Guilloche Detection for ID Authentication: A Dataset and Baselines

Musab Al-Ghadi, Zuheng Ming, Petra Gomez-Krämer, Jean-Christophe Burie, Mickaël Coustaty, Nicolas Sidère

Guilloche Detection for ID Authentication: A Dataset and Baselines

Musab Al-Ghadi*, Zuheng Ming*, Petra Gomez-Krämer*, Jean-Christophe Burie*, Mickaël Coustaty* and Nicolas Sidere*
Computer Science, Image and Interaction Laboratory, La Rochelle University, France
Email: *{musab.alghadi,zuheng.ming,petra.gomez,jean-christophe.burie,
mickael.coustaty,nicolas.sidere}@univ-lr.fr

***Abstract*—In cases of digital enrolment via mobile and online services, identity documents (IDs) verification is critical to efficiently detect forgery and therefore build user trust in the digital world. In this paper, we propose a copy-move public dataset, called FMIDV (forged mobile ID video dataset) containing forged IDs with respect to guilloche patterns. Also, we propose two fraud detection models on guilloche patterns of IDs, which are based on contrastive and adversarial learning. In the sequel, each proposed model manages to read the entire ID and to recognize the guilloche pattern to check its similarity to the pattern of an authentic ID. The objective of the similarity check is to validate its authenticity or its rejection. Experiments are conducted on MIDV and FMIDV datasets to analyze and identify the most proper parameters to achieve higher authentication performance. The code and the dataset are available at https://github.com/malghadi/CheckID.**

***Index Terms*—Fraud detection, identity documents, CNN, Guilloche pattern, Contrastive learning, Adversarial learning**

I. Introduction

Confirming the authenticity of the IDs such as a passport, identity card, or driving license has become a critical part of online security and digital on-boarding for businesses [1]. The governments have incorporated a number of sophisticated security features in all issued IDs to combat forgery and counterfeiting on IDs. These features are difficult to reproduce accurately, making them effective anti-counterfeiting features.Guilloche patterns, holograms, anti-scan patterns, watermarks, and micro types are examples of security features. Guilloche is one of the interesting visual patterns that can be used for ID verification, is a geometrical pattern of computer-generated fine lines that are interlaced to form a unique shape [2] and is printed on the background of the IDs. The use of guilloche patterns for ID verification is based on the fact that it is difficult to reproduce accurately by hand or using a computer, making it a good anti-counterfeiting feature.

In this paper we propose a new forgery detection dataset called FMIDV, and two guilloche detection models to confirm whether a user's ID is real or fake. The solution is based on designing an intelligent and precise verification solution that can read the entire ID and recognize the guilloche pattern, and then check its similarity to other patterns of real IDs of the same country. The objective of the similarity check is to validate its authenticity or to reject it if it is considered as forged. The contribution of this paper can be summarized as follows: (i) *Data set*: this paper introduces a new data set of fake IDs with respect to the manipulation of guilloche patterns. (ii) *Novelty*: this paper introduces new architectures to design guilloche detection models for ID authentication based on contrastive and adversarial learning.

This work is part of the IDECYS project (n° DOS0098984/00) supported by BPI France in the Framework of the FUI AAP25 program.

II. Literature Review

Visual features, optical character recognition (OCR), and machine learning-based methods are considered for IDs verification and fraud detection.

In [3], a hologram detection approach for ID verification is proposed. The approach is based on the shape and the color analysis thanks to the pixel properties to extract the hologram for a given ID and decide the presence of the hologram in a given ID or not. In [4] the authors proposed a passport verification approach based on the detection of periodic patterns that are printed on the passport. The presence or absence of the periodic patterns on a given passport is studied through k peaks of fast Fourier transform (FFT) to discriminate between a real and a fake passport. In [5], an authentication approach for IDs, based on the conformity of visual features and patterns is proposed. The approach is based on generating a visual descriptor from a set of visual features, which are relevant enough with the color connected components of the processed ID. The similarity between the descriptors of a real ID and a query ID is measured to decide whether the query ID is real or fake. In [6], the authors used OCR to extract some information, such as name, date of birth, and address, to confirm the identity of the document's holder and ensure that the document is not being used fraudulently.

