Universidade de Pernambuco
Escola Politécnica de Pernambuco
Programa de Pós-Graduação Acadêmica em Engenharia de Computação

Victor Kléber Santos Leite Melo

A Deep Learning Approach to Generate Off-line Handwritten Signatures Based on On-line Samples

Dissertação de Mestrado

Recife, setembro de 2017

Universidade de Pernambuco
Escola Politécnica de Pernambuco
Programa de Pós-Graduação Acadêmica em Engenharia de Computação

Victor Kléber Santos Leite Melo

A Deep Learning Approach to Generate Off-line Handwritten Signatures Based on On-line Samples

Dissertação de Mestrado

Dissertação apresentada ao Programa de Pós-Graduação acadêmico em ENGENHARIA DE COMPUTAÇÃO da Universidade de Pernambuco como requisito parcial para obtenção do título de Mestre em Engenharia de Computação.

Prof. Dr. Byron Leite Dantas Bezerra
Orientador

Recife, setembro de 2017

O epígrafe é uma pagina onde o autor pode colocar uma citação ou pensamento que, de alguma forma, influenciou em seu trabalho acadêmico.

Abstract

One of the main challenges of off-line signature verification is the absence of large databases. A possible alternative to overcome this problem is the generation of synthetic signature databases. In this work, a novel method for the generation of synthetic off-line signatures based on dynamic information is presented. In contrast to the state-of-the-art, we propose an synthesis approach under the perspective of supervised training, in which our learning model is trained to perform the task of "on-line signature to off-line signature conversion". The proposed approach is based on a Deep Convolutional Neural Network trained to learn how on-line handwritten manuscripts of the IRONOFF dataset are transformed into the off-line domain. The main goal of the proposed method is to synthetically enlarge existing off-line signature datasets based on on-line signature samples towards an improvement on the recognition rates of off-line signature verification systems. For these purposes, a machine-oriented evaluation on the BiosecurID signature dataset is carried out. We show that the synthetic samples generated with our proposed method achieve a verification performance similar to the one offered by real signatures and promising improvements of the Equal Error Rate results in comparison with and the current state-of-the-art method.

Resumo

Um dos principais desafios de sistemas de verificação de assinaturas *off-line* é a ausência de grandes conjunto de dados. Uma alternativa possível para superar esse probema é a geração de assinaturas sintéticas. Neste trabalho é proposto um método para a geração sintética de assinaturas off-line baseado em informações dinâmicas. Em contraste com o estado-da-arte, o método método de síntese proposto se baseia na perspectiva da aprendizagem supervisionada, o nossa máquina de aprendizagem é treinada para realizar a tarefa de "conversão de assinatura *on-line* para *off-line*". O método proposto é uma *Deep Convolutional Neural Network* treinada para aprender como textos manuscritos *on-line* da base IRONOFF são transformados para o domínio *off-line*. O objetivo principal do método proposto é o de aumentar sinteticamente bases de assinatura *off-line* baseando-se em amostras *on-line* em direção a uma melhora nas taxas de reconhecimento de sistemas de verificação de assinaturas *off-line*. Para isso, uma avaliação na base de assinaturas BiosecurID é realizada. Mostra-se que as amostras sintéticas geradas pelo método proposto obtém uma performance de verificação similar aos oferecidos por assinaturas reais e uma melhora promissora no *Equal Error Rate* em comparação com o método do estado-da-arte.

Contents

List of Figures

List of Tables

List of symbols and abbreviations

ABNT	Associação Brasileira de Normas Técnicas
abnTeX	ABsurdas Normas para TeX
Γ	Letra grega Gama
Λ	Lambda
ζ	Letra grega minúscula zeta
$\in$	Pertence

Acknowledgements

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

CHAPTER 1

Introduction

In the modern society, biometric technology is used in several security applications for personal authentication. The aim of such systems is to confirm the identity of a given subject based on physiological or behavioral traits. In the first case, recognition is based on biological characteristics such as fingerprint, palm print, iris, face. The latter relies on behavioral traits such as voice pattern and handwritten signature [1].

The Handwritten Signature biometry stands as one of the primary methods for identity authentication. One of the reasons for its widespread is the fact that signature acquisition is easy, non-invasive, and most individuals are familiar with its use in their daily life [2]. Due to its convenient nature, signatures can be employed as a sign of confirmation in a wide set of documents, namely, bank checks, identification documents and a variety of business certificates and contracts.

As a behavioral trait, signatures present a high intra-user variability and are susceptible to spoof attacks, which is the attempt to forge the signature of a legitimate subject [1]. Two types of impostors are considered: casual impostors (producing random forgeries) when no information about authentic writer signature is known, and real impostors (producing skilled forgeries) when some information of the signature is used [3].

If a signature on a document is forged, this document is also considered invalid. Thus, preventing frauds in the signature verification process has been a challenge for researchers around the world. However, manual signature-based authentication of a large set of documents is a time-consuming and labor-intensive task. Hence, several Automatic Handwritten Signature Verification Systems (AHSVS) have been proposed to support this task. These systems aim to automatically decide if a query signature is in fact of a particular person or not.

An AHSVS is essentially a pattern recognition system that receives a signature as input, extracts a feature set from the data and classifies the sample using a template database as the reference. These datasets contain signatures digitized either by using an optical scanner to obtain the signature directly from the paper or using an acquisition device such as digitizing tablets or electronic pens with digital ink. The two domains are identified as off-line (static) and on-line (dynamic), respectively. In the on-line modality, data is stored during the writing process and consists of a temporal sequence of the two-dimensional coordinates (x, y) of consecutive points, whereas in the off-line case, only a static representation of the completed writing is available as an image. Moreover, each representation has specific attributes not present in the other [4].

In order to improve the performance of signature verification systems, bigger databases are required. Since the acquisition and distribution of real signatures arise legal and privacy concerns, the use of realistic synthetic signatures could be regarded as a good alternative. As a consequence, over the last years, several works on both on-line [5], [6] and off-line [7], [8] signature synthesis have been carried out. These synthetically generated signatures show a similar behavior to real ones, thus enabling to enlarge existing databases and offering new possibilities for off-line recognition.

Some efforts have been performed on the generation of synthetic static data taking into account dynamic features during the synthesis process [9]. Among others, this type of synthesis approach presents the following possible practical applications: (i) generation of synthetic static samples to be fused with the original on-line signatures in order to improve the performance in an on-line verification scenario; (ii) enlarge existing off-line signature databases; (iii) development of systems capable of integrating both on-line and off-line samples interchangeably, towards a unified signature biometry.

Despite the advancements for this category of synthesis, the synthetic off-line samples created with the state-of-the-art systems still struggle to improve the recognition rates when used to enlarge existing off-line signature databases.

In this work, we propose an approach based on Fully Convolutional Neural Networks (FCN) trained in a supervised manner, to learn the representation of off-line manuscripts using as the input the on-line representation, expecting that the network predicts the corresponding static sample. This type of approach is interesting for our problem since the neural network learns how the dynamic features, in particular, the pressure, of the on-line representation of the manuscript translates into the static domain (pen on the paper).

In contrast to the models proposed in the literature [7], [8], [9], the approach proposed in this work is designed under the perspective of supervised training. In which a learning model is trained to perform the task of "on-line to off-line conversion" using as the training data a data set containing both the on-line and off-line versions of manuscripts. We expect that the Deep Neural Network model can learn how on-line information is transformed into the off-line manuscript. Moreover, we expect that the trained model synthesizes off-line signatures with improved discriminative power (i.e., better recognition rates).

1.1 Problem statment

Encouraged by the motivations depicted previously the goal of this dissertation can be stated as follows:

"The goal of this work is to design an approach to generate synthetic off-line handwriting signatures based on on-line data for biometric purposes, modeling this problem as a supervised machine learning task, using a Deep Convolutional Neural Network."

