Siamese Network for Fake Item Detection⋆

(Discussion Paper)

Erica Coppolillo[1], Daniela Gallo[2], Angelica Liguori[1,*], Simone Mungari[1],
Ettore Ritacco[3] and Giuseppe Manco[4,†]

[1] *University of Calabria, Via P. Bucci, Rende, 87036, Italy*

[2] *University of Salento, Piazza Tancredi, 7, Lecce, 73100, Italy*

[3] *University of Udine, Via Palladio, 8, Udine, 33100, Italy*

[4] *Institute for High Performance Computing and Networking, Italian National Research Council (ICAR-CNR), Via P. Bucci 8-9/C, Rende, 87036, Italy*

Abstract

Currently, most multimedia users choose to purchase items through e-commerce. Nevertheless, one of the main concerns of online shopping is the possibility of obtaining counterfeit products. Therefore, it is crucial to monitor the authenticity of the product, thus adopting an automatic mechanism to validate the similarity between the purchased item and the delivered one. To overcome this issue, we propose a Siamese Network model for detecting forged items. Preliminary experimentation on a publicly available dataset proves the effectiveness of our solution.

Keywords

Siamese Networks, Supply Chain, Counterfeit Detection, Brand Protection, Deep Learning

1. Introduction

Forgery is an ever-growing and valuable issue in a sharing era where everyone is accustomed to online shopping. Unfortunately, users often unconsciously acquire a counterfeit item, paying a price that does not match its effective quality. Indeed, it might happen that the replica is so faithful that it is impossible to distinguish it from the original one. Counterfeiting leads to severe consequences for supply chain operations, therefore it is crucial to define solutions to overcome forgery issues by adopting effective traceability. A traceability system should include mechanisms for storing, accessing, and verifying information. To monitor product authenticity, it is hence useful to exploit such information and adopt specific approaches for discovering counterfeit goods. Traditional methods are based on marking techniques in which a visual eye mark, such as barcodes, or QR codes, is placed on the products or is encrypted or placed

SEBD 2023: 31st Symposium on Advanced Database System, July 02–05, 2023, Galzignano Terme, Padua, Italy

[*] Corresponding author.

[†] These authors contributed equally.

erica.coppolillo@unical.it (E. Coppolillo); daniela.gallo@unisalento.it (D. Gallo); angelica.liguori@dimes.unical.it (A. Liguori); simone.mungari@unical.it (S. Mungari); ettore.ritacco@uniud.it (E. Ritacco); giuseppe.manco@icar.cnr.it (G. Manco)

0000-0002-4670-8157 (E. Coppolillo); 0009-0009-3245-7738 (D. Gallo); 0000-0001-9402-7375 (A. Liguori); 0000-0002-0961-4151 (S. Mungari); 0000-0003-3978-9291 (E. Ritacco); 0000-0001-9672-3833 (G. Manco)

CEUR Workshop Proceedings (CEUR-WS.org)

in invisible parts of the items [1, 2]. More sophisticated traceability approaches are based on information technology solutions, including machine/deep learning-based approaches. Ahmadi et al. [3] propose a framework consisting of a feature extractor from electronic circuits (IC) images and a logistic regression algorithm employed to validate the authenticity and integrity of IC components. More recently, also Ant Colony Optimization algorithm (ACO) [4] and Convolutional Neural networks (CNN) [5] have been applied for counterfeit prevention. [6] apply Optical Character Recognition (OCR) for the digital transformation of the wine supply chain to prevent counterfeit wine commerce. In our work, the aim is to validate the authenticity of a product, comparing it with the original one. It is hence useful to define an automatic mechanism to validate the similarity between the actual item, previously chosen from the shopping catalog, and the delivered one. For this reason, we define a Siamese Neural Network [7, 8] model that, given two images in input, provides a similarity score by adopting two sub-networks. In particular, all the sub-networks share the same architecture, parameters, and weights, so that the updating of the weights happens simultaneously. Preliminary experimentation over a publicly available dataset proves the effectiveness of the proposed solution.

The rest of the work is organized as follows. In Section 2 we present the problem definition. Section 3 describes the methodology. Experimental evaluation is provided in Section 4. Final remarks and pointers for future work are discussed in Section 5.

