AER(%)
20(gen+forg)CEDAR	35synth+35real CEDAR	1.87
20(gen+forg)GPDS	280synth+280real GPDS	6.23

Table 4. Deepfakes detection Using Real writers of mixed database (Scenario 3)

Training writers	Test Writers	AER(%)
20CEDAR vs 20 Synth	Auth 1 4Nsig Gen VS synth	00
20CEDAR vs 20 Synth	Auth 1 4Nsig Disg VS synth	01.06
20CEDAR vs 20 Synth	Auth 2 4Nsig Gen VS synth	11.45
20CEDAR vs 20 Synth	Auth 2 4Nsig Disg VS synth	12.5
20CEDAR vs 20 Synth	Auth 3 4Nsig Gen VS synth	00
20CEDAR vs 20 Synth	Auth 3 4Nsig Disg VS synth	00

Table 5. Deepfakes detection Using writers of 4NsigComp authors in mixed database Scenario (including Attacks with disguised signatures)

Database	FAR	FRR	AER
Real CEDAR	01.96	00.57	01.27
Real GPDS-300	24.80	13.96	19.38
Synthetic GPDS-4000	30.51	51.15	40.83

Table 6. Verification Performances using Dissimilarity thresholding (global threshold)

it attacked with synthetic genuine ones. The results of this scenario are reported in table 4.

We further perform verification results in table 6 to evaluate the the characterisation effectiveness in authentication genuine vs skilled forgeries using a unique threshold for the hole writers database in both real writers ans synthetic writers cases.

1.8. Comparative visualization

In order to analyse the separability of real signatures comparatively to synthetic ones, we generate the dissim-

AER(%)	Author1	Author2	Author3
Best 4Nsigcomp system	4.43	20.65	5.49
Proposed	00	26.51	00

Table 7. Verification Performances of 4Nsigcomp dataset using SVM classification without Disguised signatures

AER(%)	Author1	Author2	Author3
Best 4Nsigcomp system	6.4	22.42	31.71
Proposed	00	26.47	00

Table 8. Verification Performances of 4Nsigcomp dataset using SVM classification with Disguised signatures

ilarities scores distributions obtained through DCCM features using Feature Dissimilarity Measures or dissimilarities scores which are computed between each possible genuine-genuine (G-G) signature feature and Genuine-Forgery (G-F) ones of the aimed couple of signatures using Canberra distance [5]. Thus, a low score of dissimilarity conveys a high degree of resemblance between the two signatures and conversely a high score of dissimilarity conveys a low degree of resemblance. We further include in this analysis (G-D) Scores which are dissimilarities between Genuine and Disguised signatures. These dissimilarities scores are the result of matching of the feature vectors of the aimed couple of signatures using Canberra distance [5] As experimental interpretation, we illustrate in Figures 2, 3 and 4 the distributions of scores values computed between all Genuine-Genuine (G-G) feature vectors pairs and Genuine-Forgery (G-F) for both real and synthetic GPDS datasets.

1.9. Evaluation per Author (Real vs Disguised and Synthetic)

Since the 4Nsigcomp12 contains only few authors and in order to analyze with more details and compare synthetic and disguised signatures, we carry out the distributions of dissimilarity scores by the authors individually for 2 real authors of 4Nsigcom12 with their genuine, disguised and forgery signatures and 2 randomly synthetic identities of GPDS synthetic dataset. The distribution curves are shown in figures 5, 6, 7 and 8. Table 7 and 8 provide the verification results using svm classifier considering the with and without disguised verification as well as the comparison to the best stat of the art comparative results on the the same dataset.

1.10. Discussion

The proposed handcrafted feature method provides good performances in synthetic signatures detection for all the experimented databases. The visualisation of the dissimilarities distributions scores (FDMs) reveals interesting differences with are coherent with the obtained verification results when comparing Real databases with respect to the

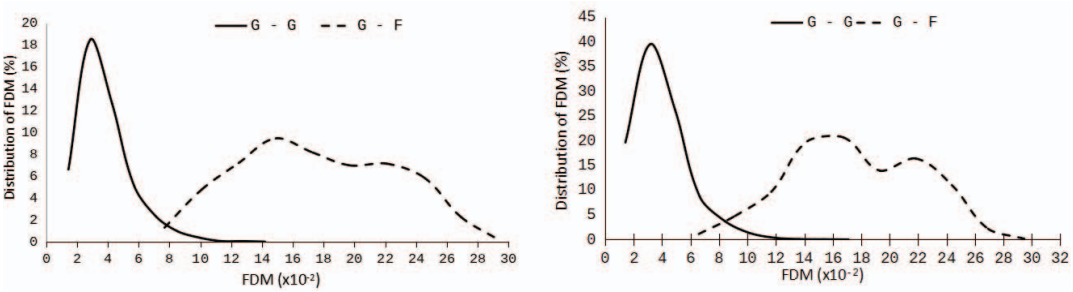

Figure 2. Distribution of Genuine-Genuine (G-G) and Genuine-Forgery (G-F) Feature dissimilarity Measures wicht DCCM method (left) and Proposed features (right) of Real CEDAR dataset)