This statement is developed through the following actions: (i) Creation and training of a Deep Neural Network model able to translate dynamic handwritten information into an off-line manuscript (ii) Generation of an off-line synthetic dataset based on a publicly available on-line signature dataset (iii) Compare the proposed approach's performance with state-of-the-art methods and to evaluate the closeness of synthetic signatures with respect to real signatures.

To achieve the point (iii), machine-oriented validations are carried out. A state-of-the-art automatic signature verifier is used with publicly available signature databases and our synthetic specimens. It is expected that similar results will be obtained with both kinds of signatures. Moreover, we also evaluate the use of synthetic signatures in the enrollment set analyzing the improvements in the system performance.

1.2 Dissertation structure

From this introduction, the remainder of this work is organized as follows:

TODO Chapter 3 presents the theoretical background about the main topics around this study: automatic handwritten signature verification, synthetic signature generation from on-line data and previous studies performed in this context and describe the concept of Deep Learning. Chapter 4 describes our proposed method. Chapter 5 presents the experimental protocol and results. Finally, in Chapter **??** conclusions of this study are presented together with suggestions for future work.

CHAPTER 2

Handwritten Signature Verification

In this chapter, we introduce some essential concepts related to Handwritten Signature Verification systems used in this work. First, we give an introduction and a general overview of the handwritten signature biometry, then we discuss how an Automatic Handwritten Signature Verification system works and finally we give a brief overview of the state-of-the-art on off-line signature synthesis based on on-line data.

2.1 Handwritten Signature: a behavioral biometry

The term “Biometrics” is derived from the Greek word “bio-metriks”. In which “bio” means “life” and “metrics” means “to measure”. Biometrics refers to the measurements and statistical analysis of unchanging biological characteristics peculiar to an individual. Biometric systems are a constantly growing technology [1] and have been introduced as forms of identification and access control. Biometric identifiers are a unique measurable characteristic used to distinguish and describe individuals [10].

Biometric systems are often categorized as physiological or behavioral [11]. The physiological category is related to measurements of the body. Examples include fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris/retina pattern, and body scent, while behavioral characteristics are acquired traits by an individual and are related to the pattern of behavior of a person. They include typing rhythm, gait, temperament, voice, and handwritten signatures [12].

Most biometric identifiers require a special type of device for security and control of human identity. However, handwritten signature based biometric systems can be realized requiring no sensor except a pen and a piece of paper. According to [13] handwritten signatures are considered the most legal and social attributes for person identification. Nevertheless, the challenge that comes with automatic signature-based authentication is the need for high accuracy results to avoid false authorization or rejection.

Handwritten signature authentication is based on systems for signature verification. Whether a given signature belongs to a claimed person or not is decided through a signature verification system, which ultimately strives to learn the manner in which an individual makes use of their muscular memory (hands, fingers and wrist) to reproduce a signature [14].

A generic handwritten signature based biometric system is shown in Figure 1. Once the user $\boldsymbol{Y}$ deposits the signature, a sensor digitalizes the sample. Later, a feature matrix $\boldsymbol{X}$ is built with the information extracted from the input sample. Next, the systems typically have two stages: enrollment $\boldsymbol{X_E}$ and recognition $\boldsymbol{X_R}$. The former builds a system database $\boldsymbol{D}$ where the users store their reference signatures as a set of templates, whereas the latter is used to recognize, identify or verify the identity of a user, who typically claim to be one of the registered users. Then, a score $\boldsymbol{S}$ is obtained according to the similarity of the questioned sample to the claimed template. Finally, the system accepts or rejects the questioned sample.

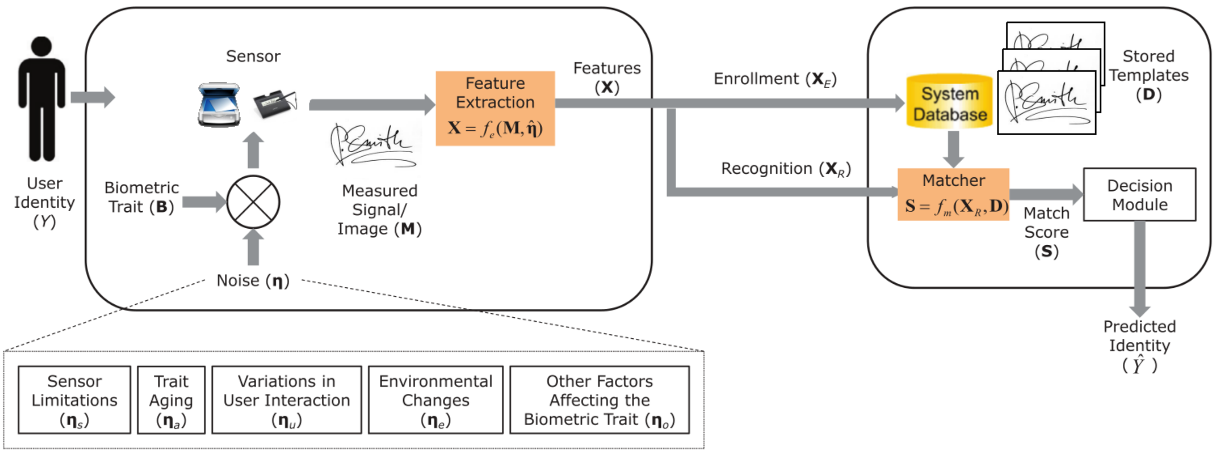


Figure 1 – Overview of a typical handwritten signature based system. Figure adapted from [12].

As Figure 1 shows, the signature acquisition sensor can be either an optical scanner or an acquisition device such as a digitizing tablet. These two different acquisition tools characterizes the two classes of signatures, namely: static and dynamic.

In the static modality, also referred to as off-line, an optical scanner is used to obtain the signature directly from the pen on the paper and only the digital image of the signature is available, see Figure 2 (a). In the dynamic mode, also called on-line, signatures are acquired by means of a graphic tablet or a pen-sensitive computer display, see Figure 2 (b). In this mode, data is stored during the writing process and consists of a temporal sequence of the two-dimensional coordinates (x, y) of consecutive points.

An example of a colored off-line signature and a plotted matching on-line signature can be found in Figure 3. Specifically, what characterizes both domains is that the on-line singatures do not convey information about the overall shape of the signature, the width of the strokes and the texture of the ink on the paper [9], whereas the off-line representation has lost all dynamic information about the manner in which the signature is signed during the acquisition process. As a result, features such as pen trajectory, which can be easily computed in the on-line domain, can only be inferred from a static image [15].

(a) (b)

Figure 2 – Different signature acquisition methods. (a) a signature scanned from paper and (b) digitizing tablet Wacom STU-500 [16].

Figure 3 – An off-line and a matching on-line signature sample. Figure extracted from [17].

Once the signature sample is acquired, during the enrollment phase the system tries to create the subject identity based on behavioral features in the signature. Because of the way we sign, however, it is a subtle task. The rapid movement behind the signature creation is determined by a motor program stored in the brain of each signer applied to tools such as pen and paper [18]. According to [19] the handwritten signatures can be influenced by country, age, time, habits, acquisition tool, psychological or emotional state, creating a significant variability that must be taken into account in the authentication process.

In fact, the unpredictable intra-personal variability, i.e. the similarity between signatures executed by the same writer, is a crucial challenge of signature-based biometric systems. This variability can be attributed to the several sources of noise (η) that distort the measured trait. According to Figure 1, the intra-personal variability which affects the measured sample $\boldsymbol{M}$

can be characterized by: sensor limitations like resolution or sample rate; biological aging effects or cognitive-motor impairments; user interaction with the sensor; environment changes like background noise and; other factors as consequence of the individuals' mood, hurry or unwillingness to cooperate. This effect is illustrated in Figure 4.

Figure 4 – Superimposed genuine signatures of the same writer. A high intra-class variability can be noticed. Extracted from [20].

Figure 5 – The first column signatures are genuine references, the following three samples are questioned signatures. How many forgeries would you be able to detect?[1] Signatures extracted from [21].

