ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 8 N. 4 (2019), 19-32
eISSN: 2255-2863
DOI: http://dx.doi.org/10.14201/ADCAIJ2019841932

Deep Learning in Biometrics: A Survey

Alberto Botana López

University of Salamanca
alberto.botana@usal.es

KEYWORD

Deep learning; biometrics; fingerprint; ocular recognition; convolutional neural networks; electrocardiogram

ABSTRACT

Deep learning has been established in the last few years as the gold standard for data processing, achieving peak performance in image, text and audio understanding. At the same time, digital security is of utmost importance in this day and age, where everyone could get into our personal devices like cellphones or laptops, where we store our most valuable information. One of the possible ways to prevent this is via advanced and personalized security: biometrics. In this survey, it is considered how the scientific advances in the field of deep learning are applied to biometrics in order to enhance the protection of our data. Firstly, a study will be conducted on tackling ocular identification of twins using deep learning. Then, an improved method for avoiding fingerprint spoofing will be presented, thus solving this method's biggest issue. Finally, a brand new method for biometric identification is proposed based on the usage of the user's electrocardiogram. On every one of these methods, the results manage to top the standard alternative performances.

1. Introduction and motivation

The mobile phone and wearable device industry has been evolving wildly in the last years and, with it, evolved the use of apps and its importance on a daily basis, such as mobile banking or payment apps, health insurance or even password managing apps. All these services handle very sensitive and thus need proportional security. In this day and age, just pattern or PIN code locks for these services are simply not enough, since, as the security methods evolve, so do the penetration methods through which these barriers can be breached (Abdullayeva *et al.*, 2008).

Arguably, the most efficient methods for securing personal assets like these are the biometric ones, such as fingerprint reading, ocular scanning, or face recognition (Darve and Theng, 2015), but the efficiency of these methods alone can only get so far. In this state-of-the-art survey, a study is conducted on how recent technological advances like deep learning can help improve the efficiency of these methods and even propose new ones.

The reason of why these methods are being developed so extensively just now is because of the latest technology and scientific advances which allowed this technological field to bloom, such as:

- Increased availability for machine learning (ML) and deep neural network (DNN) training datasets.
- Increased computational power available, specially due to the bloom of the Graphical Processing Units (GPUs) in the late years, which are optimized for high performance parallel processing, significantly reducing the computational time needed for the DNNs to operate.

- Years of advances in processing algorithms for DNNs, in depth as in output size, which allowed them to increase significantly its performance.

More specifically, in this survey we will tackle in section 2 twin identification, one of the biggest problems with ocular recognition, applying deep learning (Gautam et al., 2019). In section 3, an improved method to prevent fingerprint spoofing is discussed, potentially solving this biometric system's biggest drawback (Arora and Bhatia, 2019). In section 4, a new method for biometric identification is proposed, based on the heartbeat pulse of the user, utilizing the electrocardiogram (ECG) to recognize different users (Kim and Pan, 2019). Finally, some conclusions will be brought up as well as a final review of what was done in this survey.

1.1. But what ***is*** deep learning?

Deep learning (DL) is a paradigm of machine learning algorithm which main feature is the ability of using multiple layers to extract higher features the deeper the network is.

The main difference with the rest of the regular neural networks lies in its size, since, whereas many regular neural networks are composed of the input layer, a few hidden layers and the output layer; deep neural networks have the same input and output layer, but are comprised of many more hidden layers beneath these two (Schmidhuber, 2015). Its main use, and the one applied in this survey is that of Convolutional Neural Networks (CNN), which are primarily used to extract information from images by sweeping a series of convolutional filter to the input image and then are ran through a pooling layer, which reduces the size of the image to be processed by the next filter (Denker *et al*., 1989).

2. Twin Ocular Identification

Biometric distinction on twins has been of increasing interest for some time now due to many reasons, including reliability for legal systems as well as the proven increasing rate of twin births. Besides, distinguishing twins has been proved to be one of the hardest issues in the field, and it has become interesting as a validation biometric factor (Bowyer and Flynn, 2016). In this section of the survey, an attempt to identify twins using ocular biometric measures is studied. Since this area is relatively new, there is a need to study every aspect of this trait including stability, uniqueness, and reliability. Contrary to popular belief, ocular biometrics are not bound to a specific region; instead of that, it comprises various sub-parts such as iris, cornea, pupil, retina, lens, periocular region and conjunctival vasculature, all of them useful to extract discriminating information. In this paper, special emphasis will be set on the iris and its surrounding region. In order to do that, a Siamese Neural Network (SNN) will be used. SNNs consist of twin neural networks with shared weights which learns feature representation via a pair of images taken from the positive and negative classes and then minimizing the Euclidean distance for positive and maximizing it for negative classes (Bromley *et al.*, 1994).

The main contributions of this section are as follows:

- Two frameworks, CNN-Siamese and MCNN- Siamese are designed so that significant results on twin identification is achieved.
- Four existing different models (VGG-Siamese, ResNet-Siamese, NASNet-Large-Siamese & sNN-Siamese) are used to determine the proposed framework validation, being the first three pre-trained networks (He *et al.*, 2015) (Simonyan and Zisserman, 2014) (Zoph *et al.*, 2017).
- Proper generalization of CNN and MCNN will be proved by experimenting on different ocular datasets. By doing so the gender classification problem is addressed. This method will perform at state-of-the-art levels.