In [7], the authors proposed a specific classifier to verify the authenticity and legitimacy of IDs. The classifier module started by extracting local and global features like gray-scale histograms, hue and saturation differences, structural similarity score, and histogram of oriented gradients from the given ID. Then, these features are fed into support vector machine and random forest classifiers to test if the ID is real or fake. Another solution was designed in [8]. Here, two CNN models called *Siamese* and *Triplet* are adapted to design a technique for ID verification. The role of these models is to extract feature vectors from a pair of IDs and then to

measure the similarity between these vectors to decide if a given ID is real or fake. [9] used *Siamese*, *Triplet*, and *PeleeNet* CNN models to design a verification approach for Spain IDs. The approach performed a recurrent comparison between two textured background blocks; one block from the genuine ID and the other from the counterfeit ID. The difference between the two processed blocks is learned iteratively with an attention model into specific zones in the ID background.

III. Proposed FMIDV dataset: Forged Mobile ID Video

Due to the lack of available datasets for fake IDS, we propose in this paper a dataset called FMIDV[1], which contains 28000 forged IDs of 10 countries. The forged samples contain many similar but genuine objects (SGO), which has been shown as a challenge for copy-move forgery detection (CMFD) algorithms and should be useful in many works in digital forensics research.

The reason to use copy-move operations to create a fake dataset for fraud detection is that it simulates the behavior of real-world fraudsters who often use these techniques to hide their modifications in documents. Copy-move operations are used to reuse patterns from the real document and hide modifications such as a fraudulent name being shorter than the original one. Areas without any information in the foreground, such as spaces or blank zones, are good candidates for copy-move operations because they are less likely to be noticed. However, if the area contains a guilloche pattern, the copy-move operation will create irregularities in the global pattern, which can be detected by efficient methods of fraud detection. The goal is to detect these irregularities in the global pattern, which can be indicative of fraud.

For generating FMIDV, we use the IDs of MIDV-2020 [10]. MIDV consists of 4000 IDs of 10 different countries. For each country, MIDV-2020 introduces 1000 template IDS (dummy IDS were created from Wikimedia Commons), 2000 scanned IDS (were created by scanning the template samples using Canon LiDE 220 and Canon LiDE 300 scanners with a resolution of 2480×3507) and 1000 photos IDs (were created by capturing the template IDs using Apple iPhone XR and Samsung S10 with a resolution of 2268×4032 and under various environmental conditions). Then, we follow two main steps: the first step involves identifying the zones in the IDs that visually (i.e. manual inspection by naked eyes) contain only information about the guilloche patterns, and the second step involves implementing copy-move forgeries among the candidate zones in a given ID.

To accomplish the first step, we read only one real sample of each country in MIDV. Then, for each of the selected ID we resize it in such a way that we can partitioning it into a set of non-overlapping blocks of different sizes 16×16, 32×32 and 64×64. For each level of partitioning, we define a set of zones (as unique set) that visually have only information about the guilloche patterns. Subsequently, this set is fed into the next step for applying copy-move forgeries on all IDs that belong to the same country. Copy-move operations were applied on zones of sizes 16×16 and 32×32 and 64×64 pixels, which are selected randomly. Actually, for each ID in MIDV-2020, we have generated 7 forged samples. Fig. 1 illustrates an example of selected candidate zones for a given ID, and an example of a copy-move forgery operation.

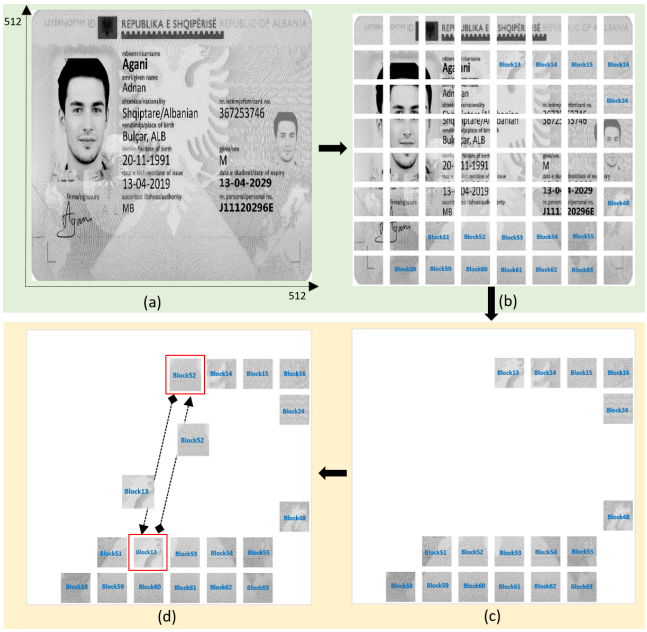


Fig. 1: An overview of copy-move forgeries on ID.