Another challenge faced by signature-based biometric systems is the unpredictable inter-personal variability, i.e. the similarity between signatures executed by different writers. In a signature-based system, inter-personal variability is mainly attributed to frauds related to malicious people faking the identity of signers. In the field of signature verification forgeries are generally classified in two different types of forgeries.

- The first one is the random forgery which is created in a situation which an impostor who has no information about the person or the shape of the original signature tries to verify the identity of a signer by using his own genuine signature. The random forgery test is a typical test used in access control and commercial transactions.

[1] From left to right, top to bottom (F means Forgery and G means Genuine): FGF FFG GFF

- The second type is the skilled forgery, represented by a proper imitation of the genuine signature model. The forger has access for both the user's name and signature, and learns the signature of a signer and tries to reproduce it with a similar intra-class variability. This test is the most relevant in signature verification for its impact in forensic applications in signature forgery detection. Figure 5 illustrates a visual comparison between genuine signatures and skilled forgeries.

2.2 Automatic Handwritten Signature Verification

An Automatic Handwritten Signature Verification System (AHSVS) is essentially a pattern recognition application. Pattern recognition is one of the most important and active fields of research. During the past few decades, there has been a considerable growth of interest in problems of pattern recognition, and in the last few years, many methods have been developed in this area.

As any Pattern Recognition system, an AHSVS has three phases: data acquisition and preprocessing, feature extraction and classification [2]. In the first step, the signatures are acquired and preprocessed, the main goal here is to correct geometric distortions and remove noise related to the signature acquisition sensor. After the images are acquired and treated, features are extracted and stored in a knowledge database. On the classification step, the extracted features are used to distinguish between genuine and forged signatures. Therefore the Signature Verification task is, in essence, a two-class classification problem, in which the system's prediction to the input signature sample is either genuine or fraud.

Verification errors occurring in AHSVS are usually categorized as two types [22]. On the one hand, a genuine signer may be rejected by the system as a potential impostor (e.g. it could happen when the signer carelessly executes his/her signature), resulting in what is denoted a Type-1 error or False Rejection. On the other hand, a skilled forger might be able to produce a sample which would be accepted as genuine, resulting in what is called a Type-2 error or False Acceptance.

Therefore, AHSVS efficiency is quantitatively measured by two rates: False Rejection Rate (FRR) which is the percentage of genuine signatures treated as forgeries, and False Acceptance Rate (FAR) which is the percentage of forged signatures treated as genuine. A derived metric that is usually used is the Average Error rate (AER) which is the average of FAR and FRR. Moreover, when experimenting an AHSVS, the trade-off between FRR and FAR must be taken into account based on the type of application and other aspects related to where the system is used. When the decision threshold of a system is set to have the FRR approximately equal to the FAR, the Equal Error Rate (EER) is calculated.

In order to improve the performance of signature verification systems, bigger databases are required. The amount of data available for each user is often insufficient in real applications.

During the enrollment phase, users are often required to supply only a few samples of their signatures. In other words, even if there is a significant number of users enrolled in the system, a classifier needs to perform well for a new user, for whom only a small set of samples are available. Since the acquisition and distribution of real signatures arise legal and privacy concerns, the use of realistic synthetic signatures could be regarded as a good alternative.

2.3 Off-line Signature Synthesis Using On-line Samples

TODO - quero colocar aqui uma visão geral das propostas existentes do estado da arte

assessment [23]

rabasse 2008 [24]

ferrer synthetic online to synthetic offline [8]

[9]

[25]

CHAPTER 3

Neural Networks and Deep Learning

This chapter introduces and gives a brief overview of the theoretical concepts related to Neural Networks, and Deep Learning treated in this work. The first section gives an overview of Artificial Neural Networks, the next section we give an introduction and a general overview of the deep learning research field. Later, we briefly describe the fundamentals of CNN's and present the Fully Convolutional Networks, which is a model concept used in this work. Finally, we present the techniques used for training our model.

3.1 Neural Networks

A biological neural network is an essential part of human brain. The human brain is a highly complex information processing system capable of interpreting large amounts of information and making decisions. It is a complex, non-linear and parallel "computer" consisting of millions of connected neurons [26]. In many tasks, the human brain is more efficient than computers. For instance, the human brain can recognize a familiar face in about 100-200 ms, while modern computers require minutes or even hours for solving the same problem [26].

Based on examples and feedback from the "teacher", our brain allows us learning how to distinguish an apple from an orange or recognize letters. Moreover, even without the "teacher", we are still able to group similar patterns. Those and other strengths of human brain challenged scientists to emulate those processes by researching how to use machines for tasks that are common for humans. Moreover, one of the concepts that appeared as the result of that research is the Artificial neural network (ANN) concept. Which can be thought of as an approximation or fitting function.

The first of these models was the perceptron [27], which simulates a single neuron and is the elemental computing unit of an ANN. The learning rule algorithm for learning relations in data can be summarized as: for every input x_i, make a linear prediction about its label: $y_i^* = w^T x_i$ and update the weights (w) as,

$$w \leftarrow w + x_i(y_i - y_i^*) \tag{3.1}$$

Nonetheless, a critical evaluation by Minsky and Papert [28] showed that "for data sets that are not linearly separable, the perceptron learning algorithm will never converge" [29]. This observation is related to the perceptron's limited representational power, the learning rule only converges to the correct solution if the data is linearly separable.

Stacking several perceptron units together in one layer and connecting these stacks sequentially, without connections between the neurons in the same layer, produces what is known as a multilayer perceptron (MLP) neural network. A MLP can be thought of as a function that maps from input to output vectors. Since the behavior of the function is parameterized by the connection weights, a single MLP is capable of instantiating many different functions. It has been proven [30] that a MLP with a single hidden layer can approximate any continuous function on a compact input domain to arbitrary precision. For this reason MLPs are said to be *universal function approximators* [30].

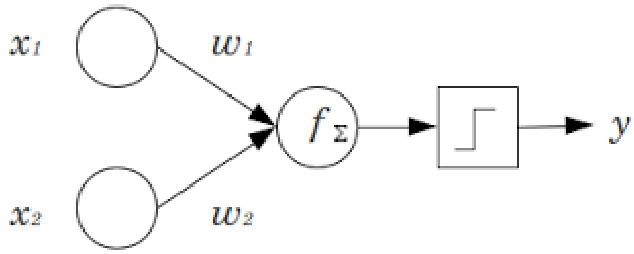


Figure 6 – Perceptron representation. x_1 and x_2 represent the input signal, w_1 and w_2 the weights, $f_\sum$ is the activation function (in this case, a step function) and the output signal is given by y.

Figure 11, Figure 12. Simple convolution [2] With strides [3]

[2] Animated representation can be found in: <https://raw.githubusercontent.com/vdumoulin/conv_arithmetic/master/gif/no_padding_no_strides.gif>

[3] Animated representation of strides can be found in: <https://raw.githubusercontent.com/vdumoulin/conv_arithmetic/master/gif/no_padding_strides.gif>

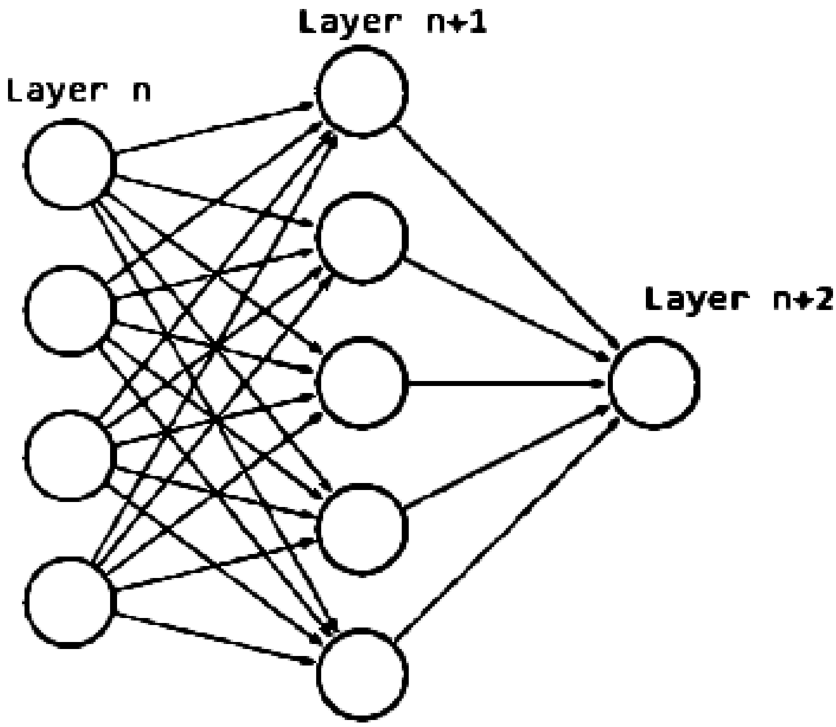


Figure 7 – Multilayer perceptron representation. Each layer contains several perceptron units, which are then connected to units in the subsequent layer.