2.1. Proposed model

When using SNNs (Koch *et al.*, 2015), a new kind of loss function must be used in order to join both of the networks and compute the similarity between the feature output vectors obtained from each of the networks. This function, named *Contrastive Loss Function* (CLF) is described by:

$$CLF(M) = \sum_{i=1}^{N} f\left(M, (x, T_1, T_2)^i\right) \qquad (1)$$

Where T_1 and T_2 are a pair of images, and x is a binary value indicating whether said pair of images are a twin pair or not, and M is the shared matrix of parameters from which to learn. Following these parameters, the function f is defined by $f\ (M, (x, T_1, T_2)i = (1 - x)\ \cdot max(p - D_M\ (T_1, T_2)^i, 0) + x\ \cdot D_M\ (T_1, T_2)$, Where p is a positive number representing a safety margin, and $D_M\ (T_1, T_2)$ is the distance between the pair of images.

Both of the branches on the SNN can be used with a grafting function what transforms the input image into a apce and the CLF allows said space to have a property that will bring twin images closer than the non-twin ones. Both of these branches will be connected through a layer that calculates the Euclidean Distance between the outcomes of these, and, filtering it through a threshold, a certain input can be classified as twin or non-twin.

In this study, back-propagation (BP), will be used to train all the models. Deep learning model training using BP makes them computationally tractable where the gradient computation is more efficient. However, where BP presents this advantage, it also suffers from the problems of local minima and slow convergence speed.

2.1.1. *CNN-Siamese Framework*

The used architecture on the CNN, as shown in figure 1 is as follows: Eight weighted layers, being the first five convolutional (Conv) followed by a pooling layer, and the other three being fully connected (FC) layers. On these last layers, ReLU is being used as the activation function due to its computational simplicity and its advantages when calculating gradient descent backpropagation. The output of the last FC layer of each branch is fed to a distance computation module in order to estimate the similarity between the two input images. Then a threshold metric is used on the distance to classify wether the input pair belongs to twins or not.

The outputs of the last FC layers of each of the subnetwork is fed to a distance metric computation module in order to estimate the similarity between two feature vectors. Then, we have used a threshold value on the distance metric D output by the CNN-Siamese to determine whether a pair of ocular images (T1, T2) belongs to the positive or negative class.

2.2.2. *MCNN-Siamese Framework*

The multi-scale model is more reminiscent of the human vision model. The kernel scale denotes in the neighbourhood what can be a crucial parameter for feature extraction. The disadvantage of using small and large kernel scales are poor localization characteristics as well as poor noise immunity. Besides, what is relevant for a certain neighbourhood might not be so for another. This implies that trying with different kernel sizes might be extremely useful. Considering these reasons, a multi-scale filter is implemented for extracting features. This framework consists on four different filters (1x1, 3x3, 5x5 & 7x7) each with a MaxPool layer. These multi-scale filters are averaged instead of contatenated for the sake of keeping computatinal costs at bay, since the difference between one and the other did not suppose a significant difference in accuracy.

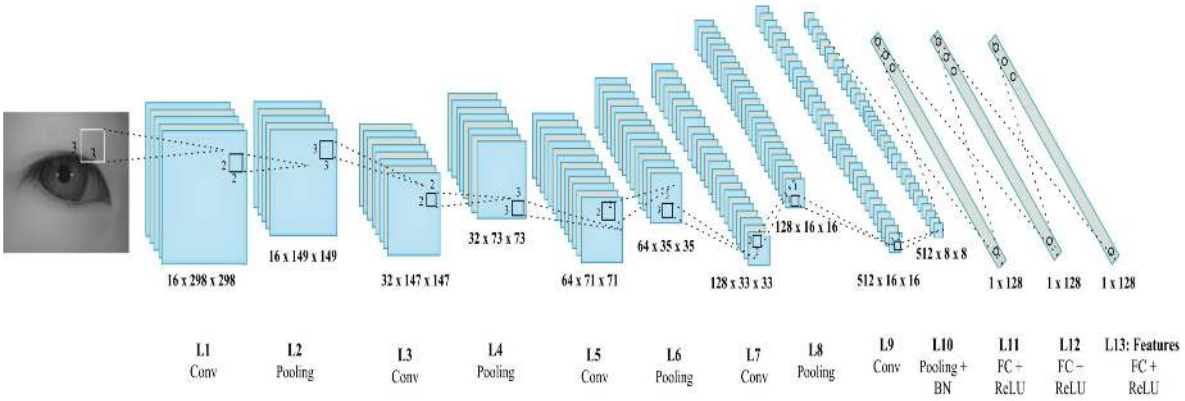

Figure 1: Structure of each of the branches on the CNN-Siamese framework. Reprinted from (Gautam et al., 2019).

The architecture of the MCNN, shown in figure 2 is as follows: The multi-scale convolution layer outputs are applied followed by a single convolution layer and downsampling. The multi-scale output averages of specific features from each scale, extracted using each of the individual filters.

At the output of the MCNN, padding has been applied so that it has the same shape as the input. It has been found that reducing the size of the filter enhances the generalizability instead of increasing the number of filters. Therefore, with the purpose of obtaining a more generic feature representation, features are extracted from an early layer. For further improving the performance, the pre-trained model must be fine- tuned. In the end, the Sigmoid function is used for class prediction. It takes any real number as input and returns a value following the equation:

$$y = \frac{1}{1 + e^{-x}} \qquad (2)$$

Which will be ranging from 0 to 1. In this application, the meaning of this output can be interpreted as a probability of the image being a twin pair.