2. Problem Definition

Let $\mathcal{X}$ be an online shopping catalog consisting of a set of items $\{x_1, x_2, ..., x_n\}$. Let $\mathcal{C}$ be the user/consumer/customer, i.e., a user that visits the catalog to buy an item, and $\mathcal{S}$ be the supplier, i.e., the provider of the items. When a consumer chooses an item, to certify its exchange it is needed to define a contract among the entities involved in the process. The contract contains information about the consumer and the supplier as well as information about the purchase and the characteristic of the item.

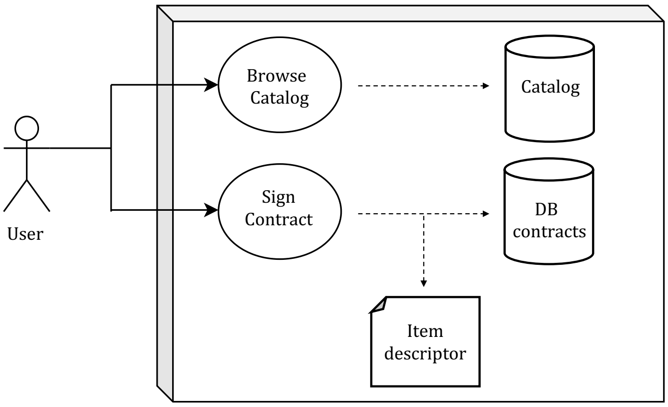


Figure 1: User-item workflow

As shown in Figure 1, we can depict in four steps the overall workflow that an item x fulfills, starting from the shopping catalog $\mathcal{X}$ to the client $\mathcal{C}$:

1. $\mathcal{C}$ chooses an item x from the shopping catalog $\mathcal{X}$;
2. $\mathcal{C}$ enters into an agreement containing contractual and goods specifications;
3. $\mathcal{S}$ delivers x to $\mathcal{C}$;
4. $\mathcal{C}$ receives x.

The item x is exposed to several vulnerabilities during the supply chain, e.g., replacement with a counterfeit version, alteration, and damage. In this sense, it is crucial to exploit an *Item Checking* component to validate its authenticity. Using such a component requires that the signed contract also contains identifiable features allowing to identify alterations of the items. Features should be chosen based on the value of the exchange item: indeed, high-value items, e.g., vintage paintings, could be equipped with high-value features, such as RFID (Radio-Frequency IDentification) and PUF (Physical Unclonable Function), while those of medium/low-value, e.g., shoes, with features like pictures and textual description. The selected features provide an *Item Descriptor* that is embedded in the contract. Moreover, since during the purchase the item can be personalized by the client, the item checking must be done by taking into account the information contained in the contract, and not in the catalog.

When the consumer receives the item, before accepting it, she/he must check its integrity. First, given the item, its *Descriptor* is extracted and sent to the *Item Checking* component. Such a component compares the received *descriptor* with the second one stored in the contract. If the item is compromised, an alert is raised and the client can signalize the counterfeit and claim for its compensation or its replacement. Otherwise, the client can accept the item after a positive outcome. Figure 2 depicts the workflow.

Generally speaking, integrity checking can be an onerous task due to the diverse type of descriptors, i.e., the identifiable features. Indeed, with respect to the nature of the descriptors, specific and sophisticated systems must be used, e.g., considering pictures as a feature, a smartphone can be used for checking the authenticity, while if the descriptor is an RFID/PUF, the smartphone is not the appropriate system and a more sophisticate (and also costly) equipment must be used, such as a microscope. Moreover, this kind of *descriptors* requires a huge amount of memory to be stored (especially in the case of PUFs). In addition, a new trend is to exploit Blockchains [9, 10] to certify the delivery process, denying the possibility of storing big item descriptors. For tackling these problems, we devised an automatic *Item Checking* component to reduce economic, memory usage, and computational costs by exploiting a Neural Network architecture. Our approach aims at classifying if two similar descriptors refer to the same item, by mapping their representation into a low-dimensional latent space: in particular, we aim to distinguish counterfeit items from the original ones by comparing *delivery* and *contract* item embeddings generated from their descriptors. To do this, our methodology is based on a Siamese network. The intuition is that points close in the latent space exhibit similar characteristics, thus they refer to similar items. To quantify their closeness we compute a distance measure over the low-dimensional vectors provided by the Siamese Network.