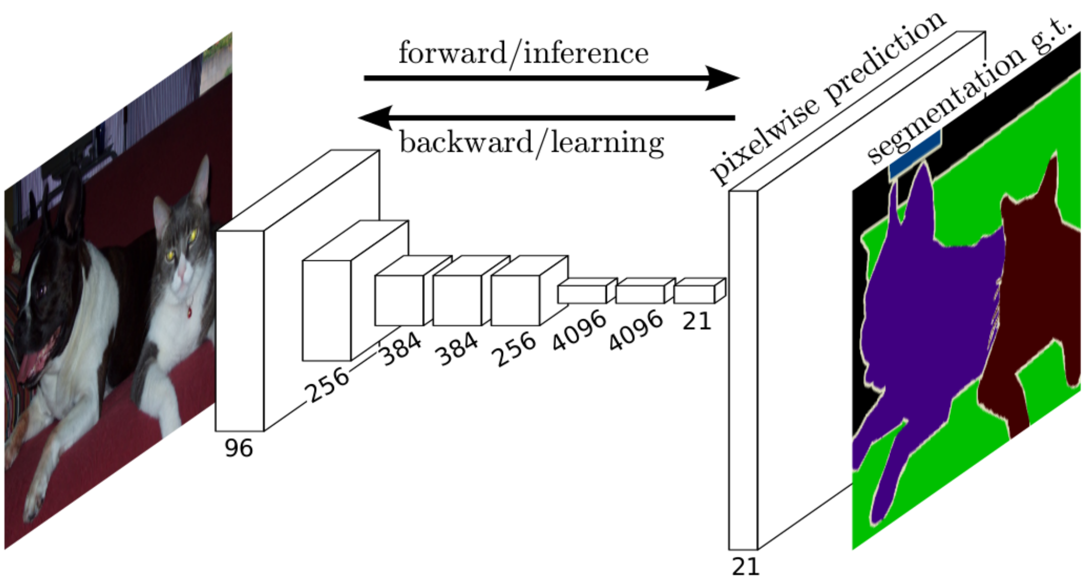
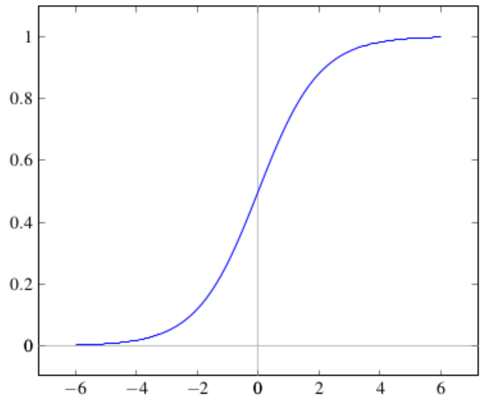
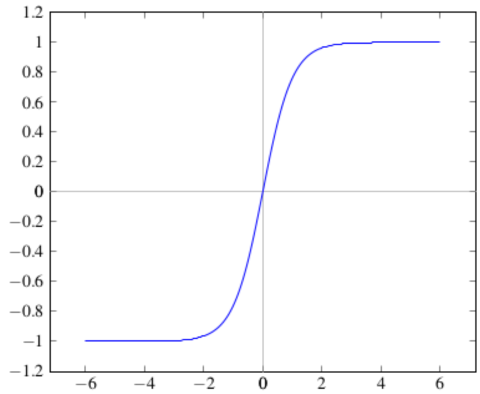


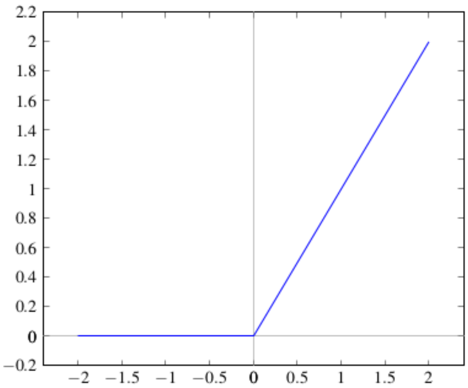
Figure 8 – Fully convolutional networks can efficiently learn to make dense predictions for per-pixel tasks like semantic segmentation. Extracted from [31]



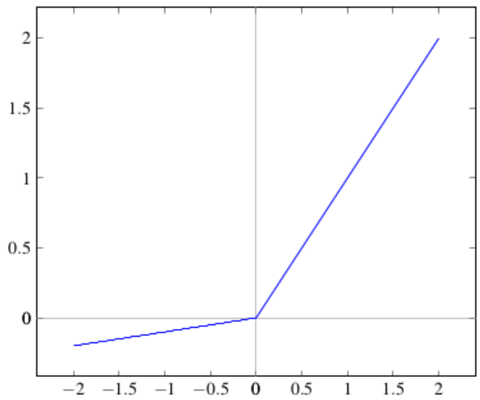
(a) Sigmoid



(b) Tanh



(c) ReLU



(d) LReLU

Figure 9 – Neural network activation functions.

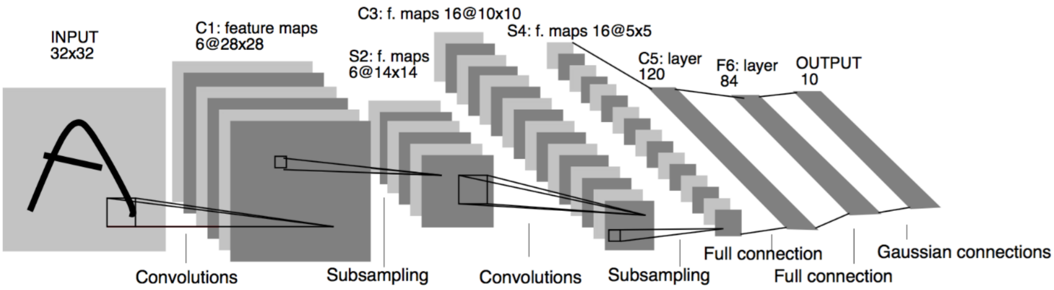


Figure 10 – Lenet, [32].

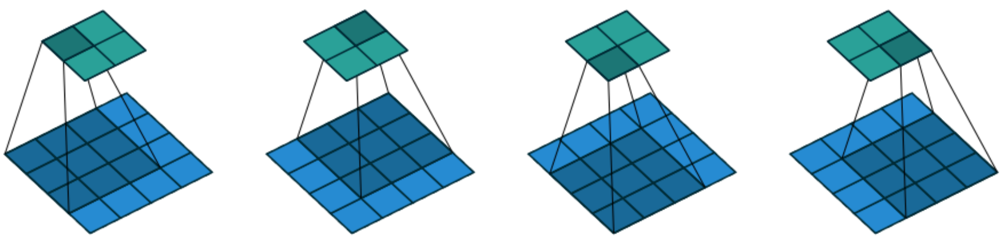


Figure 11 – Convolving a 3x3 kernel over a 4x4 input. Extracted from [33].

