Ashok Kumar Yadav, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 11, Issue 2, (Series-V) February 2021, pp. 23-29

RESEARCH ARTICLE OPEN ACCESS

Fingerprint Authentication Using CNN for Minutiae based Method

Ashok Kumar Yadav[1], ECE, JNTU, Hyderabad and Prof. T. Srinivasulu,[2]
UCE, K U Warangal, India

ABSTRACT
There has been an expansion in security concerns with respect to unique finger print based verification. This issue emerges because of advancement in technology in imitation and hacking innovations. This has provoked the requirement for a safer stage for recognition. In this research, we have involved a Deep Neural Network as a pre-confirmation channel to sift through artificial or imitated finger prints. As deep neural networks permit the framework to be more precise at identifying and decreases non genuine distinguishing proof via preparing itself over and over with test specimens, the proposed strategy works on the security and exactness by numerous folds. The execution of new secure finger prints recognition stage that takes the optical picture of a finger print as info. The given information is pre-confirmed utilizing Google's pre-train inception method for deep neural net applications, and afterward give through a ridge and valley minutia-based techniques for subject verification. Then, at that point, the outcomes are contrasted and prevailing models.
Keywords: Biometrics, deep learning, convolutional neural network, inception model, minutiae, fingerprint.

Date of Submission: 13-02-2021 Date of Acceptance: 27-02-2021

I. INTRODUCTION

A person may be identified by their distinctive qualities and attributes. The nature of these traits are two types: physical and behavioural. As of now, when we consider recognition, we quickly connect it with biometrics. Recognition, as a general rule, is finished by noticing and recognizing the extraordinary qualities of a person. These qualities can be highlights, for example, face features, iris texture, voice, offline signature, unique finger print vein and even fingerprint. We have planned numerous systems for distinguishing people in light of their special characteristics, however the majority of them are passed on as speculations because of the limitation of computing power and speed. In any case, nowadays, we can change over these speculations into common sense uses, and can make them accessible for everyday applications [10]. Previously, identification and validation of individuals were done by information-based systems, which make use of passwords or cards for authentication. As these methods are less reliable and less secure, the stored information can be easily hacked or lost. Therefore, there has been a need for more secure, complex, and unique identifiers for user authentication. Hence, biometric traits such as such as fingerprints, palm prints, face, iris, and ECG are found to be very useful for the recognition of individuals. Among the above-mentioned biometric traits, fingerprint-based authentication is the most popular one. Because of the above-mentioned risks, people have adopted fingerprint sensors for biometric authentication in many financial transaction platforms [10].

Already, ID and approval of people are carried with data-based frameworks, which utilize passwords or smart cards for verification. These strategies not much dependable and secure, the repository data can be simply hacked or miss used. In this way, there has been a requirement for safer, composite, and special identifiers for client validation. Henceforth, biometric characteristics, for example finger prints, palm prints, face, iris, voice and offline signature are viewed as extremely helpful for the authentication of a person. In all the biometric characterises previously mentioned finger print characteristics is unique and the most well-known one. In light of the above-mentioned threats, individuals have embraced unique fingerprints sensors for biometric confirmation in numerous monetary transaction stages [10]. Individuals' fingerprints patterns make the backbone of Unique fingerprint algorithms. The textures are made by extraordinary design of ridges and valleys.

These ridges are formed during our time in the birth of child in the womb, where a few factors like grinding, maternal circumstances, and so on influence their last shape and design. The development of these textures is all around the human body, including the palms, soles, and even veins. As such countless circumstances and variables assume a significant part in deciding the last ridge and valleys texture format, we consider finger print pattern examples to be novel to every single person. Verification of fingerprint turned into a standard in our everyday society that its weakness is rarely questioned. Because of innovation in technology, malicious efforts which sidestep security frameworks utilizing counterfeit fingerprints have been surged. Numerous frameworks today use techniques that tune the records in the repository with the info gave by the scanner to client verification. As these strategies in explicit applications are not altered and refreshed routinely at a speed that equivalents or surpasses the headway made by malicious people, it leaves biometric authentication system at an expanded danger and makes these systems vulnerable to cyber hacking.

Currently, there are many fingers print based solutions that can verify in very much less time in view of cutting edge and better computational power. It is greatly depended on man-made communication to give us expected outcomes. In this study, we are attempting in basically on finger print patterns and how we can additionally work on its security by utilizing upgraded integrated recognition systems.