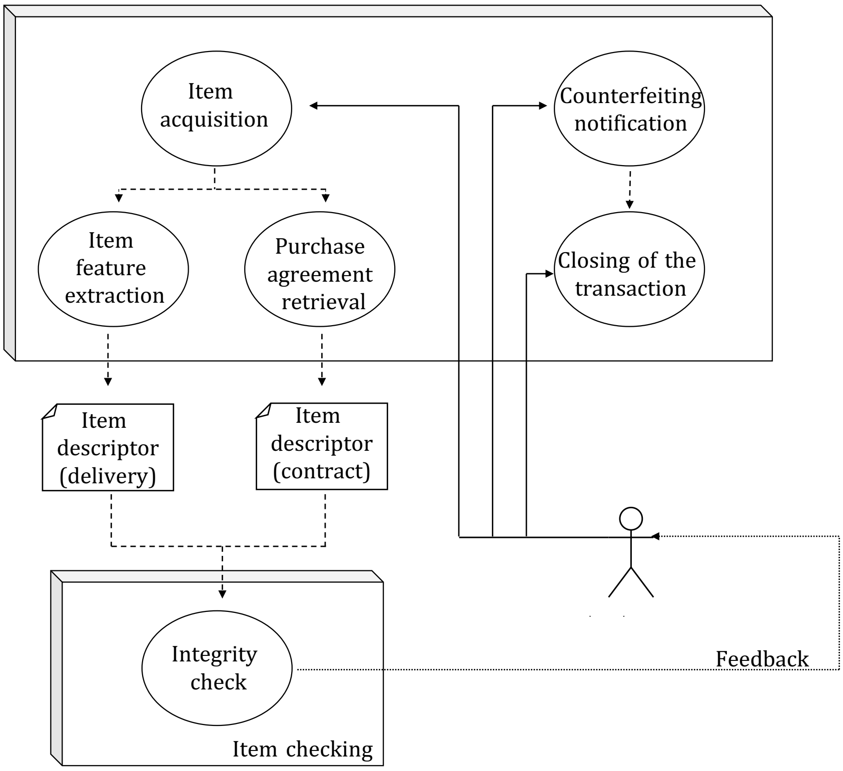

Item acquisition
Counterfeiting notification
Item feature extraction
Purchase agreement retrieval
Closing of the transaction
Item descriptor (delivery)
Item descriptor (contract)
Integrity check
Feedback
Item checking

Figure 2: Integrity check workflow

3. Methodology

In traditional classification tasks, a considerable amount of samples per class is necessary to obtain acceptable performances. However, if the network is trained against certain classes, it will not be able to classify the unseen ones. To overcome this issue, Siamese Networks (SNs) are particularly suitable and widely used. Bromley et al. [11] introduce the concept of SN to address the problem of signature verification via image matching.

SNs consist of two or more sub-networks processing two or more distinct inputs. The sub-networks are intended to be identical since they share not only their structure but also their weights. In this sense, supposing to have two inputs (and therefore two sub-networks) x_1 and x_2, if x_1 and x_2 are identical or very similar, their embeddings, named z_1 and z_2, will be similar as well since the two sub-networks share the weights and the two inputs have the same discriminative characteristics. The two embeddings are fed into a *distance module* that calculates their distance, e.g., euclidean distance, in order to provide their similarity score.

Figure 3 depicts the architecture of our model. Sub-network is composed of a pre-trained Res-Net model [12] followed by three fully-connected linear layers interleaved with a dropout