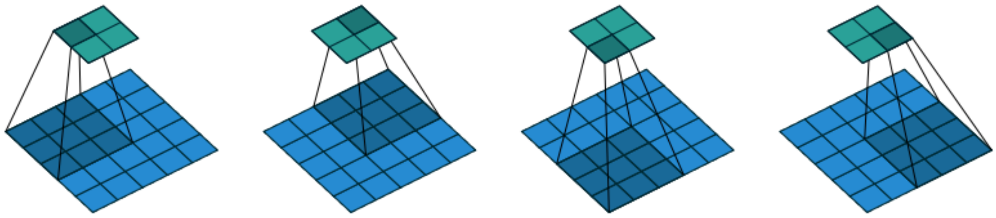


Figure 12 – Convolving a 3x3 kernel over a 5x5 input using 2x2 strides. Extracted from [33].

3.1.1 Backpropagation

3.1.2 Loss function

3.1.3 Activation function

3.1.3.1 Linear

3.1.3.2 Sigmoid

3.1.3.3 ReLU

3.1.3.4 LReLU

3.2 Convolutional Neural Networks

3.2.1 Layers

3.2.1.1 Convolution

3.2.1.2 Transposed Convolution

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

3.3 Neural Networks training

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

3.3.1 Weight initialization

3.3.1.1 Uniform

3.3.1.2 Glorot

3.3.2 Optimization algorithm

3.3.2.1 Stochastic Gradient Descent

3.3.2.2 Adaptive Moment Estimation

CHAPTER 4

Proposed Method

Although a simple static signature can be generated linking the points of the dynamic trajectory, additional dynamic information could be used to enrich the static signature. This addition is expected to lead more realistic and more discriminative images. Figure 13 gives an overview of the proposed approach. In this section, we describe our proposed approach. First, the dataset used to train our model is described. Afterwards, we describe how the data was preprocessed. Finally, the CNN model is detailed.

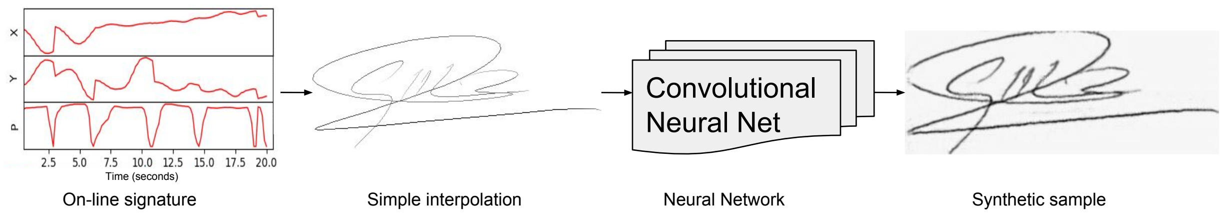


Figure 13 – The proposed approach diagram and an example of the synthetic signature generation.

4.1 Training Dataset

The neural network was trained using the data from the IRONOFF [4] dataset, this database contains on-line manuscripts mapped to the corresponding static handwriting sample. It contains 1000 digitized documents in English and French written by 700 different writers.

4.2 Preprocessing

The neural networks expect inputs of a fixed size, where signatures vary significantly in shape (in BiosecurID, they range from small signatures of size 153x258 to large signatures of size 819x1137 pixels). In order to have a fixed size, we first normalize the images to the largest image size, by padding the images with white background. In this case, we centered the signatures in a canvas of size 840x1360 pixels, aligning the center of mass of the signature to the center of the image, similar to previous approaches in the literature, e.g. [34]. We then rescaled the images to 383x150 pixels. This size was chosen to be large enough to keep details from the pen strokes in the manuscript, while still small enough to enable to train on the GPU.

Besides resizing the images to a standard size, we also performed the following preprocessing steps:

- Inverted the images: we inverted the images so that the white background corresponded to pixel intensity 0.
- Normalized the input: we normalized the input to the neural network by dividing each pixel by the standard deviation of all pixel intensities. We do not normalize the data to have mean 0 (another common pre-processing step) since we want the background pixels to be zero-valued.
- Interpolation: The on-line sequences (x_t, y_t, p_t) are linearly interpolated using Bresenham's line algorithm to obtain 8-connected sequences.

Figure 14 shows an example of the preprocessed input and the ground truth that are fed to the neural network during training phase.

(a) input (b) ground truth

Figure 14 – Preprocessed data used during the training phase. (a) is the interpolated on-line sample, used as input and (b) is the expected prediction from the neural network, the ground truth.

4.3 Neural Network model

Our model is based on the concept of autoassociative memory [35], [36], commonly known as autoencoders. Autoencoders are normally used to reduce high-dimensional data into a low-dimensional code to later reconstruct the data from the compressed code, i.e., the desired output is the same of the input pattern [37], [38]. In our case, instead of expect the output to be the same as the input, our Neural Network model is fed with the interpolated on-line sample and we expect the respective off-line sample on the output, i.e. the input is the dynamic information and the desired output is the static manuscript.

We use an architecture based on the Convolutional Autoencoder [39]. The expectation is that by learning to transform between on-line information to off-line manuscripts, the network will learn convolution filters that are relevant to synthesize off-line signatures based the on-line sample.

Layer	Size
Convolution	16x3x3
Convolution	32x3x3
Convolution	32x3x3
Convolution	64x3x3
Transpose Convolution	64x3x3
Transpose Convolution	32x3x3
Transpose Convolution	32x3x3
Transpose Convolution	16x3x3

Table 1 – Summary of the CNN Layers

For the purpose of replicating our experiment, we provide a full list of the parameters used in our tests. Table **??** lists the definition of the Convolutional Autoencoder layers. For convolution and transpose convolution layers, we list the size as NxHxW where N is the number of filters, H is the height and W is the width of the convolution and transpose convolution windows, respectively. For every layer we use a stride (the distance between applications of the convolution operation) of 2x2, and we pad the input for every layer with 0 evenly left and right. We use Leaky Rectified Linear Units (LReLUs) as the activation function for all convolutional layers. The weights of the model are initialized using the technique proposed by Glorot and Bengio [40], and the biases to 0. We trained the model with Adam optimizer to minimize the minimum squared error (MSE) loss for 100 epochs, using a learning rate of 0.001, and mini-batches of size 16. The network was trained using the library Tensorflow, and took around 72h to train on a GTX 670 GPU.

CHAPTER 5

Experimental Evaluation

In order to evaluate the quality of the synthetic signatures generated by our system we follow the same protocol presented on the work of Diaz [9]. Namely we use a state-of-the-art off-line verification system and a dataset comprising both on-line and off-line signatures in order to train the verification system to evaluate the synthetic signatures.

The main idea of the experiments is to measure the quality of the synthetic signatures taking into account an off-line verification system performance. The questions raised on the experiments are (i) is the synthetic signatures system performance similar to the real off-line signatures performance? (ii) is the performance even if the enrollment protocol changes? (iii) is it feasible to increase the number of samples at the enrollment stage with synthetic signatures?

5.1 Off-line signature verification system

The system used for the evaluation of the real and synthetic signatures is a Linear SVM classifier and is based on a state of the art feature extraction approach [41]. The feature extraction system [4] use ideas from transfer learning and multi-task learning to learn features using Convolutional Neural Networks (CNN).