In Fig. 1, one Albania (alb) real sample is selected and resized into 512×512 as shown in Fig. 1-a. Then, this sample is partitioned into blocks of size 64×64 as in Fig. 1-b. Here, we can see (visually) that all blue annotated zones (i.e. blocks$\{13,14,15,16,24,48,51,52,53,54,55,58,59,60,61,62,63\}$) have no information except the guilloche patterns. Thus, we have selected these zones as candidate zones as in Fig. 1-c for implementing copy-move forgery operations and to generate a fake dataset of the given country. An example of copy-move forgery operation between blocks 13 and 52 is illustrated in Fig. 1-d. A sample of real and fake IDs are shown in Fig. 2.

IV. Proposed Guilloche Detection Models for IDs verification

In this paper we propose two guilloche detection models for IDs authentication. The first model uses a contrastive learning [11] to learn a representation of input ID, and then uses this representation to identify instances of abnormal or fraudulent data. This model is called contrastive based fraud detection (CFD). The second model uses an adversarial learning [12] to detect fraudulent activities by training a model to identify and flag suspicious instances that deviate from normal patterns. This model is called fake-sample-adversary based fraud detection (FsAFD).

[1]http://l3i-share.univ-lr.fr/2022FMIDV/2022FMIDV.html

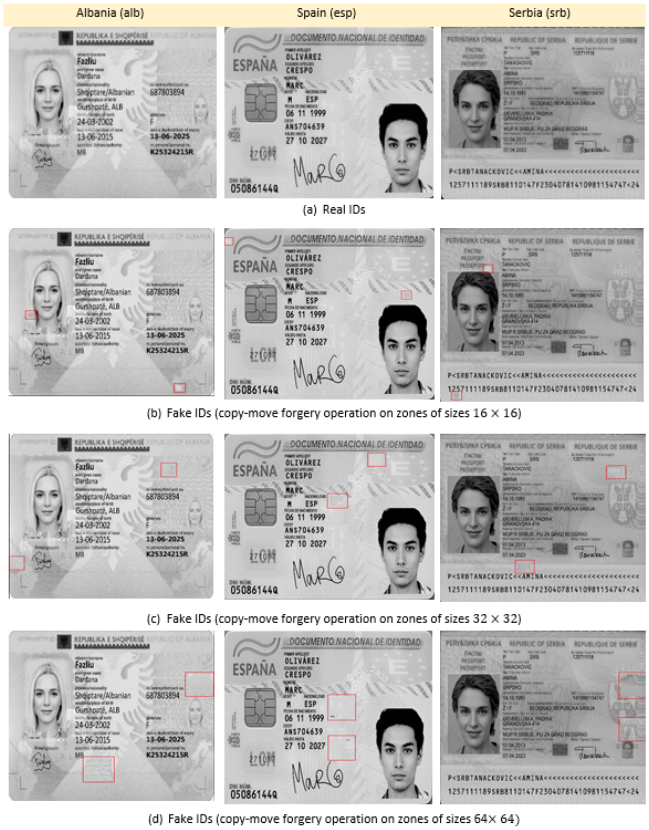


Fig. 2: Sample of MIDV and FMIDV: (a) real samples of three different countries, (b-d) fake samples of the three real IDs after applying copy-move forgeries with different zone sizes; red boxes present the forgery locations.

Both models use Siamese Neural Network as the CNN backbone. Siamese neural network is a type of neural network architecture that consists of two or more identical sub-networks that share the same parameters [13]. These sub-networks are used to process different inputs and their output is then compared to measure the similarity or the difference between the inputs. In the context of ID verification, the Siamese neural network is used to compare the guilloche pattern on the query document to the guilloche pattern on a reference document. By comparing the patterns and measuring their similarity, the model can determine whether the query document is real or fake. The use of a CNN backbone allows the model to learn and extract features from the image data, making it more robust to different lighting conditions, image distortions, and other variations in the data.