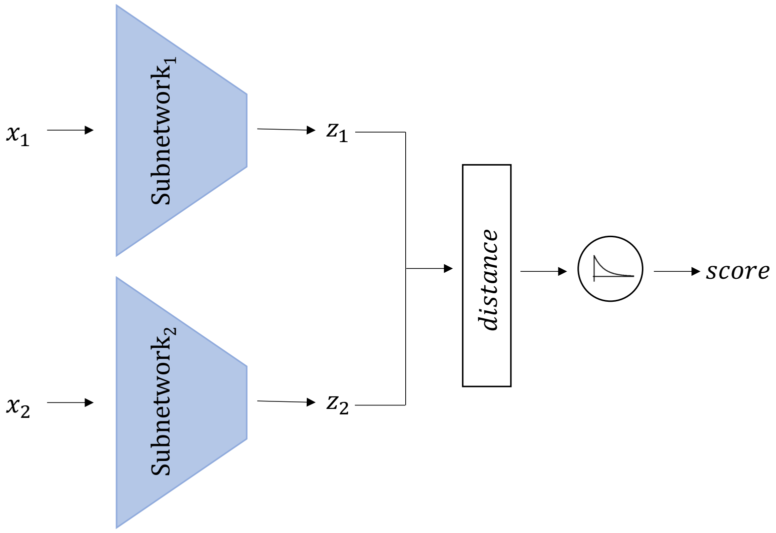


Figure 3: Our architecture

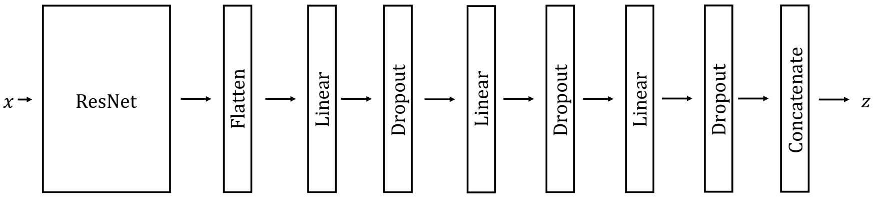


Figure 4: Sub-network architecture

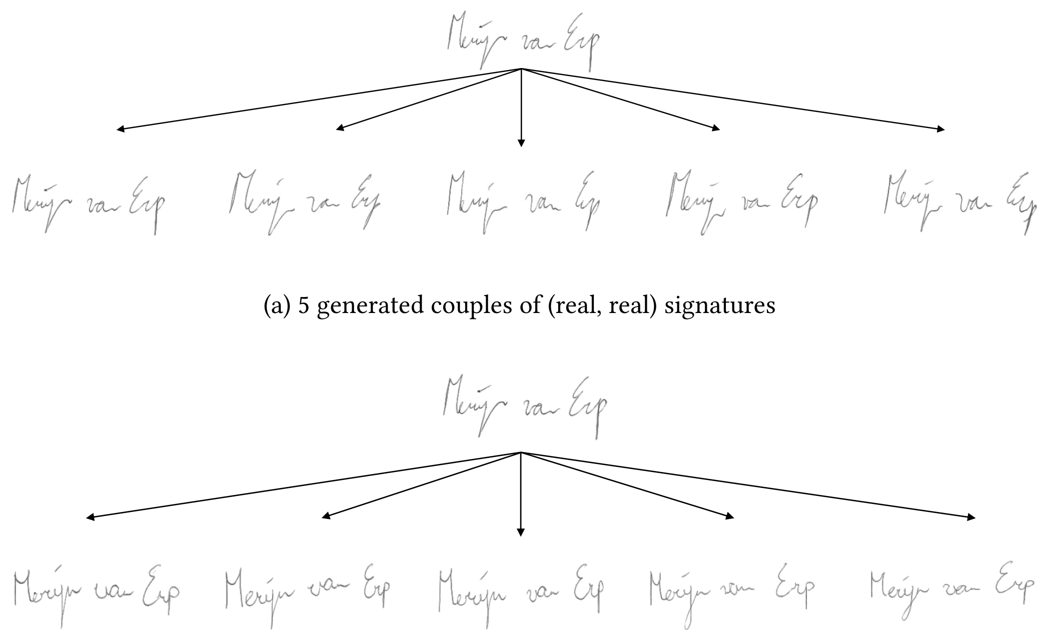
layer (to reduce overfitting issues). The outputs of these layers are concatenated to form the embedding vector. Sub-network architecture is shown in Figure 4. In our setting, since we have two inputs, two sub-networks are instantiated. A simple absolute distance is computed between the two embeddings produced by the sub-networks, and then a negative exponential function is applied to provide a similarity score in the range [0, 1]. A similarity score close to 1 means the two inputs are similar, while they are different otherwise. The loss function used to train the model is the *binary-cross entropy*.

4. Experiment Assessment

For the experimentation, we considered a use case whose aim is to identify counterfeit signatures. Specifically, we employed a dataset of handwritten signatures, publicly available on Kaggle[1]. The dataset contains:

- 140 real signatures provided by 28 subjects (i.e., each subject provided 5 signatures)
- 140 corresponding fake signatures

[1] https://www.kaggle.com/divyanshrai/handwritten-signatures



(a) 5 generated couples of (real, real) signatures

(b) 5 generated couples of (real, fake) signatures

In the following, we illustrate the adopted evaluation protocol. We generated both the signature couples (real, real) and (real, fake). The first group has been created by combining each real signature with the other real ones (itself included). Hence, for each subject, we obtained 25 combinations in total. Since they are couples of real signatures, they have been tagged with label 1. The second group has been created by combining each real signature with the 5 fake corresponding ones, hence we obtained other 25 combinations as well. These couples have been tagged with label 0. Figure 5a and Figure 5b depict a graphical example of 5 so-generated combinations of (real, real) and (real, fake) signatures, respectively.