SVMs represent a special class of linear classifiers. In order to classify a pattern as belonging to one of two classes, an SVM constructs a hyperplane in the feature space, such that it maximally separates the margin between the two classes. For this reason, SVMs are also referred to as maximum margin classifiers

[4] https://www.etsmtl.ca/Unites-de-recherche/LIVIA/Recherche-et-innovation/Projets/Signature-Verification

5.2 Evaluation Database

The evaluation experiments were carried out on the BiosecurID database [42]. This multimodal database comprises on- line and off-line signatures of 400 users. Signatures were captured using a special digital inking pen on a paper placed over a digitizing tablet. This way, both versions, on-line and off-line, of the exact same real signature were acquired at the same time. The database was captured in 4 sessions distributed over 4 months. Each subject signed 4 times and forged 3 signatures, thus leading to 4x4 = 16 genuine samples and 3x4 = 12 skilled forgeries. The performance of the real and synthetic signatures is evaluated on a subset of 132 subjects.

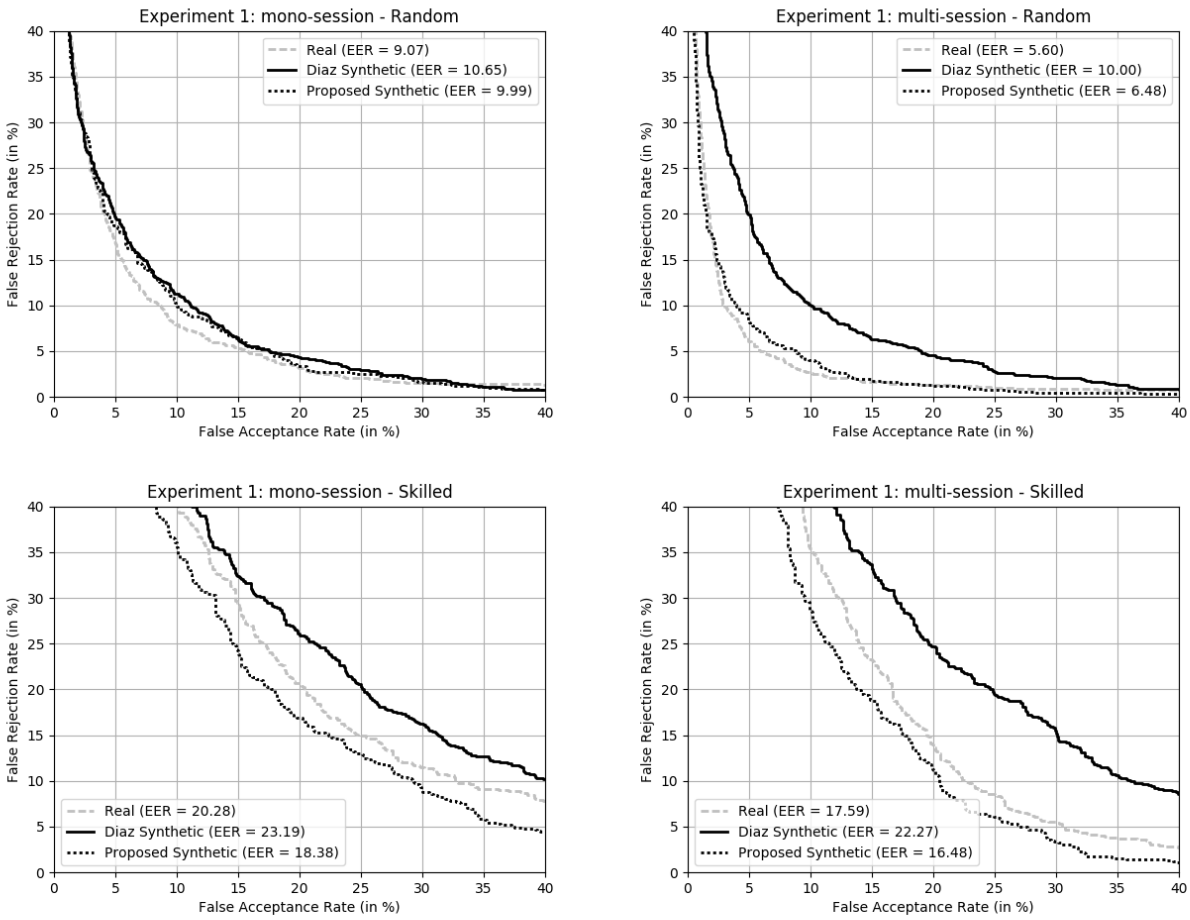


Figure 15 – DET curves for real off-line signatures and synthetic signatures (from Diaz and our proposed method), for the first experiment (mono-session and multi-session enrollment), for the two scenarios considered (random and skilled impostors)

5.3 Experimental Protocol

In order to answer the questions stated at the beginning of this section and accomplish a fair comparison of our work and the state of the art, we follow the same experiment protocol proposed by Diaz [9]. Two different experiments are carried out. The Experiment 1 focus on evaluating the synthetic signatures performance in comparison to real signatures and the Experiment 2 evaluates the feasibility of synthetically increasing the number of samples available in a dataset.

For both experiments the BiosecurID dataset is split into two subsets. The first 90 users are separated as the enrollment set, used to compute the genuine and skilled impostor scores. The remaining 42 authors are considered as the test set and are used to compute the random impostor scores. The performance is evaluated in terms of equal error rate (EER), which is the point in the Detection Error Tradeoff curve (DET) where the false acceptance rate equals the false rejection rate.

5.3.1 Experiment 1: synthetic signatures in comparison to real signatures

Two different protocols have been considered to compute the 90 user enrolled models: (i) a mono-session approach, using the four samples of the first session (ii) a multi-session approach, using one sample of each session.

In both cases, genuine scores are computed matching the non-enrolled genuine samples of the subject (12) to the enrolled model (90×12 = 1080 genuine scores). Random impostor scores are calculated comparing the first sample of the test subjects to the enrolled model, leading to 90×42 = 3780 random impostor scores, and skilled impostor scores are calculated with the skilled forgeries samples of the enrolled users (12 per subject) to the enrolled model (90×12 = 1080 skilled impostor scores).

5.3.2 Experiment 2: synthetically increasing the enrollment samples

This experiment is designed to assess whether synthetically increasing the enrollment dataset leads to a better recognition performance. Three different enrollment sets are considered in this experiment:

- 4 real samples belonging to the first acquisition session
- 8 real samples belonging to the first and the second sessions
- 4 real samples belonging to the first session plus 4 synthetic samples belonging to the second session.

5.4 Statistical Evaluation

CHAPTER 6

Experiments Result

As described in Chapter 5, two different experiments are carried out in order to analyze the quality of the synthetic signatures and the feasibility of synthetically increasing the enrollment set samples. The goal of the experiments is threefold, namely: (i) measure the similarity between real and synthetic images (ii) assess whether using synthetic signatures affects the recognition performance (iii) analyze the feasibility of using real and synthetic signatures on the enrollment set.

We compare our results with the state of the art, specifically the the approach proposed by Diaz [9]. Our proposed method is compared with the "Image enhanced" synthetic signatures made available as part of the BiosecurID [42] dataset. The reported EER is achieved for both approaches on the same experimental conditions.

6.1 Experiment 1

In order to evaluate the performance of the synthetic signature signatures described in Sect. II and the state of the art, two different protocols are followed:

- mono-session: signatures from the first session on the enrollment set
- multi-session: one signature per session.

Table 2 shows the EER achieved by the real and the synthetic signatures databases. As it may be observed, under the random forgeries scenario, the EERs achieved by the real and both types of synthetic signatures are very close. On the other hand we observe that under the skilled

Table 2 – EER for real, synthetic samples from Diaz [9] and our proposed method synthetic off-line signatures, for all the approaches considered under the two possible scenarios (i.e., random and skilled forgeries)

Mode	Skilled Forgeries		
	Real	**Diaz**	**Proposed method**
mono-session	20.28%	23.19%	18.38%
multi-session	17.59%	22.27%	16.48%
	Random Forgeries		
	Real	**Diaz**	**Proposed method**
mono-session	9.07%	10.65%	9.99%
multi-session	5.60%	10.00%	6.48%

forgeries our proposed method synthetic signatures EERs yields better performance than both the real dataset and the synthetic signatures generated by Diaz.