A. CFD Model: contrastive based fraud detection model

This model employs encoder-classifier sub-networks. The role of the encoder component (i.e. Siamese neural network) is to extract the features from a pair of IDs and compressing them into a lower-dimensional representations. While, the classifier component uses the encoded data to make predictions (i.e. classify the input ID into a real or fake ID). An overview of the CFD model is depicted in Fig. 3.

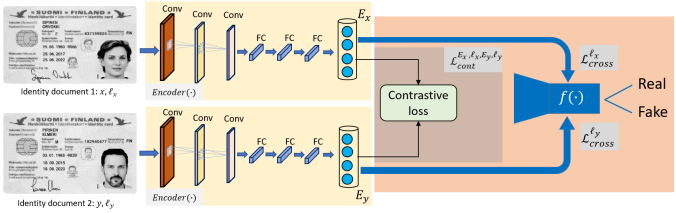


Fig. 3: An overview of CFD model.

As we can see in Fig. 3, an encoder network $E(.)$, receives a pair of IDs $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ and extracts latent feature vectors $E_x \in \mathbb{R}^{d\times 1}$ and $E_y \in \mathbb{R}^{d\times 1}$ where $E_x = E(x)$ and $E_y = E(y)$ respectively. These latent vectors E_x and E_y are used to compute a contrastive loss (denoted as $\mathcal{L}_{cont}^{E_x,\ell_x,E_y,\ell_y}$) to discriminate between E_x and E_y. Here, an image pair (x, y) is fed into the model as input and the objective is to discriminate between them. Where ℓ_x is the label of the input x and ℓ_y is the label of the input y. It is worth noting that in CFD model the input pair could be real-real or real-fake. The other part of the model is a classifier $f(.)$ network, whose task is to classify the latent feature vectors E_x and E_y into the class of "$real$" or "$fake$".

1) CFD model training: The objective of the CFD model is achieved by: (i) minimizing the distance between the latent spaces (E_x and E_y) of an input pair of IDs if they both belongs to the same class (i.e. either both are real, or both are fake). (ii) maximizing the distance between them if the pair does not belong to same class (i.e. one is real and the other is fake). (iii) maximizing the ability of the classifier $f(.)$ to classify the input pair correctly. Two loss functions are modeled here to achieve the mentioned objective: (i) contrastive loss ($\mathcal{L}_{cont}^{E_x,E_y,\ell_x,\ell_y}$) and (ii) cross-entropy loss ($\mathcal{L}_{cross}^{\ell}$) of the classifier $f(.)$.

Contrastive loss $\mathcal{L}_{cont}^{E_x,\ell_x,E_y,\ell_y}$: The contrastive loss function is used to train the encoder $E(.)$ to produce compact feature representations (E_x, E_y), where samples from the same class are embedded close together, and samples from different classes are embedded far apart in the feature space. This can be done by comparing the features of different samples, and penalizing the encoder $E(.)$ if the features of samples from the same class are not similar, or if the features of samples from different classes are similar. Mathematically, the contrastive loss is represented as follows:

$$\mathcal{L}_{cont}^{E_x,\ell_x,E_y,\ell_y} = [\ell_x = \ell_y]\|E_x - E_y\|_2^2 + [\ell_x \neq \ell_y] \; max(0, \epsilon - \|E_x - E_y\|_2)^2 \quad (1)$$

where the margin (ϵ) is a hyperparameter defining the lower bound distance between samples of different classes.

Cross-entropy loss $\mathcal{L}_{cross}^{\ell}$: With $\mathcal{L}_{cross}^{\ell}$ we are trying to minimize the probability of a negative class by maximizing an expected value of $f(.)$ on our training data. Indeed, the cross-entropy loss is used to measure the difference between two

probabilities that a model assigns to classes. Mathematically, the $\mathcal{L}_{cross}$ represented as follows:

$$\mathcal{L}^{\ell}_{cross} = -\frac{1}{N}\left[\sum_{i=1}^{N}[\ell_i\, log(p_i) + (1-\ell_i)\, log(1-p_i)]\right] \quad (2)$$

where N is the number of samples, ℓ is the true class label (0 for fake and 1 for real), p is the predicted probability for the correct class, and log is the natural logarithm.

In the sequel, the overall objective function for training CFD model is defined as follows:

$$\mathcal{L}_{CFD} = \alpha\, \mathcal{L}^{E_x,\ell_x,E_y,\ell_y}_{cont} + (1-\alpha)\, \mathcal{L}^{\ell}_{cross} \quad (3)$$

where α is a hyperparameter that controls the weight of each loss function in the overall objective function.