II. RELATED WORKS

The basis of fingerprints authentication is that every individual is having unique pattern of ridges and valleys. Fingerprints pattern can be considered as an special texture of edges and valleys (Figure 1). Accordingly, finger print authentication is based on classification of special textures. This specific sort of issue is significantly interesting to address in view of the enormous intra-class and few inter class contrasts. Optical pictures of fingerprints can be arranged in light of the subtleties of its ridge setup. We can separate them into two distinct classes of ridges and valleys.

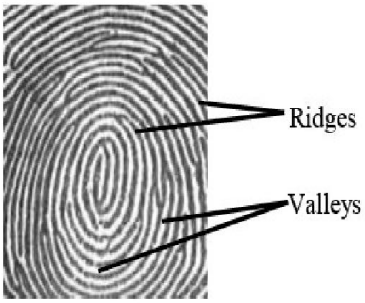

Figure 1 Ridges and Valleys in a Fingerprint.

The highest or first-layer (otherwise called worldwide) grouping depends on the visual characterization shaped by the ridge design, which gives us three definite area as loop, whirl, and delta. In the next layer, we can penetrate down further to see as more distinct and informative combination in these ridges, which are regularly alluded to as particulars. At long last, in the final layer, we can characterize based on every one of the elements of the ridge design. In the Market, there are many solutions are available based on finger print pattern. These solutions utilize include based learning methods. The elements incorporate worldwide elements, for example, the direction of the optical information, edge design, solitary focuses, and so on. Gabor channels [2] might be applied to chosen textures highlights of the information input. These characteristics can be extricated and arranged in number of ways relying upon the system utilized. A large number of these techniques are checked for precision and execution against well-known finger print data sets like NIST SD4, SD14, and SD9. The wide attributes of fingerprints are likewise utilized for grouping, specifically ridgeline stream, direction picture, particular focuses, and Gabor channel reactions. Among them, the direction picture is the most generally utilized. Texture extraction can be acted in more than one way, contingent upon the sort of component, the nature of the picture, and the exactness that the accompanying characterization stage requires. The objective of the order stage is to become familiar with a classifier in light of named fingerprints. The calculations proposed by different methods can be ordered as follows:

Directive: These techniques separate given finger print information input based on the unique pattern, considering their number and positions. Here, the peculiarity focuses are found and the last arrangement is done in view of the example framed by these singularities. A fine model is exhibited in Ref. [8].
Semantic: These set of rules are based on a general grammar, like in the case of natural language processing applications. Here, the features extracted

from the input data are stored as symbols in the database. The symbols are formed from ridgeline flows, which are then classified by a set of grammar.

Statistical: These methods are totally founded on the measurable information figured. This information are for the most part determined by utilizing normal measurable applications, for example, Bayesian choice rule, support vector machine (SVM), and K-closest neighbor (KNN). We can see an illustration of measurable methodologies in SVM-based arrangement and improvement of unique finger prints check in Ref.[12]. Deep Learning Net: These set of rules utilize multi-facet perceptron. The information are taken and the sorted elements are gone through the calculation subsequent to decreasing the dimensions [3]. The selected characteristics are by and large singularities and the direction of the picture, which is utilized to prepare the perceptron to work on its presentation. These organizations give extraordinary arrangement results. A Deep Neural Network - based methodology for the division of idle fingerprints is proposed in Ref. [19]. The design has two convolutional layers with 48 and 96 quantities of 3 × 3 channels, separately, in each layer to gain the start to finish highlights from video groupings. Multi-classifier: These techniques incorporate every one of the methodologies that consolidate at least two classifiers [11]. This exploration is remarkable, as we utilize the measurable (particulars based) and neural organization-based methodologies and consolidate them to accomplish better security and exactness. The model proposed here is the first of its sort, and it contrasts from the past works in the accompanying perspectives: Our analysis continues through two stages - pre-check stage and confirmation stage. In the pre-confirmation stage, great and phony fingerprints are sifted through. Then, at that point, the check stage confirms a decent unique finger impression. Unique mark pictures with low quality are considered as phony fingerprints. By utilizing the pre-check stage, the security of the framework can be expanded. We have applied the strategy of move learning in the pre-check stage. Google's Inception-v3, which is a pre-prepared profound CNN model, is utilized for preparing the pre-check stage. Confirmation of the fingerprints is finished by utilizing Gabor channel and KNN-based strategies.