2.2. Results

It has been found that gradually increasing the size of the kernel, along with monitoring the error rate in a feasible computational time allowed finding the ideal kernel sizes. Figure 3 represents the accuracy of each configuration varying kernel sizes along with combination of kernels.

The necessary codebase is implemented using Keras, and the outcoming results are checked by 3-fold cross-validation (CV), in which the whole dataset is randomly split in three separate categories, and then taken two of those categories and train the network using them, utilizing the remaining as a test set. Additional performance validation metrics used are CCR, training loss and the AUROC curve.

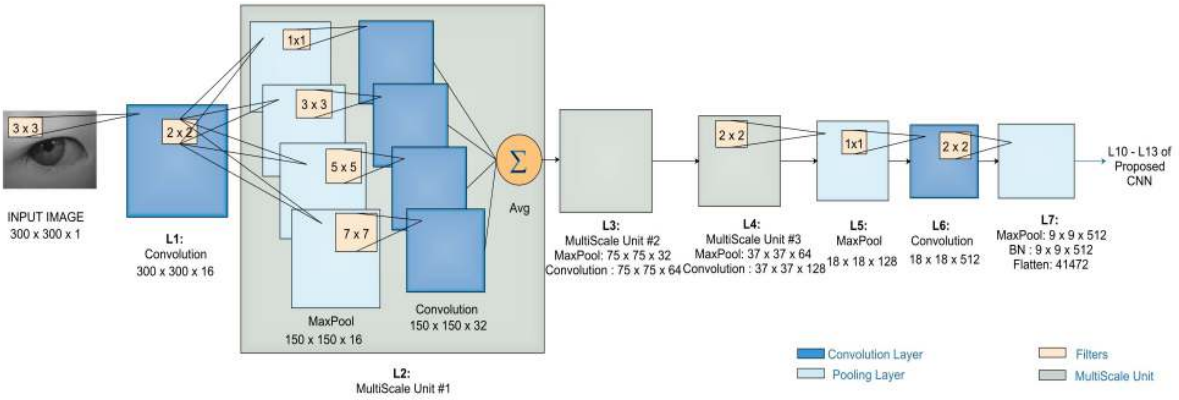

Figure 2: Structure of the MCNN-Siamese framework. Reprinted from (Gautam et al., 2019).

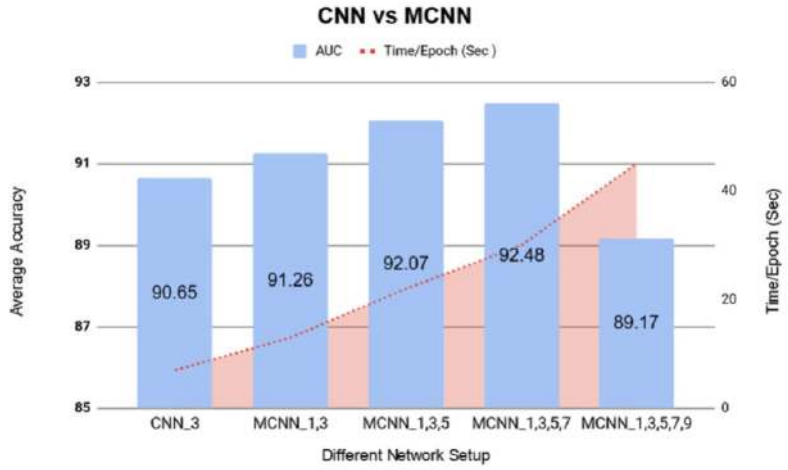

Figure 3: Accuracy of CNN vs MCNN frameworks. Reprinted from (Gautam et al., 2019).

The database used in the study has been the publicly available CASIA-Iris-Twins dataset for experimentation, containing pictures of 100 pair of twins. In order to obtain rotational invariance, random pairs of this dataset have been preprocessed by rotating them at different angles, and afterwards, for the sake of keeping computational times low enough, resized from their original 640x480 resolution to 300x300, being this size the minimum working size, experiencing significant accuracy losses if working below that resolution. Dropout tests were concurred with 10, 20, 50 and 90% dropout, observing that deterioration ensued the higher the dropout. Therefore, it was kept at its lowest setting, 10%.

Results have shown that NASNet-Large-Siamese framework yields the best results, scoring an accuracy of 96.40%. However, average accuracy results give 92.93% with a standard deviation being 2.16%, thus it can be said that the standard deviation shows that the accuracies from all the studies frameworks are set around the mean.

In order to determine the best model when it comes to class predicting, AUROC (Area Under the Receiver Operating Characteristics) must be used, where higher scoring models are preferred to those with lower ones. As shown in figure 4, the results show that in Fold 1, NASNet-Large-Siamese is the best performer with an AUROC of 0.95, whereas in Fold 2, NASNet-Large- Siamese, VGG-Siamese and ResNet-Siamese perform at equal AUROCs of 1.0. Finally, in Fold 3, every framework performs with a similar score, obtaining all AUROCs of 1.0.

ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 8 N. 4 (2019), 19-32
eISSN: 2255-2863 - http://adcaij.usal.es
Ediciones Universidad de Salamanca - CC BY NC DC

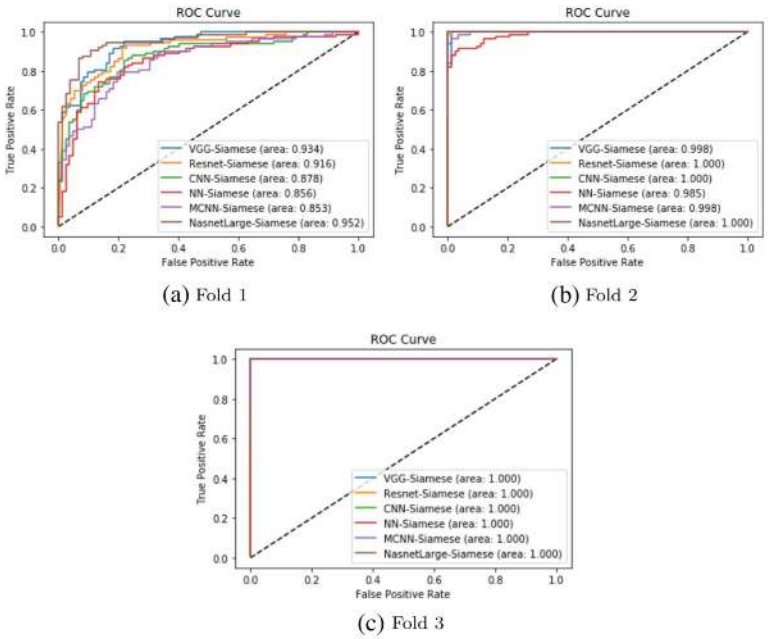

Figure 4: AUROC Performance on every framework for each CV fold. Reprinted from (Gautam et al., 2019).

3. Fingerprint spoofing

There's no denying that, in the last few years, the need for a strong authentication system is personal services like financial, healthcare or insurance is of utmost need (Hamza *et al*., 2019). Biometrics in mobile payments has come to be the next generation way of making financial transactions, and the use of fingerprint sensors in smartphones has been a necessary change in order to secure these precious goods. Flagship smartphone brands like Samsung or Apple were the first to introduce this kind of sensors for user authentication (Roy *et al.*, 2017). In addition to that, a fingerprint-secured credit card has been developed by MasterCard in collaboration with Zwipe. Fingerprint authentication has proven to be relatively foolproof compared with its main competitors: PIN authentication and password authentication. However, fingerprint authentication is not perfect and thus is, as is every other method, prone to faking of spoofing attacks. To counter that, in this section, a method is proposed to detect fake fingerprints by performing histogram equalization on input images. These inputs shall be trained using a CNN and then a prediction will decide whether said input image is a faked one or not. Original authors focused on impersonation attacks by creating a physical forged fingerprint. In order to do so, the most common methods are latent fingerprinting, done by analyzing a fingerprint left on a surface, and then extracted via powder or scotch tape; or direct molding, which is obtained by pressing target finger against a mold and then filling it with a skin-line gel like gelatin or silicone.

3.1. Proposed model

The proposed framework on this section features the following advantages compared to its competitors:

- Lower training parameters needed, lowering overfitting and computational cost. Additional 10-fold cross-validation also helps lowering overfitting and making the model robust.
- Improved recognition rate due to the use of histogram equalization.
- Architecture suitable to use in real-life fingerprint sensors, with superior accuracy than the actual state-of-the-art sensors.

Histogram equalization is a process of studying fingerprint images in order to increase contrast on said images. For any given input, the gradient of cumulative density function (cdf) at any point will be equal to the probability density, described by function 3 at that same point. With this, the steeper the cdf plot, the higher the histogram will be at that point. In the probability density equation, *nk* represents the number of pixels, *rk* the pixel intensity and *k* represents the gray level. The histogram plot of cdf vs histogram on an input fingerprint can be seen on figure 5, and the before and after histogram equalization images of a real and a fake fingerprint can be seen on figures 6 to 9.

$$p_r(r_k) = n_k/n, 0 < p_r(r_k) < 1, 0 < k < 255 \quad (3)$$

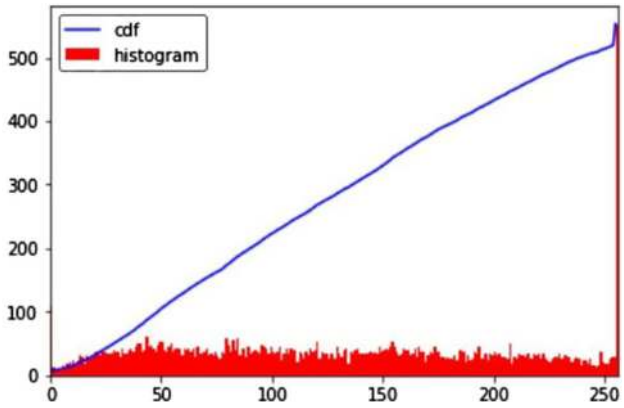

Figure 5: cdf vs histogram plot on an input fingerprint.

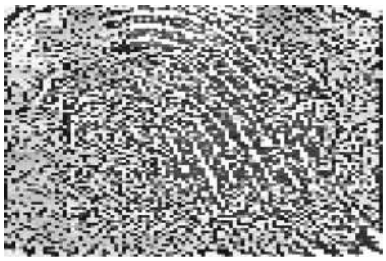

Figure 6: Fake fingerprint before any treatment occurs.

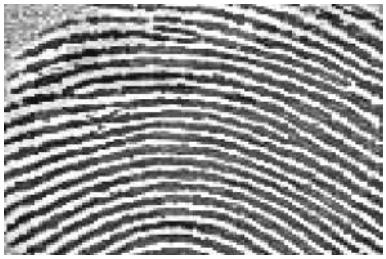

Figure 7: Real fingerprint before any treatment occurs.

Figure 8: Fake fingerprint after contrast. enhancement

Figure 9: Real fingerprint after contrast enhancement.