After the couples generation procedure, we obtained a final dataset of 1400 tuples, equally partitioned into signatures couples of (real, real) and (real, fake). This dataset has been randomly split into training, validation, and test sets by using a proportion of 60-20-20%. The test set is composed of 125 couples of real signatures and 155 fake ones.

The model is implemented by using the TensorFlow framework[2]. The three fully-connected layers used in the sub-network are instantiated with 256, 64, and 8 neurons, respectively. Layer kernels are regularized with an L2 regularization penalty and a factor equal to 0.001. The dropout rate is set to 0.1. The model has been trained by using *k-fold Cross Validation*, with $k = 10$, over 50 epochs with a batch size of 8. The best model has been chosen according to the accuracy computed over the validation set. RMSprop [13] is adopted as optimizer with a learning rate equal to 0.0001. The metrics adopted for validating our approach are *Precision*, *Recall*, and *F1-score* as well as the AUROC (Area Under the ROC Curve) [14].

[2] https://www.tensorflow.org

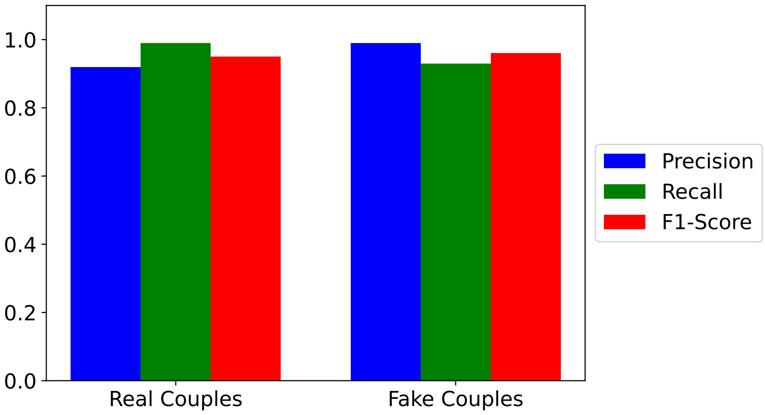


Figure 6: Results obtained over test set in terms of *Precision, Recall* and *F1-score*

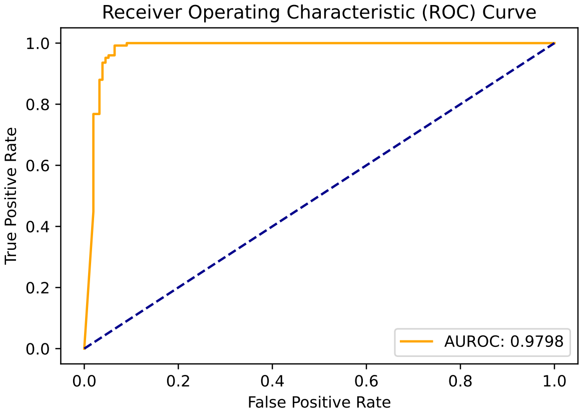
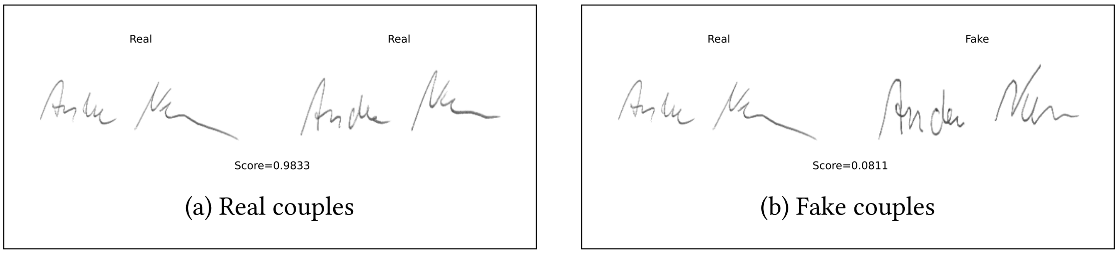


Figure 7: AUROC

Figure 6 shows the results obtained over the test set. As we can see, just a small percentage of fake couples (about 7%) have been misclassified as real, thus proving the robustness of our model also supported by the AUROC, shown in Figure 7, which is equal to 0.98. Figure 8 shows a visual example in which we can observe that the real and fake couples are correctly classified (see Figure 8a and 8b).