III. PROPOSED METHOD

The optical information that is acquired from the unique fingerprint sensor is put away and gotten to by the framework in explicit organizations (for example .bmp, .jpeg, and so forth) We are utilizing these acquired contributions to prepare our deep neural net. These sources of info should be given additional consideration in advance, as, by and large, issues emerge during the check interaction (Figure 2).
For preparing to function admirably, we should assemble basically 100 visual examples of the fingerprints. The more we accumulate, the better the exactness of the prepared model. We additionally need to ensure that the sources of info gave are great to help us in the confirmation and arrangement processes.

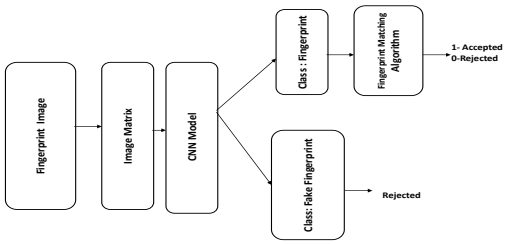

Figure 2 Proposed Block Diagram.

The information that we have gathered won't be totally utilized for the preparation interaction, as this can cause an opportunity for overfitting the neural organization model. This normal issue is handily settled by partitioning our information tests and involving a piece of them for the preparation cycle. Utilizing a piece of the information keep the model from remembering the examples gave. We can utilize the leftover information contributions to check whether or not overfitting is happening. How much overfitting is estimated by the exactness and accuracy of the prepared model. We have the choice to divide the information into various proportions. By and large, neural organization based applications split the information by 1:1:8. The 80% of the split is utilized for the preparation interaction; the 10% of the examples is utilized to approve the info information during the preparation cycle; and the leftover 10% is utilized as the testing information contribution to confirm the exactness and execution of the now prepared model [15]. The delivered outcomes can be additionally improved by applying mathematical operations to the information (for example editing, lighting up, misshaping, and so forth). These mathematical operations will assist the classifier with adjusting certifiable situations to additionally work on the correctness and execution. It utilized a customary optical finger impression sensor to catch our finger print input. The .NET system, which utilizes tensor flow [1], is utilized to foster the neural organization model for the pre-order process.

Inception Model

We are involving a CNN for the grouping of the information pictures (Figure 3). CNNs are artificial neurons organizations that involve various layers and are by and large used to group optical information. CNNs take the optical info and cycle them as tensors. Tensors are the portrayal of the information input as a multi-faceted lattice. The optical picture is for the most part handled by applications as a two-layered (2D) input. Here, the model will change the 2D contribution over to a 4D network [16].

We are involving a CNN for the grouping of the information pictures (Figure 3). CNNs are artificial neurons organizations that involve various layers and are by and large used to group optical information. CNNs take the optical info and cycle them as tensors. Tensors are the portrayal of the information input as a multi-faceted lattice. The optical picture is for the most part handled by applications as a two-layered (2D) input. Here, the model will change the 2D contribution over to a 4D network [16].

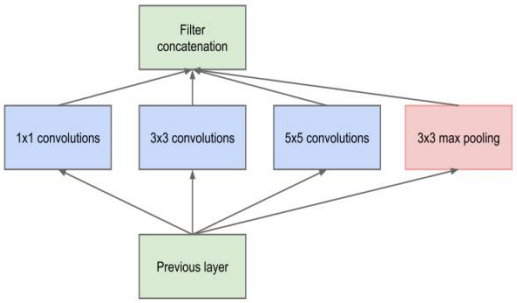

Figure 3: Basic Inception CNN Architecture.

The CNN model here utilized is Google's Inception-v3 [4]. This model has effectively been pre-prepared on all picture information from ImageNet [5]. As this is a pre-train net, the training time expected for the grouping system can be decreased by many folds. This model can be retrained utilizing move learning, by which we can alter the model for our requirements. The abatement in preparing time is conceivable in light of the fact that we are just preparation the last layer of the model to make it reasonable for our application. ImageNet is a data set that comprises of numerous hubs, and every hub contains more than100,000 pictures coordinated by the WorldNet ordered progression.