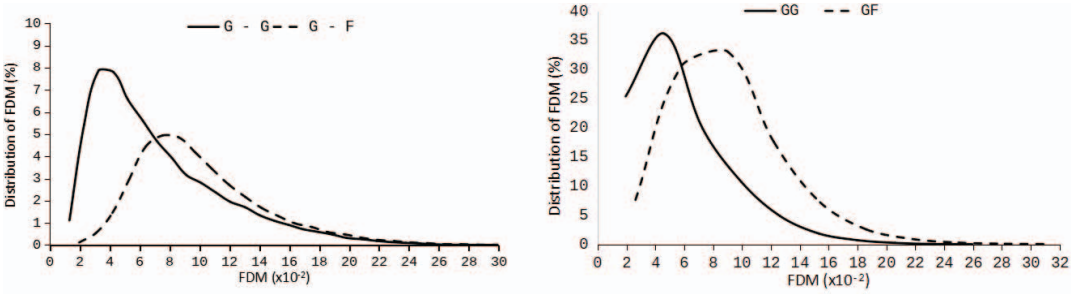

Figure 3. Distribution of Genuine-Genuine (G-G) and Genuine-Forgery (G-) Feature dissimilarity Measures wicht DCCM method (left) and Proposed features (right) of Real GPDS dataset)

synthetic one.

The signature verification performances show that the propose handcrafted features are highly effective to authenticate signature of real writers databases even in the case of highly skilled forgeries and disguised signatures attacks and using simple thresholding for classification whereas the same features are not efficient for synthetic writers signature verification, which can be explainable through the dissimilarities distributions curves comparison of real vs synthetic writers databases.

The Synthetic vs real comparison can be depicted in the following observations: All of real writers distributions of both CEDAR, real GPDS and 4NsigComp have low scores of dissimilarity for G-G cases and higher scores of dissimilarity for G-F cases. whereas, in synthetic 4000 writer database, there is no low and high dissimilarity for G-G and G-F classes.

Both curves of GG and GD have less intra-class variability comparatively to GF intra-variability which is larger in real authors. Whereas for synthetic signatures, the intra-class variability range is exactly the same in both GG and GF classes.

Both real curves (GG and GD) have close mode values, follow a Gaussian distribution which is far from GF mode. Whereas in synthetic signatures distribution, we can observe that both categories distribution (GG and GF) are completely overlapped with two modes for GG and two modes for GF which are positioned at the same scores values.

The curves obtained for 4NsigCom authors point out the reliability of the proposed handcrafted features, since the writer traits are captured even when disguising signatures. The disguised signatures are very close to the genuine ones, which confirms that a real signature even when being disguised, it still comports the behavioural characteristics of its authentic writer, whereas an expert forger is trying to imitate a signature with her/his own involuntary handwriting characteristics.

Conversely to all real writers, we can not observe low dissimilarities and less intra-variability in the within-writer signatures for synthetic signatures curves, which rises the representatives issue of training verification systems using synthetic data.

In the case of synthetic writers dataset, both of the obtained curves and verification accuracy suggest that, synthetic data do not have the same characteristics in the handcrafted feature space, which is interesting to be investigated more.

2. Conclusion

In this work, we analysed the characterization of synthetic handwritten signatures in the handcrafted feature space. The used handcrafted feature characterization

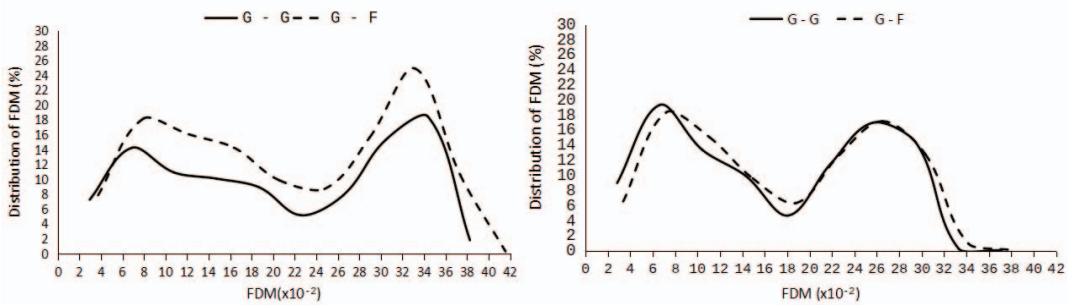

Figure 4. Distribution of Genuine-Genuine (G-G) and Genuine-Forgery (G-F) Feature dissimilarity Measures with DCCM method (left) and Proposed features (right) of Synthetic GPDS dataset)