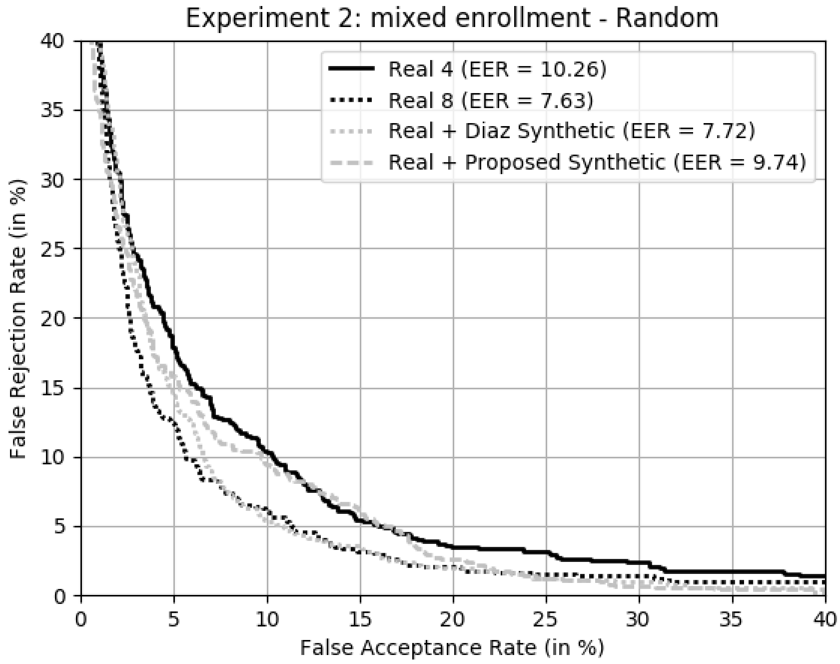
In Figure 15 (left - mono-session, right - multi-session) we may observe that the behaviour of the system with real (gray dotted) and our proposed method synthetic signatures is quite similar, regardless of the training protocol or the scenario considered. Nevertheless, our proposed method synthetic samples show a bigger discriminative power for skilled forgeries.

Table 3 – EER for real, synthetic samples from Diaz [9] and our proposed method synthetic off-line signatures for the Experiment 2 under the two possible scenarios, i.e., random (RF) and skilled forgeries (SF)

Genuine Training	SF	RF
4 real samples	21.55%	10.26%
4 real + 4 real samples	19.72%	7.63%
4 real + 4 synthetic from Diaz	24.19%	7.72%
4 real + 4 synthetic from the Proposed Method	19.17%	9.74%

6.2 Experiment 2

In the last experiment, the feasibility of synthetically increasing the enrollment set is analyzed. As described in Sect. III, three different enrollment sets are considered. As it may be observed in Figure **??**, the DET curves for the mixed enrollment (real + synthetic, grey dashed line), show a better performance compared to the case with only four real enrolled samples (black line), regardless of the operating point or the scenario considered. More specifically, the EER decreases from 10.26% to 9.74% on the random forgeries scenario and from 21.55% to 19.17% for skilled forgeries, respectively. The addition of synthetic samples for training thus leads to better recognition results.



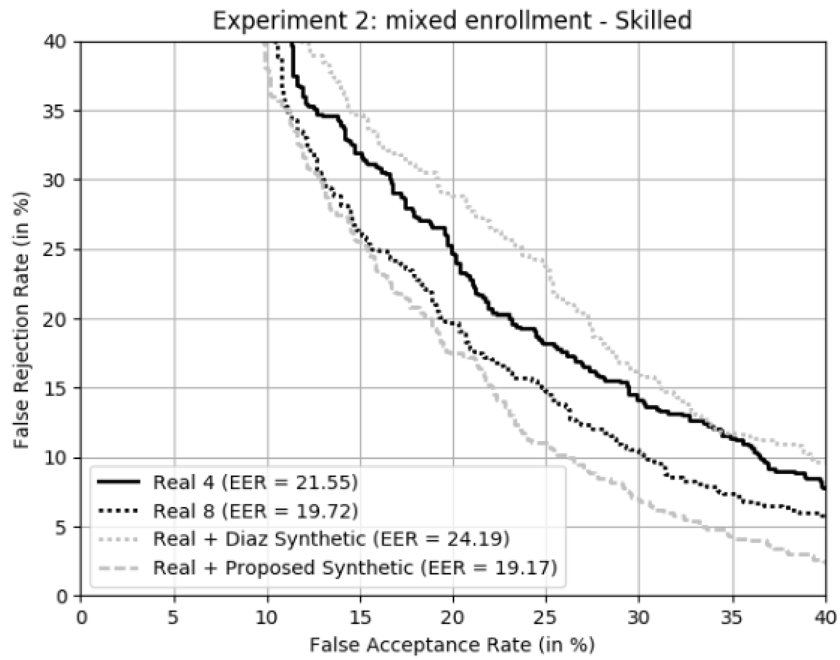


Figure 16 – DET curves for real off-line signatures and synthetic signatures (from Diaz and our proposed method), for the second experiment, for the two scenarios considered (random and skilled impostors)

It should also be noted that the behavior of the mixed enrollment is similar to the scenario with eight real enrolled samples (i.e., using eight real samples instead of four real and four synthetic, black line) for skilled forgeries, and even yields a small improvement on the skilled forgery recognition rates.

We may thus conclude that, our proposed system can be a good alternative to synthetically increase the off-line signatures samples when complementary on-line samples are available in order to increase the accuracy of the off-line verification system.

CHAPTER 7

Conclusion and Future Works

A novel method to synthesize off-line signatures from dynamic information has been proposed. We describe our Neural Network approach that learns how to transform on-line manuscripts into static samples taking advantage of the data present in the IRONOFF dataset.

We observe that our proposed synthetic images offer better performance when compared to the state of the art and similar performance to real signatures. We show that the synthetic signatures present high discriminative power when used to increase the enrollment set under the skilled forgeries scenario, one of the biggest challenges in handwriting recognition.

We intend to explore in future works the combination of real on-line and synthetically generated off-line signatures from our method, when only the on-line information is available, towards improved recognition results.

Bibliography

[1] JAIN, A. K.; ROSS, A.; PRABHAKAR, S. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, IEEE, v. 14, n. 1, p. 4–20, 2004.

[2] IMPEDOVO, D.; PIRLO, G. Automatic signature verification: the state of the art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, IEEE, v. 38, n. 5, p. 609–635, 2008.

[3] FIERREZ, J.; ORTEGA-GARCIA, J. On-line signature verification. In: *Handbook of biometrics*. [S.l.]: Springer, 2008. p. 189–209.

[4] VIARD-GAUDIN, C.; LALLICAN, P. M.; KNERR, S.; BINTER, P. The ireste on/off (IRONOFF) dual handwriting database. In: IEEE. *Document Analysis and Recognition, 1999. ICDAR'99. Proceedings of the Fifth International Conference on*. [S.l.], 1999. p. 455–458.

[5] HERRERO, J. G.; FIERREZ, J.; DÍAZ, M. M.; ORTEGA-GARCIA, J. Synthetic generation of handwritten signatures based on spectral analysis. In: SOCIETY OF PHOTO-OPTICAL INSTRUMENTATION ENGINEERS. *Proceedings of SPIE-The International Society for Optical Engineering*. [S.l.], 2009.

[6] GALBALLY, J.; FIERREZ, J.; ORTEGA-GARCIA, J.; PLAMONDON, R. Synthetic on-line signature generation. part ii: Experimental validation. *Pattern Recognition*, Elsevier, v. 45, n. 7, p. 2622–2632, 2012.

[7] FERRER, M. A.; DIAZ-CABRERA, M.; MORALES, A. Synthetic off-line signature image generation. In: IEEE. *Biometrics (ICB), 2013 International Conference on*. [S.l.], 2013. p. 1–7.