B. FsAFD Model: fake-sample-adversary based fraud detection model

The second model employs encoder-(fake-sample-adversary) sub-networks that consists of two main components: an encoder $E(.)$ and an adversary $A(.)$. An overview of FsAFD model is depicted in Fig. 4.

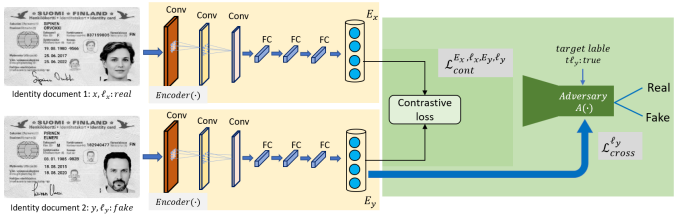


Fig. 4: An overview of FsAFD model.

In Fig.4, the role of the encoder component $E(.)$ (i.e. Siamese neural network) is to extract features from the input pair (x, y) and compressing them into a lower-dimensional representation E_x and E_y. And the adversary component $A(.)$, also known as the discriminator, uses the encoded data to determine whether the input is real or fake.

It's worth noting that in this model we arbitrarily select the first input x as real and the second input y as fake (the truth label of input $x; \ell_x$ is real $(\ell_{x:real})$ and the truth label of input $y; \ell_y$ is fake $(\ell_{y:fake})$), and we only insert the encoded representation E_y of the second input y, which is fake, into the adversary network $A(.)$. This is the reason why we call the adversary here as fake-sample-adversary. In this scenario, the encoder $E(.)$ maps the true and fake samples to lower-dimensional representations E_x and E_y. And the adversary $A(.)$ assigns a low probability to the encoded representation of the fake sample E_y. This is used to identify samples that deviate from the normal data distribution and can be considered as anomalies.

1) FsAFD model training: The encoder $E(.)$ works to maximize the probability of the adversary $A(.)$ classifying the input as fake, while the adversary $A(.)$ minimizes the probability of the encoder $E(.)$ producing encoded representations that are classified as real. Effectively, employing the fake-sample-adversary in this model yields to enhance the quality of latent spaces implicitly by maximizing the distance between the latent spaces E_x and E_y from the side of E_y only. Additionally, this leads to maximize the ability of the adversary to correctly classify the inputs as real or fake. Two loss functions are modeled here to achieve the mentioned objective: (i) the contrastive loss ($\mathcal{L}^{E_x,\ell_x,E_y,\ell_y}_{cont}$) as in (1), and (ii) the adversary loss $\mathcal{L}^{\ell,t\ell}_{adv}$.

Adversary loss $\mathcal{L}^{\ell,t\ell}_{adv}$: This loss function measures the ability of the classifier to detect an input as real. Here, the classifier incurs an adversary loss from its predictions. To this end, the loss value is calculated by assigning a contrary target label $(t\ell)$ to the truth one (ℓ). Hence, if ℓ is real, then $t\ell$ is fake and vise versa. Mathematically, the adversary loss is represented as follows:

$$\mathcal{L}^{\ell}_{adv} = -\frac{1}{N}\left[\sum_{i=1}^{N}[\ell_i\, log(p_i) + (1-\ell_i)\, log(1-p_i)]\right] \quad (4)$$

where N is the number of samples, ℓ is the true class label (0 for fake and 1 for real), p is the predicted probability of the input being real.

In the sequel, the overall objective function for training the FsAFD model can be defined as:

$$\mathcal{L}_{FsAFD} = \delta\, \mathcal{L}^{z_x,\ell_x,z_y,\ell_y}_{cont} + (1-\delta)\, \mathcal{L}^{\ell}_{adv} \quad (5)$$

where δ is a hyperparameter that controls the weight of each loss function in the overall objective function.

V. Experimental Results

A. Real and Fake Samples

To evaluate the performance of the proposed models, the MIDV dataset [10] is used as dataset that has the real samples, and the FMIDV dataset is used as dataset that has the fake samples. Totally, MIDV consists of 4000 IDs of 10 different countries: Albania (alb), Azerbaijan (aze), Spain (esp), Estonia (est), Finland (fin), Greece (grc), Latvia (iva), Russia (rus), Serbia (srb), and Slovakia (svk). And FMIDV consists of 24000 forged IDs of the same 10 countries as in MIDV (after out-casting the fake samples of 64×64).