3.2. Results

The resulting CNN architecture has been trained using the Tensorflow implementation on Python, and ran on Google Cloud, which benefits of great CPU and GPU power, for 100 epochs on each dataset. Additionaly, OpenCV library was used for some required preprocessing. The outcoming results of the model were tested against popular fingerprint benchmarks, and its results, which obtained remarkably high accuracy, were validated using 10-fold cross-validation.

Different tests are conducted in order to calculate the threshold of a given dataset, which will be used to identify a certain fingerprint between genuine and forged. This threshold estimation will assure that this system would be able to withstand spoofing attacks. The main metrics used for these are:

- False Acceptance Rate (FAR), which is calculated by $FAR = \frac{FP}{T}$, with FP meaning the amount of false positives, or the amount of times the system classifies as positive an entry that should have been negative; and T begin the total amount of entries.
- False Rejection Rate (FRR), calculated by $FRR = \frac{FN}{T}$, with FN being the amount of false negatives, which means the amount of times the system classifies negatively an allegedly positive attempt.
- Equal Error Rate (EER), or the value where FAR and FRR are equal. The lower this metric gets, the more accurate the system is.
- Average Classification Error (ACE), calcualted by $ACE = \frac{FAR+FRR}{2}$. As with EER, the lower this metric is, the more accurate the system gets.

The optimal threshold will have the smallest value of FAR and FRR manageable, thus having the lowest EER and ACE possible. Obtained results after testing the proposed framework on different datasets can be found on table 1. As it shows, this framework obtains an accuracy higher than 99% on all of the benchmarks. In table 2 a comparison is shown between different state-of-the-art method (CNN-VGG, AlexNet and Inception V3) performances against the proposed framework. On it, different instances of Italdata 2013 can be found. These were all results from different researchers, being (Jang et al., 2017) (Marasco et al., 2011) (Ghiani et al., 2017) respectively, It is shown that the proposed framework surpasses all of the state- of-the-art methods and thus can be qualified as robust, allowing it to be used to secure fingerprint-based devices.

4. ECG user recognition

In the fast-growing heavily connected society of today, the wearable technology industry has evolved with it. One of the main advantages of these devices are that they are continuously collecting a wide range of information on the users as well as the environment surrounding them, which can be specially useful when applying it to user recognition methods. So far, the main user recognition methods are those of face, fingerprint and iris, which are relatively safe means of user recognition, but they all require user cooperation, thus requiring a voluntary user action. They also present the disadvantage of being susceptible to faking and spoofing, which can be a huge risk when valuable information such as financial services, healthcare or position-based services are at stake.

To solve these, current studies are tackling alternative methods such as electrocardiograms (ECG), electroencephalograms (EEG) and electromyograms (EMG). These methods present several major advantages compared to those used until now: i) These signals are generated from within the body instead of relying on anatomical methods, which renders spoofing much more difficult. ii) These kind of signals can be obtained from any living person, which could not be said with the previous methods, since there are rare occasions where, for example, a human being can be born with no fingerprints (Burger *et al.*, 2011), thus rendering this method useless. Additionally, this method renders spoofing attempts which involve any dead body. iii) The signals can also provide additional information, such as clinical state and psychological state. And iv) they make recognizing users multiple times easier, since these signals do not tend to change over time (Ogiela and Ogiela, 2016).

In this section, ECG signals will be studied as a next-gen user recognition method, since they are unique to each individual due to the fact that they may present variations based on many factors, such as heart position,

age, gender, and size. Some existing user recognition techniques using ECG utilize machine learning methods such as SVM (Mehta and Lingayat, 2008), k-NN (Qibin Zhao and Liqing Zhang, 2005) and Random Forest Regressor (Khazaee and Zadeh, 2014), but since the ECG has so many different features to be learned, most of these methods incur in overfitting, thus decreasing performance levels. In this section, an ensemble network is proposed to solve this problem by tackling the recognition on separated layers, each one working with different parameters. 1-dimensional ECG signals present simple patterns, so the number of separate layers was kept on 2-3.

4.1. Proposed model

To understand the proposed model, the concepts of fiducial and non-fiducial point-based classification methods must be explained. In a fiducial classification, the ECG signal features are recognized and get classified based on periods. In order to obtain this, some preprocessing on the signal must be issued such as noise removal for enhanced feature detection. This can be seen in figure 10.

In a non-fiducial classification method performs its task by sliding a fixed size window all along the ECG signal, as shown in figure 11. Both figures taken from (Kim and Pan, 2019).

Table 1: Obtained results after applying proposed fingerprint anti-spoofing model on different existing datasets

Dataset	*Accuracy (in %)*	*FAR*	*FRR*	*ACE (in %)*	*Threshold*
CrossMatch 2013	99,33	0,019	0,024	1,82	0,55
Italdata 2013	99,56	0,004	0,008	0,6	0,58
Swipe 2013	99,22	0,029	0,033	3,3	0,55
Biometrika 2013	99,31	0,015	0,018	1,6	0,53
Greenbit 2015	99,13	0,03	0,032	3,18	0,52
CrossMatch 2015	99,25	0,04	0,011	2,5	0,6
DigitalPersona 2015	99,8	0,009	0,001	0,54	0,59
ATVSFF_p DB	99,54	0	0,006	0,3	0,53
FVC2006	99,78	0,024	0	1,2	0,53
Spoofed fingervein	99,25	0,012	0,029	2,05	0,54

Table 2: Comparison between state-of-the-art frameworks versus the proposed framework