[8] FERRER, M. A.; DIAZ-CABRERA, M.; MORALES, A.; GALBALLY, J.; GOMEZ-BARRERO, M. Realistic synthetic off-line signature generation based on synthetic on-line data. In: IEEE. *Security Technology (ICCST), 2013 47th International Carnahan Conference on*. [S.l.], 2013. p. 1–6.

[9] DIAZ-CABRERA, M.; GOMEZ-BARRERO, M.; MORALES, A.; FERRER, M. A.; GALBALLY, J. Generation of enhanced synthetic off-line signatures based on real on-line data. In: IEEE. *Frontiers in Handwriting Recognition (ICFHR), 2014 14th International Conference on*. [S.l.], 2014. p. 482–487.

[10] JAIN, A.; HONG, L.; PANKANTI, S. Biometric identification. *Communications of the ACM*, ACM, v. 43, n. 2, p. 90–98, 2000.

[11] ROSS, A.; NANDAKUMAR, K.; JAIN, A. K. Introduction to multibiometrics. In: *Handbook of Biometrics*. [S.l.]: Springer, 2008. p. 271–292.

[12] JAIN, A. K.; NANDAKUMAR, K.; ROSS, A. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, Elsevier, v. 79, p. 80–105, 2016.

[13] UPPALAPATI, D. Integration of Offline and Online Signature Verification systems. *Department of Computer Science and Engineering, IIT, Kanpur*, 2007.

[14] GUPTA, G.; MCCABE, A. A review of dynamic handwritten signature verification. *James Cook Univ., Australia*, 1997.

[15] NEL, E.-M.; PREEZ, J. A. D.; HERBST, B. M. Estimating the pen trajectories of static signatures using Hidden Markov models. *IEEE transactions on pattern analysis and machine intelligence*, IEEE, v. 27, n. 11, p. 1733–1746, 2005.

[16] WACOM. *STU-500*. 2016. Disponível em: <http://www.wacom.com/en-us/enterprise/business-solutions/hardware/signature-pads/stu-500>.

[17] HEUVEL, C. van den; FRANKE, K.; VUURPIJL, L. The ICDAR 2009 signature verification competition. *ICDAR2009 proceedings*, 2009.

[18] PIRLO, G.; IMPEDOVO, D.; FAIRHURST, M. *Advances in Digital Handwritten Signature Processing: A Human Artefact for E-society*. [S.l.]: World Scientific, 2014.

[19] PLAMONDON, R.; LORETTE, G. Automatic signature verification and writer identification—the state of the art. *Pattern recognition*, Elsevier, v. 22, n. 2, p. 107–131, 1989.

[20] HAFEMANN, L. G.; SABOURIN, R.; OLIVEIRA, L. S. Offline handwritten signature verification-literature review. *arXiv preprint arXiv:1507.07909*, 2015.

[21] ORTEGA-GARCIA, J.; FIERREZ-AGUILAR, J.; SIMON, D.; GONZALEZ, J.; FAUNDEZ-ZANUY, M.; ESPINOSA, V.; SATUE, A.; HERNAEZ, I.; IGARZA, J.-J.; VIVARACHO, C. et al. MCYT baseline corpus: a bimodal biometric database. *IEE Proceedings-Vision, Image and Signal Processing*, IET, v. 150, n. 6, p. 395–401, 2003.

[22] FAIRHURST, M. Signature verification revisited: promoting practical exploitation of biometric technology. *Electronics & communication engineering journal*, IET, v. 9, n. 6, p. 273–280, 1997.

[23] GUEST, R. M.; HURTADO, O. M.; HENNIGER, O. Assessment of methods for image recreation from signature time-series data. *IET biometrics*, IET, v. 3, n. 3, p. 159–166, 2013.

[24] RABASSE, C.; GUEST, R. M.; FAIRHURST, M. C. A new method for the synthesis of signature data with natural variability. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, IEEE, v. 38, n. 3, p. 691–699, 2008.

[25] DIAZ-CABRERA, M.; FERRER, M. A.; MORALES, A. Cognitive inspired model to generate duplicated static signature images. In: IEEE. *Frontiers in Handwriting Recognition (ICFHR), 2014 14th International Conference on*. [S.l.], 2014. p. 61–66.

[26] HAYKIN, S. S.; HAYKIN, S. S.; HAYKIN, S. S.; HAYKIN, S. S. *Neural networks and learning machines*. [S.l.]: Pearson Upper Saddle River, NJ, USA:, 2009. v. 3.

[27] ROSENBLATT, F. The perceptron: A probabilistic model for information storage and organization in the brain. *Psychological review*, American Psychological Association, v. 65, n. 6, p. 386, 1958.

[28] PAPERT, M. M. S.; MINSKY, M. Perceptrons: an introduction to computational geometry. *Expanded Edition*, 1969.

[29] BISHOP, C. M. *Pattern recognition and machine learning*. [S.l.]: springer, 2006.

[30] HORNIK, K.; STINCHCOMBE, M.; WHITE, H. Multilayer feedforward networks are universal approximators. *Neural networks*, Elsevier, v. 2, n. 5, p. 359–366, 1989.

[31] LONG, J.; SHELHAMER, E.; DARRELL, T. Fully convolutional networks for semantic segmentation. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. [S.l.: s.n.], 2015. p. 3431–3440.

[32] LECUN, Y.; BOTTOU, L.; BENGIO, Y.; HAFFNER, P. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, IEEE, v. 86, n. 11, p. 2278–2324, 1998.

[33] DUMOULIN, V.; VISIN, F. A guide to convolution arithmetic for deep learning. *arXiv preprint arXiv:1603.07285*, 2016.

[34] POURSHAHABI, M. R.; SIGARI, M. H.; POURREZA, H. R. Offline handwritten signature identification and verification using contourlet transform. In: IEEE. *Soft Computing and Pattern Recognition, 2009. SOCPAR'09. International Conference of*. [S.l.], 2009. p. 670–673.

[35] JENSEN, O.; IDIART, M.; LISMAN, J. E. Physiologically realistic formation of autoassociative memory in networks with theta/gamma oscillations: role of fast nmda channels. *Learning & Memory*, Cold Spring Harbor Lab, v. 3, n. 2-3, p. 243–256, 1996.

[36] WEINBERGER, N. M. Specific long-term memory traces in primary auditory cortex. *Nature reviews. Neuroscience*, Nature Publishing Group, v. 5, n. 4, p. 279–290, 2004.

[37] KRAMER, M. A. Nonlinear principal component analysis using autoassociative neural networks. *AIChE journal*, Wiley Online Library, v. 37, n. 2, p. 233–243, 1991.

[38] HINTON, G. E.; SALAKHUTDINOV, R. R. Reducing the dimensionality of data with neural networks. *science*, American Association for the Advancement of Science, v. 313, n. 5786, p. 504–507, 2006.

[39] MASCI, J.; MEIER, U.; CIREŞAN, D.; SCHMIDHUBER, J. Stacked convolutional auto-encoders for hierarchical feature extraction. *Artificial Neural Networks and Machine Learning–ICANN 2011*, Springer, p. 52–59, 2011.

[40] GLOROT, X.; BENGIO, Y. Understanding the difficulty of training deep feedforward neural networks. In: *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*. [S.l.: s.n.], 2010. p. 249–256.

[41] HAFEMANN, L. G.; SABOURIN, R.; OLIVEIRA, L. S. Learning features for offline handwritten signature verification using deep convolutional neural networks. *Pattern Recognition*, Elsevier, v. 70, p. 163–176, 2017.

[42] FIERREZ, J.; GALBALLY, J.; ORTEGA-GARCIA, J.; FREIRE, M. R.; ALONSO-FERNANDEZ, F.; RAMOS, D.; TOLEDANO, D. T.; GONZALEZ-RODRIGUEZ, J.; SIGUENZA, J. A.; GARRIDO-SALAS, J. et al. BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications*, Springer, v. 13, n. 2, p. 235–246, 2010.