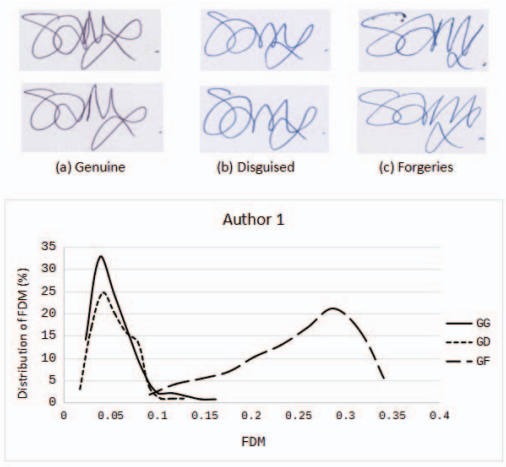

Figure 5. Distribution of Genuine-Genuine (G-G), Genuine-Disguised (G-d) and Genuine-Forgery (G-F) DCCM dissimilarities of the fist Real Author of 4NSIGCOMP dataset)

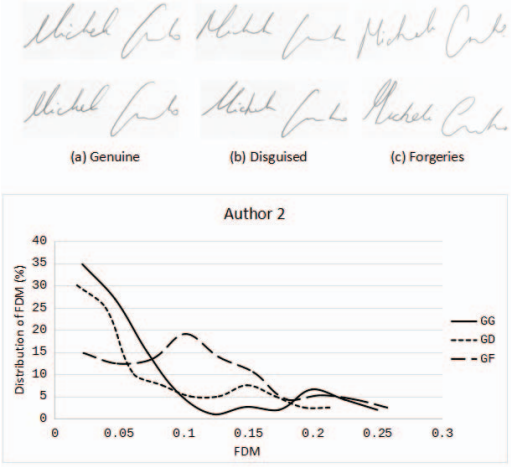

Figure 6. Distribution of Genuine-Genuine (G-G), Genuine-Disguised (G-d) and Genuine-Forgery (G-F) DCCM dissimilarities of the second Real Author of 4NSIGCOMP dataset)

method offers high performances in detecting synthetic signatures as well as the signature verification of real writer. The inefficiency of the method for synthetic signature verification while being highly effective for three different widely used real writers' databases show that synthetic signatures could be not enough realistic especially to be used for training data-augmentation issues. The analysis of the disguised kind of signatures demonstrated that it has the same characteristics as real genuine ones in spite of the intention of the owner to fake the system which corroborate that the real handwriting contains involuntary personal traits and characteristics of the human writers which are not represented in synthetic data.

References

[1] Azeddine Benlamoudi, Salah Eddine Bekhouche, Maarouf Korichi, Khaled Bensid, Abdeldjalil Ouahabi, Abdenour Hadid, and Abdelmalik Taleb-Ahmed. Face presentation attack detection using deep background subtraction. *Sensors (Basel, Switzerland)*, 22, 2022. 1

[2] Jordan J Bird. Robotic and generative adversarial attacks in offline writer-independent signature verification. *arXiv preprint arXiv:2204.07246*, 2022. 1, 2

[3] Jordan J Bird, Abdallah Naser, and Ahmad Lotfi. Writer-independent signature verification; evaluation of robotic and generative adversarial attacks. *Information Sciences*, 633:170–181, 2023. 2

[4] Miguel A Ferrer, Moises Diaz-Cabrera, and Aythami Morales. Static signature synthesis: A neuromotor inspired approach for biometrics. *IEEE Transactions on pattern analysis and machine intelligence*, 37(3):667–680, 2014. 1, 2, 3

[5] Assia Hamadene and Youcef Chibani. One-class writer-independent offline signature verification using feature dissimilarity thresholding. *IEEE Transactions on Information Forensics and Security*, 11(6):1226–1238, 2016. 2, 4

[6] Indu Joshi, Marcel Grimmer, Christian Rathgeb, Christoph Busch, François Brémond, and Antitza Dantcheva. Synthetic data in human analysis: A survey. *ArXiv*, abs/2208.09191, 2022. 2