B. Experiment Setup

Obviously, the training and testing of the proposed models are carried out for each country separately. And the training process takes place by handling pairs of samples, while the testing process takes place by handling one single sample. For each country, we have 400 real samples and 2400 fake samples. $2/3$ of these samples are randomly selected and can be used as training data set and the rest can be used as testing data set. Nevertheless, to avoid a highly computational

complexity in the training and testing processes due to using the aforementioned samples, and to achieve a balance between the size of real and fake samples, we select the following size of training and testing samples.

In the training scenario: We select randomly 20 real samples and 20 fake samples from the training data set of each country. And as the inputs of the proposed models are pairs of IDs. So, we have totally 780 pairs for training the CFD model, distributed as: $20 \times 19 = 380$ (real-real) pairs, $20 \times 20 = 400$ (real-fake) pairs. And, totally we have 20×20=400 (real-fake) pairs for training the FsAFD model, as we have arbitrarily defined the first input as real and the second input as fake.

In the testing scenario: In all of our experiments, we test the performances of the proposed models on $\{30, 60, 90, 120, 150, 180, 210, 240\}$ samples, which are selected randomly from the testing dataset.

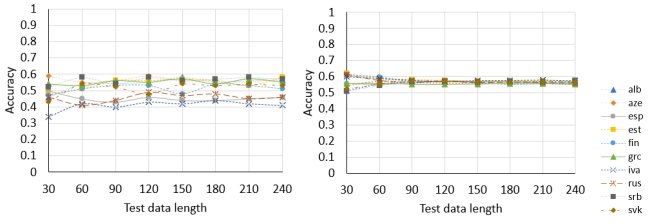
The training and testing implementation have been carried out on a local server (28 CPUs, 128 Go RAM, 1 $\times$ GPU Nvidia RTX 2080Ti), with the batch size = 8, and the number of epochs = 100. The Adam optimizer is used, where the learning rate (lr) equals $10e-4$ and the weight decay equals 0. The learning rate lr is scheduled every 20 epochs by $gamma = 0.1$. In (3) and 5, $\alpha = 0.5$ and $\delta = 0.5$. In (1), $\epsilon = 2.0$.

C. Evaluation Metrics

Four metrics are used in this paper to evaluate the performance of the proposed models, the accuracy, the precision, the $F1_{score}$, and the area under Curve (AUC). The definition of these metrics are reported in [3] [9].

D. Performance Test

Here, we report the performance results of the proposed models on the test data. The results are reported as an average of 5 execution rounds. Initially, Fig. 5 presents the obtained accuracy results of the proposed models on the test samples of 10 processed countries. In Fig. 5 we can see that the

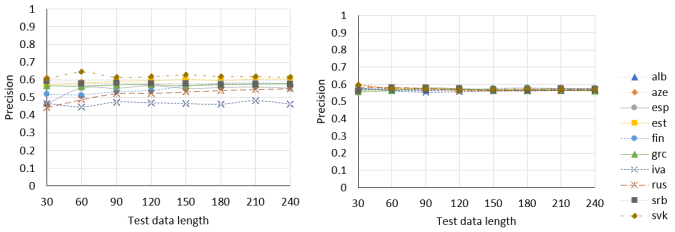


(a) (b)

Fig. 5: Accuracy results of (a) CFD model, (b) FsAFD model.

FsAFD model achieves better accuracy results in comparison to the CFD model. The accuracy results via the FsAFD model are superior to 55% for the 10 countries with most test data length. While, we can see that the accuracy results of CFD model range between 40%-60% with all test data length. Indeed, the accuracy results of CFD model exceed 50% for {alb,aze,est,fin,grc,srb}, and range between 40%-50% of {esp,iva,rus,svk}. That can be explained due to the bad quality of the guilloche patterns in these countries.