Dataset	*State-of-the-art (ACE in %)*	*CNN-VGG (ACE in %)*	*CNN-AlexNet (ACE in %)*	*Inception V3 (ACE in %)*	*Proposed Framework (ACE in %)*
Swipe2013	2,8	4,3	3,7	–	3,30
CrossMatch2013	7,9	4,7	3,4	–	1,82
Italdata2013	0,8	0,5	0,4	–	0,60
LivDet2009,2011,2013	4,7	3,9	2,7	–	1,83
FVC2002	–	–	1,49	–	1,2
Biometrika2013	–	–	–	3,1	1,6
Italdata2013	–	–	–	0,8	0,6
Italdata2013	–	0,4	–	–	0,60
GreenBit2015	–	4,6	–	–	3,18
DigitalPersona2015	–	6,3	–	–	0,54
CrossMatch2015	–	1,9	–	–	2,50

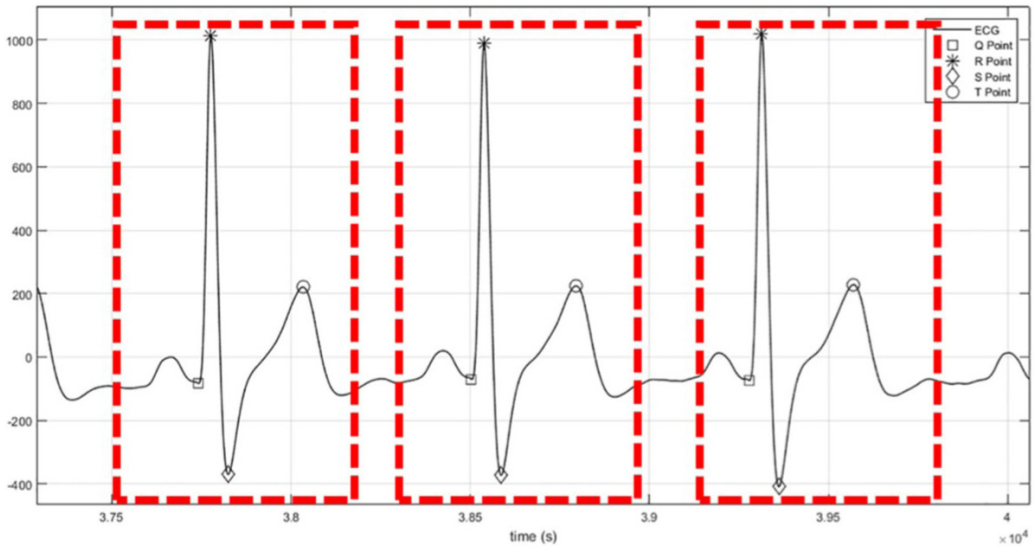

Figure 10: Fiducial point-based classification. Adapted from (Kim and Pan, 2019).

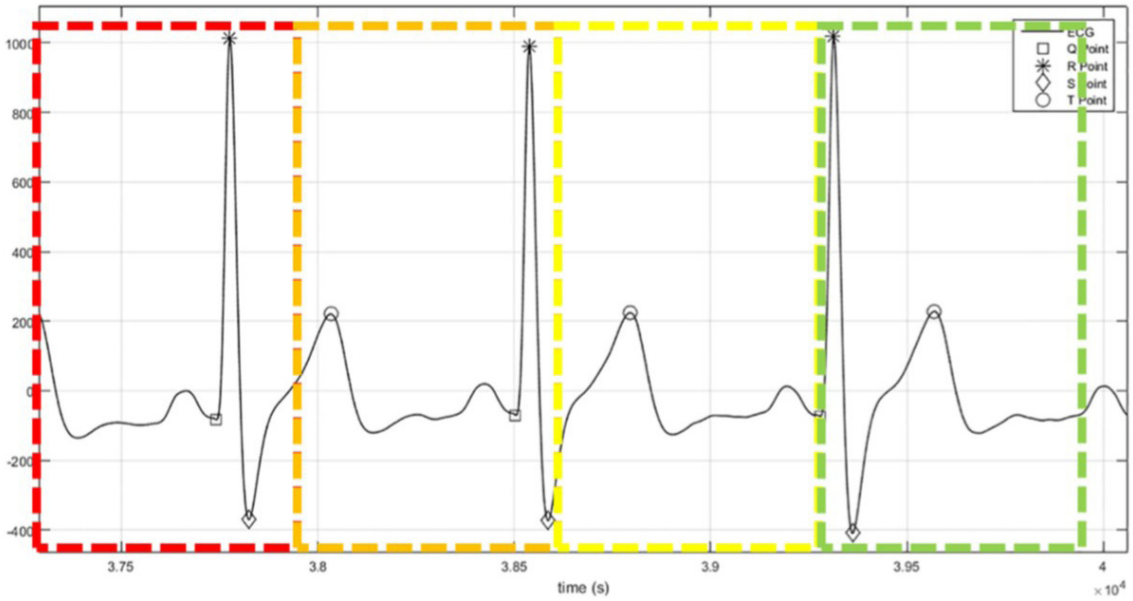

Figure 11: Non-fiducial point-based classification. Adapted from (Kim and Pan, 2019).

CNNs are mainly used for two-dimensional data like images, but recent studies are conducted on the analysis on 1-D time series using this kind of networks. In this case, they are used to extract local subsequence features from sequences, as well as distinguishing local patterns within the convolution window.