5. Conclusion

In this paper, we proposed a Siamese Neural Network that uses two sub-networks to validate product authenticity. Experimental results on public datasets prove the effectiveness and robustness of our model. This work is a starting point for future applications. First of all, we can consider sets of feature descriptors that vary depending on the asset price being traded. For instance, we may employ a set of more sophisticated descriptors for high-value assets to ensure



(a) Real couples

(b) Fake couples

Figure 8: A visual example of real and fake image couples

that we are accurately capturing their worth. Furthermore, we can explore several ways to strengthen security on multiple levels. One potential solution would be to carry out assessments on batches of items, certifying both the quality of the entire batch and the individual elements within it. By implementing these improvements, we can further simplify the sales process and inspire more trust in the system as a whole.

Acknowledgments

This work was partially supported by the Departmental Strategic Plan (PSD) of the University of Udine—Interdepartmental Project on Artificial Intelligence (2020-25) and by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

References

[1] Q. Dai, J. Li, U. A. Bhatti, J. Cheng, X. Bai, An automatic identification algorithm for encrypted anti-counterfeiting tag based on DWT-DCT and chen's chaos, in: ICAIS (3), volume 11634 of *Lecture Notes in Computer Science*, Springer, 2019, pp. 596–608.

[2] X. Fu, G. Li, S. Cai, H. Yang, K. Lin, M. He, J. Wen, H. Li, Y. Xiong, D. Chen, X. Liu, Color-switchable hybrid dots/hydroxyethyl cellulose ink for anti-counterfeiting applications, Carbohydrate Polymers 251 (2021) 117084.

[3] B. Ahmadi, B. Javidi, S. Shahbazmohamadi, Automated detection of counterfeit ics using machine learning, Microelectronics Reliability 88-90 (2018) 371–377.

[4] M. Shen, A. Liu, G. Huang, N. N. Xiong, H. Lu, ATTDC: an active and traceable trust data collection scheme for industrial security in smart cities, IEEE Internet Things J. 8 (2021) 6437–6453.

[5] S. A. Vo, J. Scanlan, P. Turner, An application of convolutional neural network to lobster grading in the southern rock lobster supply chain, Food Control 113 (2020) 107184.

[6] S. Cakic, A. Ismailisufi, T. Popović, S. Krco, N. Gligoric, S. Kupresanin, V. Maras, Digital transformation and transparency in wine supply chain using ocr and dlt, 2021 25th International Conference on Information Technology (IT) (2021) 1–5.

[7] A. Nandy, S. Haldar, S. Banerjee, S. Mitra, A survey on applications of siamese neural networks in computer vision, in: 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1–5.

[8] G. Koch, R. Zemel, R. Salakhutdinov, Siamese neural networks for one-shot image recognition, in: ICML deep learning workshop, vol. 2., 2015.

[9] P. Danese, R. Mocellin, P. Romano, Designing blockchain systems to prevent counterfeiting in wine supply chains: a multiple-case study, International Journal of Operations & Production Management (2021).

[10] P. Zhu, J. Hu, Y. Zhang, X. Li, A blockchain based solution for medication anti-counterfeiting and traceability, IEEE Access 8 (2020) 184256–184272.

[11] J. Bromley, I. Guyon, Y. LeCun, E. Säckinger, R. Shah, Signature verification using a "siamese" time delay neural network, in: J. Cowan, G. Tesauro, J. Alspector (Eds.), Advances in Neural Information Processing Systems, volume 6, Morgan-Kaufmann, 1993.

[12] K. He, X. Zhang, S. Ren, J. Sun, Deep residual learning for image recognition, in: CVPR, IEEE Computer Society, 2016, pp. 770–778.

[13] T. Tieleman, G. Hinton, et al., Lecture 6.5-rmsprop: Divide the gradient by a running average of its recent magnitude, COURSERA: Neural networks for machine learning 4 (2012) 26–31.

[14] F. Melo, Area under the ROC Curve, 2013.