Transfer Learning Technique is used here for pre-training of Inception-v3 model is applied for sifting through quality fingerprints. Commencement v3 utilizes a deep net design. In this design, the lower layers recognize the low-level highlights and the more significant levels distinguish high level elements. Along these lines, when we need to involve this model for an alternate reason, we really want to prepare just the last layer of this model. The result layer ought to likewise be re-imagined. With the exception of the last layer, the boundaries we use are something very similar, which the model has gained from ImageNet. The last layer of the model has 2048 channels of 1 × 1 size. We have changed this layer to a completely associated layer. This completely associated layer contains 2048 neurons. During preparing, the organization learns the loads between the neurons and the inclination of result neurons. Table 1 gives the boundaries of the model.

Table 1: Model Parameter Table

Parameters	**Value**
Nos of neurons	2048
Loss function	Cross entropy
Learning rate	0.001
Epochs	100
Batch size	32
Dropout	0.5
Optimiser	Adam

Google's Inception-v3 model comprises of numerous convolutional bits that differ in size. Each of these convolutional bits distinguishes highlights for each aspect and scale. This model takes on the type of leftover organization that utilizes skip associations (Figure 4). Residual netss take the info information and add them to the result, along these lines empowering the organization to foresee the lingering input rather than the normal result [6].

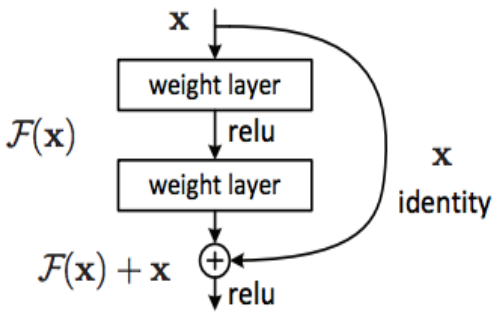

Figure 4: Basic Blocks of Residual Learning [8]

The inception model is prepared to group whether or not the gave input is a type of unique finger pattern. This model assists sift through poor quality data sources that with having looking like elements to that of a unique finger pattern input. Consequently, this classifier can recognize inputs with a specific degree of commotion. An exactness of somewhere in the

range of 90% and 95% is acquired, albeit the specific worth fluctuates from one hurry to another. This is because of the uncertainty in the preparation steps.

a) Attributes Requirements-The result of the inception method is a decent unique finger print that is an unique example of edges and valleys. A ridge is characterized to be a solitary bended portion, while a valley is the region between two neighboring edges. The significant elements of the unique fingerprint are minutiae points and are utilized to match the fingerprints. These Minutiae pattern are utilized to decide the uniqueness of the finger print. A decent quality unique finger print can have 20-75 unique pattern of ridges and valley upon the sensor and scanner used [14].

Minutiae can be defined as the points in the fingerprint where the ridges end or divide. There are several types of divisions or ends in a ridge line, which can be segregated as follows: Ridge dots - these are extremely tiny ridges that are too short to be considered as a ridge line. Ridge endings – these are the end points of a ridge line. Ridge ponds/lakes – these are the cavities formed in between diverging ridges. Ridge islands – these are longer ridge dots that are found inside ridge ponds. Ridge bifurcations – these are points where ridges begin to diverge. Ridge spurs – these are the inclinations found on a ridge line. Ridge bridges – these are found on the point where two tiny ridges adjacent to each other join. Ridge crossovers – these are found at the point of overlap between two ridge lines. Our minutiae verification techniques take the filtered fingerprint from the classifier as input and finds the minutiae points from the fingerprint pattern. Further, extracted the ridge endings and bifurcations from the fingerprints image pattern. Then, these points are used for matching with the repository.