The original signal is processed and a learning method extracts features from the multi-layer perceptron on which the CNN is based, and uses them in recognition tasks. This way, the feature extraction as well as the recognition methods are all combined into a single model, optimized to improve its performance. This sums up the equation 4, where x_k^l is the input data, b_k^l represent the bias in layer l, s_i^{l-1} represents the ith output value on layer $l-1$, and w_{ik}^{l-1} is the weighting factor between layer $l-1$'s kth neuron and layer l's ith neuron.

$$x_k^l = b_k^l + \sum_{i=1}^{N_{l-1}} conv1D\left(w_{ik}^{l-1}, s_i^{l-1}\right) \qquad (4)$$

The proposed network structure is that of three separate CNN, ConvNet-1, ConvNet-2 and ConvNet- 3 with varying layer size and parameters. The CNN uses a fixed size filter, extracts the most useful features by learning them all once, and combining all the good ones in a new dataset and learns them. By extracting only some of the features, the computational cost is reduced. As for the activation functions, *ReLU*, where *LReLU* and *ELU* are used to calculate kernel weight values. In order to minimize the cost function, the Adaptive Moment Estimation (ADAM) gradient descent function was used. ConvNet-1 and ConvNet- 2 present the same structure: Three convolution layers, each one followed by a MaxPooling layer, and three fully connected layers. The difference between these two is that ConvNet-1 has a learning rate of 0.001 whereas ConvNet-2 has a learning rate of 0.01. ConvNet-3 is smaller than the first two, having only two convolution-MaxPooling layers, followed by three fully connected layers, and presents a learning rate of 0.001.

4.2. Results

For the performance analysis on this method the three most popular metrics were used: Specificity, sensitivity and accuracy, described by the following equations:

$$Specificity = \frac{TN}{TP + FN} \quad (5)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (6)$$

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \times 100 \quad (7)$$

Where TN, TP, FN and FP are, respectively, the amount of true negatives, true positives, false negatives and false positives present in the results.

As for the ECG dataset, its comprised of 18 people: 5 male and 13 female, whose ECG were classified in 12 different types of signals depending on the location of the sensors. All the non-fiducial signals were used, whereas not the same can be said about the fiducial. This means that a larger amount of data was able to be constructed with the non-fiducial data than with the other kind. From this dataset, cross-validation was performed in a ratio of 80% training data and 20% testing data.

In the results, the ensemble network displays an improvement of a 0.8% in accuracy towards the single network for fiducial ECG signals, as shown in figure 12. As for non-fiducial signals, a minimum performance improvement of 0.4% and maximum of 1% within a period of 1 second is shown, and a maximum of 1.3% improved performance for a n- second period.

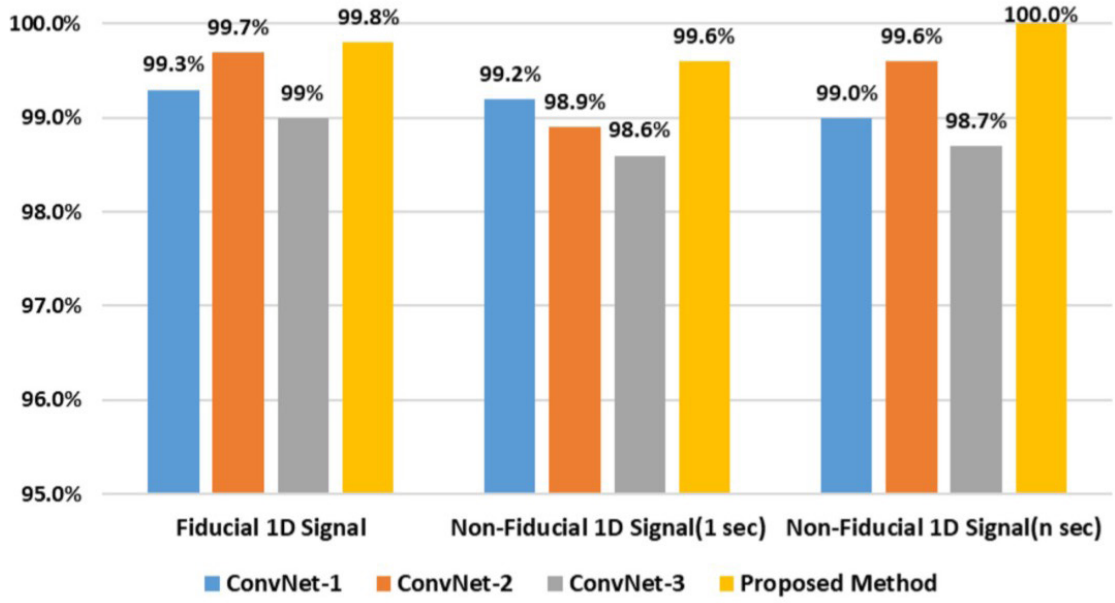

Figure 12: Performance improvements on fiducial and non-fiducial signals. Adapted from (Kim and Pan, 2019).