Secondly, Fig. 6 presents the precision results of the proposed models. The mentioned results in Fig. 6 are come

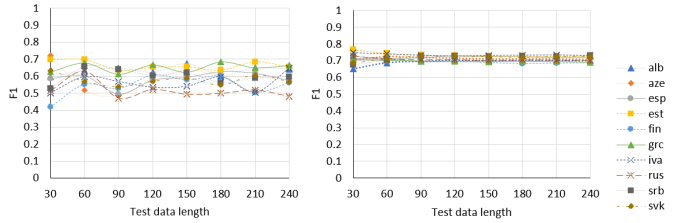


(a) (b)

Fig. 6: Precision results of (a) CFD model, (b) FsAFD model.

coherent with the accuracy results in Fig. 5. As we can see that the FsAFD model achieves better precision in classification between real and fake IDs in comparison to the CFD model. The precision results via the FsAFD model are superior to 55% for the 10 countries with the different test data length. As well as we can see that the precision results of CFD model range between 45%-60% with the different test data length. Indeed, the precision results on the test data of {iva,rus} countries were the worst; this is as we have mentioned before due to the bad quality of the guilloche patterns in these countries.

Thirdly, Fig. 7 presents the F1-score results of the proposed models. Obviously, we can see that the results of $F1_{score}$ in



(a) (b)

Fig. 7: F1-score results of (a) CFD model, (b) FsAFD model.

Fig. 7 are coherent with the aforementioned accuracy and precision results. Hence, we can see that the FsAFD model achieves more interesting $F1_{score}$ results compared to the achieved $F1_{score}$ results of the CFD model. The $F1_{score}$ of the FsAFD model exceed 65% for all countries. While, the $F1_{score}$ of the CFD model range between 45%-70% with different test data length of all countries. More precisely, we can see that the $F1_{score}$ results using CFD model on the test data of {iva,rus} countries were the lowest due to the bad quality of the guilloche patterns in these countries. In fact, the results of $F1_{score}$ give better measure of the incorrectly classified cases than the accuracy metric.

Finally, Fig. 8 summarizes the performances of the proposed models for distinguishing between the real and fake classes in terms of AUC for the 10 countries. We can see that the performance of the FsAFD model in distinguishing between

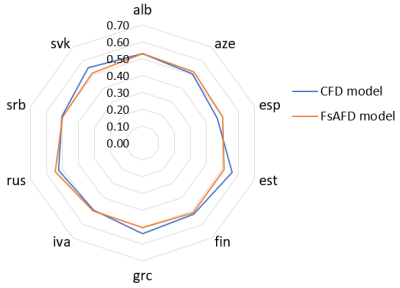


Fig. 8: AUC results of CFD and FsAFD models.

the real and fake classes in terms of AUC is slightly better than the performance of CFD model. Actually, we can see that the AUC of both models range between 50%-56%. Specifically, the AUC for {esp,iva} countries in CFD model does not exceed 50%. While it's equal to 56% for est, and 55% for svk countries. In FsAFD model the best AUC is obtained for {rus,alb,aze}, where the AUC is equal to 55%, 53%, and 52%, respectively.

E. Comparative Study and Discussion

To the best of our knowledge our work is the first attempt to design a forgery detection model on the IDs with respect to the guilloche patterns and no experiments or even results have been reported on the MIDV dataset in the literature. Therefore, a comparative study is not possible from a practical point of view. Indeed, this paper introduces the baselines for any future work in this domain. However, the novelty of our work can be demonstrated by making a systematic comparison between our work and the other works in [8], [9], which are the mostly relevant approaches to our proposal, mainly in the following aspects: (i) Generality of learning scheme: both [8] and [9] are not end-to-end learning models, as those models are concerned with specific regions of the document to analyze. While, our work is an end-to-end learning model regardless which region of the ID to analyze. Hence, the proposed approach authenticates a given ID at a whole, not merely zones targeted in the ID like in [8], [9]; (ii) Requirement of the original document (as a reference) to accomplish the fraud detection process: both [8] and [9] require the original IDs to accomplish the fraud detection process. While, our work does not require the original ID neither any other ID; (iii) Simplicity based on the number of used CNNs: the work of [8] used 1 CNN model (Siamese or Triplet) and the work of [9] used 3 CNN models (Siamese, Triplet, and PeleeNet). Similar to the work in [8], our work used 1 CNN model (Siamese). (iv) Types of processed documents: the work of [8] checks the performance of their model on four types of French IDs, and [9] test their model on banknotes of 12 countries and only on the Spain IDs. More generally, our work checks the authentication of the passports and the identity cards of 10 countries. (v) Creation of new dataset: the work of [8] used a private dataset, no forged documents are introduced publicly, and [9] adds 11 new country banknotes. While, our work introduces publicly 28000 fake IDs of 10 countries.