Pattern Extraction and Minutiae Matching

The initial step for this recognition approach is standardization, which brings about a superior differentiation of the unique finger print input. Then, at that point, this information is changed into a grey scale characterization. Then, at that point, apply a few remedial acclimations to the information, like changing the picture brightness and difference. Then, at that point, the undesired signals in the info is removed through utilizing a Gabor channel [2]. The Gabor kernel is a linear kernel that determines the output using a harmonic function, which is then multiplied using a Gaussian function. It consists of an orientation- and frequency-specific sinusoidal plane that is adjusted by a Gaussian envelope [17]. The Gabor kernel provides a suitable visual representation of the input. Then, the feature map is created, which is used as the template. This template is matched in the subsequent matching step with templates of other fingerprints. The result of the matching is the matching score, which represents how nicely two fingerprints similar to each other. To match the Template matching KNN methods [7] used. The KNN method makes use of the Euclidean distance, which can be calculated by using the following formula:

$$L(a,b) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + \cdots (a_n - b_n)^2} \quad (1)$$

The KNN Technique allocates a class tag to every minutia. Then, at that point, the k nearest individuals are found by figuring the Euclidean distance between the particulars. In our investigation, the worth relegated for k is 2. Subsequently, our calculation finds two closest particulars for every minutia. Then, at that point, during coordinating, a nearby matching is performed to observe which are the details in the question finger impression that coordinate with the particulars in the unique mark formats in the data set. Then, at that point, a worldwide matching is done to discover the number of details of the question unique finger impression coordinate with the particulars of the layout finger impression. In light of that, a matching score is created, which give a sign on whether the unique mark coordinates with any of the fingerprints in the information base [14].

IV. RESULTS AND DISCUSSION

Present Existing solutions and sensors have a certain amount of false acceptance and false rejection, which is factored into during the recognition process. Transfer learning method used here rather than going for the traditional methods to decrease the training time. By application of TensorFlow tool, an accuracy of 94.5 percent achieved with proposed solution. which can be seen in Figure 5 The orange line is the accuracy of our model on the training set. and the blue line shows the accuracy of the model on the testing set.

Model	Accuracy range	Depth	Parameters
VGG16	0.71–0.90	23	138,357,544
ResNet50	0.75–0.92	168	25,636,712
Inception-v3	0.78–0.94	159	23,851,784

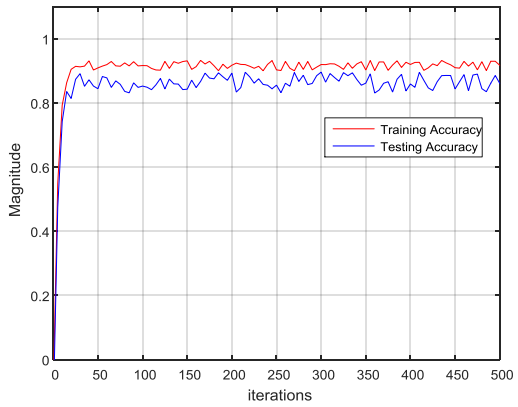

Figure 5: Training vs. Test Accuracy

A fingerprint scanner module that integrates a artificial finger detection technology has to decide, for each transaction, if the current sample comes from a real finger or from a artificial one. The error in this decision should be as low as possible.

FRR_{fd} and FRR_{iv} –Measurement of error rates.

FAR_{iv} – For real-finger system incorrectly reject the input to come from a fake finger.

FAR_{fd} – For fake-finger system incorrectly accepts input to come from a real finger.

For the fake-detection mechanism, the overall false rejection ratio (FRR) error can be estimated as follows

$$FRR = FRR_{fd} + (1 - FRR_{fd}) \times FRR_{iv} \quad (2)$$

Overall false acceptance ratio can be predicted as follows,

$$FAR^{Real\ Non\ Enrolled} = (1 - FAR_{fd}) \times FAR_{iv} \quad (3)$$

for an intruder trying to be authenticated using a fake reproduction of a finger that is not the enrolled one and

$$FAR^{fake\ Enrolled} = FAR_{fd} \times \alpha \quad (4)$$

where $\alpha < (1 - FRR_{iv})$. If a fake fingerprint is created by using sophisticated tool or device, its quality is usually lower than the real finger it is designed to imitate, and therefore the chance that the identity verification algorithm does not match it with the user's real template is higher.

It is Desired, the FAR have a certain low value; let us assume it to be *x*.

Fingerprint classification accuracy is around 94.3%. Thus, as proposed CNN is acting as a pre-filter, we can reduce the FAR of any system by using the multiplication rule of probability.

Comparison of the FNAR and FAR for existing methods of Fingerprint Recognition using Minutiae Score Matching with the proposed method. It is observed that the FNAR for both methods is zero, and the FAR is 0.026 for the existing method and 0.00156 for the proposed method.