5. Conclusions

In this article, a survey was conducted on some of the most recent applications of deep learning in the rapidly growing field of biometrics. Firstly, a study on the twin identification problem was tackled by using Siamese

ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal
Regular Issue, Vol. 8 N. 4 (2019), 19-32
eISSN: 2255-2863 - http://adcaij.usal.es
Ediciones Universidad de Salamanca - CC BY NC DC

CNNs against the CASIA-Iris-Twins database, as well as Siamese Multi-layer CNNs. Its accuracy was studied between the both of them as well as against other state-of-the-art frameworks. Secondly, an enhanced method of fingerprint identification was proposed which involved contrast enhancement using histogram equalization followed by training of CNN layers. This method was tested with several different databases and scored better accuracy than the rest of the state-of-the-art frameworks in all of them. Finally, a new user recognition method was proposed using electrocardiograms (ECG) a brand new kind of signal on this field that has the properties of being significantly harder to fake than the rest of the main competitors, apart from being unique to each individual. This was run through an ensemble network comprised of three convolutional networks (ConvNet-1, ConvNet-2, and ConvNet-3), and then studied for fiducial and non-fiducial classifications. The final results gave the insight that this framework performed better when utilized with the full ensemble network rather than separating each network on their own.

Future works could take into consideration the mentioned models in this paper as a stepping stone in the research for even more efficient models, or perhaps applying them when developing new software or hardware to apply on this field.

6. References

Abdullayeva, F., Imamverdiyev, Y., Musayev, V., and Wayman, J., 2008. Analysis of security vulnerabilities in biometric systems. In *The second international conference: problems of cybernetics and informatics*.

Arora, S. and Bhatia, M. S., 2019. Fingerprint Spoofing Detection to Improve Customer Security in Mobile Financial Applications Using Deep Learning. *Arabian Journal for Science and Engineering*, pages 1–17. Bowyer, K. W. and Flynn, P. J., 2016. Biometric identification of identical twins: A survey. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8. ISSN null. doi:10.1109/BTAS.2016.7791176.

Bromley, J., Guyon, I., LeCun, Y., Säckinger, E., and Shah, R., 1994. Signature verification using a "siamese" time delay neural network. In *Advances in neural information processing systems*, pages 737–744.

Burger, B., Fuchs, D., Sprecher, E., and Itin, P., 2011. The immigration delay disease: Adermatoglyphia–inherited absence of epidermal ridges. *Journal of the American Academy of Dermatology*, 64(5):974–980.

Darve, N. R. and Theng, D. P., 2015. Comparison of biometric and non-biometric security techniques in mobile cloud computing. In *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, pages 213–216. IEEE.

Denker, J. S., Gardner, W., Graf, H. P., Henderson, D., Howard, R. E., Hubbard, W., Jackel, L. D., Baird, H. S., and Guyon, I., 1989. Neural network recognizer for hand-written zip code digits. In *Advances in neural information processing systems*, pages 323–331.

Gautam, G., Raj, A., and Mukhopadhyay, S., 2019. Identifying twins based on ocular region features using deep representations. *Applied Intelligence*, pages 1–18.

Ghiani, L., Yambay, D. A., Mura, V., Marcialis, G. L., Roli, F., and Schuckers, S. A., 2017. Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015. *Image and Vision Computing*, 58:110–128.

Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., and Titouna, F., 2019. A privacy-preserving cryptosystem for IoT E-healthcare. *Information Sciences*. ISSN 0020-0255. doi:https://doi.org/10.1016/j.ins.2019.01.070.

He, K., Zhang, X., Ren, S., and Sun, J., 2015. Deep Residual Learning for Image Recognition. *CoRR*, abs/1512.03385.

Jang, H.-U., Choi, H.-Y., Kim, D., Son, J., and Lee, H.-K., 2017. Fingerprint spoof detection using contrast enhancement and convolutional neural networks. In *International Conference on Information Science and Applications*, pages 331–338. Springer.

Khazaee, A. and Zadeh, A. E., 2014. ECG beat classification using particle swarm optimization and support vector machine. *Frontiers of Computer Science*, 8(2):217–231. ISSN 2095-2236. doi:10.1007/s11704-014-2398-1. Kim, M.-G. and Pan, S. B., 2019. Deep Learning based on 1-D Ensemble Networks using ECG for Re-al-Time. User Recognition. *IEEE Transactions on Industrial Informatics*.

Koch, G., Zemel, R., and Salakhutdinov, R., 2015. Siamese neural networks for one-shot image recognition. In*ICML deep learning workshop*, volume 2.

Marasco, E., Johnson, P., Sansone, C., and Schuckers, S., 2011. Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism. In *International Workshop on Multiple Classifier Systems*, pages 309–318. Springer.

Mehta, S. and Lingayat, N., 2008. SVM-based algorithm for recognition of QRS complexes in electrocardiogram. *IRBM*, 29(5):310 – 317. ISSN 1959-0318. doi:https://doi.org/10.1016/j.rbmret.2008.03.006.

Ogiela, M. R. and Ogiela, L., 2016. On Using Cognitive Models in Cryptography. In *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, pages 1055–1058. ISSN 1550-445X. doi:10.1109/AINA.2016.159.

Qibin Zhao and Liqing Zhang, 2005. ECG Feature Extraction and Classification Using Wavelet Transform and Support Vector Machines. In *2005 International Conference on Neural Networks and Brain*, volume 2, pages 1089–1092. ISSN null. doi:10.1109/ICNNB.2005.1614807.

Roy, A., Memon, N., and Ross, A., 2017. MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems. *IEEE Transactions on Information Forensics and Security*, 12(9):2013–2025. ISSN 1556-6021. doi:10.1109/TIFS.2017.2691658.

Schmidhuber, J., 2015. Deep learning in neural networks: An overview. *Neural networks*, 61:85–117. Simonyan, K. and Zisserman, A., 2014. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.

Zoph, B., Vasudevan, V., Shlens, J., and Le, Q. V., 2017. Learning Transferable Architectures for Scalable Image Recognition. *CoRR*, abs/1707.07012.