VI. Conclusion

In this paper, we proposed a new dataset called FMIDV containing forged IDs with respect to guilloche patterns. Moreover, two fraud detection models are proposed to develop a learnable classification model for distinguishing between real and fake IDs based on contrastive and fake-sample-adversarial learning. The first model learns the representations in a contrastive learning setting called CFD and the second model learns the representations based on contrastive and adversarial settings called FsAFD. The reported performance results on the MIDV and FMIDV datasets prove the achievement of the proposed models for predicting the correct label either real or fake for the given IDs. As a future work, we aim to greatly improve the accuracy and reliability of the verification process using the CNNs in ID verification based on Guilloche patterns.

References

[1] M. Al-Ghadi, P. Gomez-Krämer, and J.-C. Burie, "Checkscan: a reference hashing for identity document quality detection," in *Proc. SPIE12084, Fourteenth International Conference on Machine Vision (ICMV)*, vol. 12084. SPIE-Intl Soc Optical Eng, 2022, p. 120848.

[2] S. Usilin, D. Nikolaev, and D. Sholomov, "Guilloche elements recognition applied to passport page processing," in *Conference: 8^{th} Open German - Russian Workshop Pattern Recognition and Image Understanding*, 2011, pp. 1–5.

[3] O. Kada, C. Kurtz, C. van Kieu, and N. Vincent, "Hologram detection for identity document authentication," in *Pattern Recognition and Artificial Intelligence*, M. El Yacoubi, E. Granger, P. C. Yuen, U. Pal, and N. Vincent, Eds. Cham: Springer International Publishing, 2022, pp. 346–357.

[4] T. S. Chernov, D. P. Nikolaev, V. M. Kliatskine, T. S. Chernov, D. P. Nikolaev, and V. M. Kliatskine, "A method of periodic pattern localization on document images," in *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, vol. 9875. SPIE, 2015, p. 987508.

[5] N. Ghanmi and A. M. Awal, "A new descriptor for pattern matching: application to identity document verification," in *Proceedings - 13th IAPR International Workshop on Document Analysis Systems, DAS*, 2018, pp. 375–380.

[6] M. Sirajudeen and R. Anitha, "Forgery document detection in information management system using cognitive techniques," *Journal of Intelligent & Fuzzy Systems*, vol. 39, pp. 8057–8068, 2020.

[7] A. Castelblanco, J. Solano, C. Lopez, E. Rivera, L. Tengana, and M. Ochoa, "Machine learning techniques for identity document verification in uncontrolled environments: A case study," in *Mexican Conference on Pattern Recognition*. Springer, 2020, pp. 271–281.

[8] N. Ghanmi, C. Nabli, and A. M. Awal, "CheckSim: A reference-based identity document verification by image similarity measure," in *Document Analysis and Recognition – ICDAR 2021 Workshops*, vol. 12916 LNCS. Springer Science and Business Media Deutschland GmbH, 2021, pp. 422–436.

[9] A. B. Centeno, O. R. Terrades, J. L. Canet, and C. C. Morales, "Recurrent comparator with attention models to detect counterfeit documents," in *Proceedings of the International Conference on Document Analysis and Recognition, ICDAR*. IEEE, 2019, pp. 1332–1337.

[10] K. Bulatov, E. Emelianova, D. Tropin, N. Skoryukina, Y. Chernyshova, A. Sheshkus, S. Usilin, Z. Ming, J.-C. Burie, M. M. Luqman, and V. V. Arlazarov, "MIDV-2020: A comprehensive benchmark dataset for identity document analysis," *Computer Optics*, pp. 252–270, 2021.

[11] C. L. Li, K. Sohn, J. Yoon, and T. Pfister, "CutPaste: Self-supervised learning for anomaly detection and localization," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 9659–9669, 2021.

[12] S. Akcay, A. Atapour-Abarghouei, and T. P. Breckon, "GANomaly: Semi-supervised anomaly detection via adversarial training," in *Asian Conference on Computer Vision (ACCV)*, vol. 11363 LNCS. Springer Verlag, 2019, pp. 622–637.

[13] S. Dey, A. Dutta, J. I. Toledo, S. K. Ghosh, J. Llados, and U. Pal, "SigNet: Convolutional Siamese network for writer independent offline signature verification," *Pattern Recognition Letters*, vol. 1, pp. 1–7, 2017.