Table 2: Regular Matching vs. Proposed

	Exiting Score	Proposed(DL)
FRR	0	0
FAR	0.026	0.0017

Table3: Comparison of Pre-trained Deep Learning Network.

Testing of proposed method with batch sizes 8, 16, and 32. The method gives expected results when the batch size is 32. The network is trained for 25, 50, and 100 epochs. It is found that the model performs better for 100 epochs. To avoid over fitting of the model, early stopping is also applied. Table 3 shows the comparison of various pre-trained deep neural models.

V. CONCLUSION

In our research we have followed a novel approach in first phase to pre-processing of bad fingerprint. through terrible fingerprints. Assuming the result of the commencement model says that it is a decent finger impression, it is given to the confirmation module where matching of the finger print is performed. By consolidating a profound CNN pre-channel to the details matching finger impression confirmation calculation, we have accomplished a better exactness of roughly 90-95%. There are

numerous impending advances relating to unique finger pattern biometrics, for example, on account of PDAs. Major chip manufacturers are thinking of sensors for ultrasound that can go through strong items to catch data from our fingertips. These advancements might have a few undesired signals related with them. As commotion is straightforwardly connected with a high FAR, our fuse of a pre-channel deep learning networks will decrease undesired signal considerably to keep up with security to current regulation norms.

VI. REFERENCES

[1] Antonelli. A, Capelli. R, Maio. D and Maltoni. D (2006), "Fake finger detection by skin distortion analysis", Information forensics and security, IEEE transactions on, Vol. 1, No. 3, pp. 360-37

[2] Z. Xu, S. Li and W. Deng, learning temporal features using LSTM-CNN architecture for face anti-spoofing, in: 3 rd IAPR Asian Conference on Pattern Recognition (ACPR), 2015, IEEE, pp. 141–145, 2015.

[3] Graganiello. D, Poggi. G, Sansone. C and Verdoliva. L (2013), "Fingerprint liveness detection based on weber local image descriptor", in Biometric Measurements and Systems for Security and Medical Applications (BIOMS), IEEE Workshop on. IEEE, 2013, pp. 46- 50.

[4] F. Chollet, Xception: deep learning with depthwise separable convolutions, arXiv preprint (2017), 1610–02357.

[5] J. Deng, W. Dong, R. Socher, L.- J. Li, K. Li and L. Fei-Fei, ImageNet: a large-scale hierarchical image database, in: IEEE Conference on Computer Vision and Pattern Recognition, 2009, CVPR 2009, IEEE, pp. 248–255, 2009.

[6] K. He, X. Zhang, S. Ren and J. Sun, Deep residual learning for image recognition, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, IEEE, pp. 770–778, 2016.

[7] Y. Zhu, X. Yin, X. Jia and J. Hu, Latent fingerprint segmentation based on convolutional neural networks, in: 2017 IEEE Workshop on M. Kawagoe and A. Tojo, Fingerprint pattern classification, Pattern Recogn. 17 (1984), 295–303.

[8] Ciresan. D, Meier. U and Schmidhuber. J (2012), „Multi-column deep neural networks for image classification",inc omputer vision and pattern recognition (CVPR), IEEE 2012, pp. 3642-3649

[9] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of fingerprint recognition, Springer Science & Business Media, London, 2009.

[10] D. Michelsanti, Y. Guichi, A.- D. Ene, R. Stef, K. Nasrollahi and T. B. Moeslund, Fast fingerprint classification with deep neural network, in: International Conference on Computer Vision Theory and Applications, 2018.

[11] A. Rani and D. S. Palvee, SVM based classification and improvement of fingerprint verification, Int. J. Sci. Eng. Technol. Res 3 (2014), 879–883.

[12] K. Rao and K. Balck, Type classification of fingerprints: a syntactic approach, IEEE Trans. Pattern Anal. Mach. Intell. 2 (1980), 223–231.

[13] J. Ravi, K. B. Raja, K. R. Venugopal, Fingerprint recognition using minutia score matching, Int. J. Eng. Sci. Technol. 1 (2009), 35–42.

[14] K. Simonyan and A. Zisserman, Very deep convolutional networks for large-scale image recognition, arXiv preprint arXiv:1409.1556 (2014).

[15] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke and A. Rabinovich, Going deeper with convolutions, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1–9, 2015.