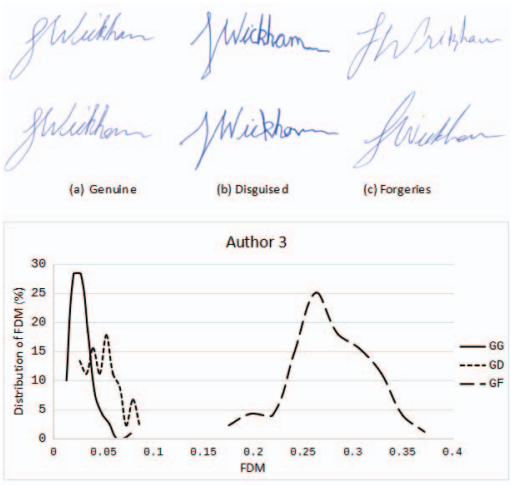

Figure 7. Distribution of Genuine-Genuine (G-G), Genuine-Disguised (G-d) and Genuine-Forgery (G-F) DCCM dissimilarities of the third Real Author of 4NSIGCOMP dataset)

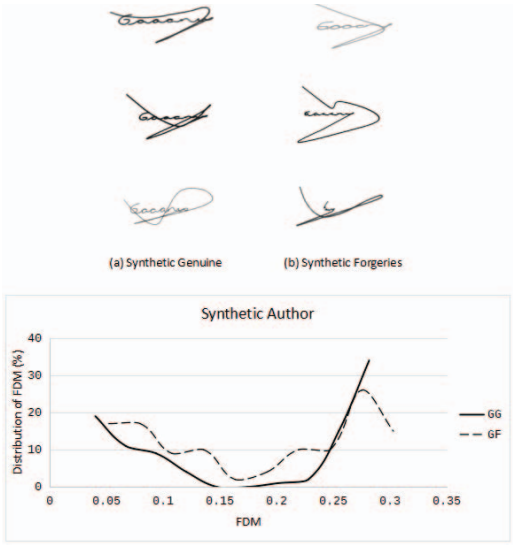

Figure 8. Distribution of Genuine-Genuine (G-G) and Genuine-Forgery (G-F) DCCM dissimilarities of one Synthetic identity of GPDS dataset)

[7] 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. 3

[8] Marcus Liwicki, Muhammad Imran Malik, Linda Alewijnse, Elisa van den Heuvel, and Bryan Found. Icfhr 2012 competition on automatic forensic signature verification (4nsigcomp 2012). In *Proceedings of the 2012 International Conference on Frontiers in Handwriting Recognition*, ICFHR '12, page 823–828, USA, 2012. IEEE Computer Society. 2

[9] Marcus Liwicki, C. Elisa van den Heuvel, Bryan Found, and Muhammad Imran Malik. Forensic signature verification competition 4nsigcomp2010 - detection of simulated and disguised signatures. In *International Conference on Frontiers in Handwriting Recognition, ICFHR 2010, Kolkata, India, 16-18 November 2010*, pages 715–720. IEEE Computer Society, 2010. 2, 3

[10] Teruo M Maruyama, Luiz S Oliveira, Alceu S Britto, and Robert Sabourin. Intrapersonal parameter optimization for offline handwritten signature augmentation. *IEEE Transactions on Information Forensics and Security*, 16:1335–1350, 2020. 1, 2

[11] Jiri Mekyska, Katarína Šafárová, Tomas Urbanek, Jirina Bednarova, Vojtech Zvoncak, Jana Marie Havigerova, Lukas Cunek, Zoltan Galaz, Jan Mucha, Christine Klauszova, et al. Graphomotor and handwriting disabilities rating scale (gh-drs): Towards complex and objective assessment. 2023. 1

[12] Safaa El Morabit, Atika Rivenq, Mohammed En nadhir Zighem, Abdenour Hadid, Abdeldjalil Ouahabi, and Abdelmalik Taleb-Ahmed. Automatic pain estimation from facial expressions: A comparative analysis using off-the-shelf cnn architectures. *Electronics*, 2021. 1

[13] Deepak Moud, Sandeep Tuli, and Rattan Pal Rana. A review on offline signature verification using deep convolution neural network. *Information Management and Machine Intelligence: Proceedings of ICIMMI 2019*, pages 15–21, 2021. 2

[14] Sara Rosenblum and Miri Livneh-Zirinski. Handwriting process and product characteristics of children diagnosed with developmental coordination disorder. *Human movement science*, 27(2):200–214, 2008. 1

[15] Francisco Vargas, M Ferrer, Carlos Travieso, and J Alonso. Off-line handwritten signature gpds-960 corpus. In *Ninth International Conference on Document Analysis and Recognition (ICDAR 2007)*, volume 2, pages 764–768. IEEE, 2007. 3