UDC 004.8:67
DOI: 10.25140/2411-5363-2020-2(20)-139-149

Olena Kryvoruchko, Bohdan Bebeshko, Karyna Khorolska,
Alona Desiatko, Nataliia Kotenko

ARTIFICIAL INTELLIGENCE FACE RECOGNITION FOR AUTHENTICATION

Urgency of the research. *Technical progress leads to a tremendous increase in number of cybercrimes. Almost every person around the globe has a range of digital accounts containing sensitive private information which is in fact protected by simple password. Therefore, security systems have a great and important role to guard privacy. It is necessary to have a solid system which can distinguish between people and act differently based on their permissions.In difference between face recognition authentication and other identification solutions such as passwords, email verification or fingerprint identification - biometric facial recognition uses unique mathematical and dynamic patterns that make such system one of the safest and most effective.*

Target setting. *Face recognition authentication is about to be one of the most stable. There is a range of methods that are available for detecting and processing faces using different levels of complexities. Summing up - face recognition for authentication purposes can emphasizes security. Convolutional neural networks (CNN) outperform any possible humans' recognition rate. However, such systems should be continuously manually improved. Another problem with such systems is that they require accurate data to be trained before they are actually being deployed. It is essential for such system to be fast enough to recognize people and that the training should be accomplished without much difficulty and also be fast.*

Actual scientific research and issues analysis. *Face recognition algorithms have been reviewed in a range of scientific papers such as Haar Cascades, Kalman Filter and applied in various spheres. Among research papers, there is a range of security systems that use face recognition technology. Facial recognition approach for security access and authentication presented by Jeffrey S. Coffin uses custom VLSI Hardware and Eigenspaces method. Systems provided by Shankar Kartik uses Eigenfaces method for face identification as well which in fact gives weak results with moderate accuracy.*

Uninvestigated parts of general matters defining. *The swiftness of the particular face recognition systems heavily depends on the changes in conditions of light, expression, camera density, and on partial blocking of the face. Several scientific works have already proposed range of approaches for face recognition under unpleasant conditions, but not much of them actually work.*

The research objective. *This article aims to describe Face Recognition authentication system experimental architecture inside informational system accessible via web interface. The Face Recognition authentication system consists of a camera node, a cloud server and input-output device for interacting with users by means of web interface.*

With the advancement in web and cloud, this article represents development of the authentication system based on Face Recognition System. Using Google next-generation system, TensorFlow with a deep learning framework on board. TensorFlow is flexible, portable and open source project.

The statement of basic material. *As it is known - the human brains vision seems to be very easy functioning. It does not take any difficulty to tell apart a dog and a cat, read a word or recognize a human face. But in difference from human - these tasks are really difficult problems for solving with a computer. Recognition process only seems easy because human brain is really good at perception and as a result in understanding images. During last years, machine learning has made great progress in solving these difficult problems. In particular, model called - deep convolutional neural network can result in reasonable performance on solving difficult visual recognition tasks which are matching or exceeding human performance in some aspects.*

Conclusions. *This paper introduced a new method of obtaining data for training security systems from social media and human interaction for future use in authentication process in various informational systems. There are several advantages of proposed system which can be described. First of all, one should mention that using of TensorFlow can be adaptive, powerful, and flexible. Moreover, training time is acceptable in comparison with other frameworks and much more faster if one uses distributed TensorFlow.*

Keywords: *artificial intelligence; face recognition; neural network; informational systems; authentication.*

Fig.: 1. Table: 2. References: 22.

Urgency of the research. Technical progress leads to a tremendous increase in number of cybercrimes. Almost every person around the globe has a range of digital accounts containing sensitive private information with is in fact protected by simple password. Therefore, Security systems have a great and important role to guard privacy. It is necessary to have a solid system which can distinguish between people and act differently based on their permissions.

Target setting. Yet, face recognition authentication is about to be one of the most stable. There is a range of methods that are available for detecting and processing faces using different levels of complexities. Summing up - face recognition for authentication purposes can emphasize security. It has already been used in many applications like mobile device authentication. Anyways convolutional neural networks (CNN) outperform any possible humans' recognition rate. However, such systems should be continuously manually improved. Another problem with such systems is that they require accurate data to be trained before they are actually being deployed. It is essential that the system is fast enough to recognize people and that the training should be accomplished without much difficulty and also be fast.

With the advancement in web and cloud, this article represents development of the authentication system based on Face Recognition System. Using Google next-generation system, TensorFlow[1] with a deep learning framework on board. TensorFlow is flexible, portable and open source project.

Actual scientific research and issues analysis. Face recognition algorithms have been reviewed in a range of scientific papers such as Haar Cascades[2], Kalman Filter[3] and applied in various spheres [4; 5; 6]. Besides, OpenCV is a swift open source project which supports many methods to recognize faces. However, in this article, Dlib C++ library was used which supports machine learning algorithms and uses histogram-of-oriented-gradient approach. Face recognition is not only used by the camera node on the stage of face detection but also useful on the stage of input data pre-processing. In this article, a modern data collection method was described (collection from social media with help of Facebook API as well as with help of human to label the unknown people, that directly helps in the process of neural network incremental learning process for the model with new data). The interface was also designed for easy uses in a range of device types.

Modern authentication in field of cyber security has been an essential feature in all aspects of digital life and received a growing interest in recent years. Numerous security systems have been used in the market for many pre-potent enterprises such as ADT [7], Vivint [8] and Protect America. However, none of them use face-recognition approach in their solutions because of low confidence and special computational requirements. NetAtmo [9] has released a device that uses deep neural network to recognize the face, nevertheless their system is far from perfect. Moreover, they provide special smart camera that in fact doesn't satisfy requirement to be compatible with any laptop or smartphone for authentication purposes. In addition - it is slow, feedback is lagged, therefore notifications are constantly delayed, and it takes valuable time to learn face sets, or search for matches in database.

Among research papers, there is a range of security systems that use face recognition technology. Facial recognition approach for security access and authentication presented by Jeffrey S. Coffin [10] uses custom VLSI Hardware and Eigenspaces method. Systems provided by Shankar Kartik use Eigenfaces method for face identification [11] as well which in fact gives weak results with moderate accuracy.

Uninvestigated parts of general matters defining. The swiftness of the particular face recognition system heavily depends on the changes in conditions of light, expression, camera density, and on partial blocking of the face. Several scientific works have already proposed range of approaches for face recognition under unpleasant conditions, but not much of them actually work. Another technology called FaceNet uses deep convolutional neural network implementing Inception model[12] architecture from Google and moreover utilize the online triplet-mining approach to train instead of an intermediate bottleneck layer. FaceNet system achieved a new record accuracy of 99.63% on the Labeled Faces in the Wild (LFW) [13], dataset, which is commonly used for testing purposes. Nevertheless, not only databases size increases but also its computational cost and therefore recognition accuracy declines respectively. That is why incremental learning algorithm should be used, as soon as it is a learning algorithm which handles large-scale training data with respective efficiency and accuracy. A short definition of incremental learning is: learning process represented as a gradual process with new data. The idea behind this algorithm is the existence of special classifiers that are identified along with new classes to be learned [14]. And the key point is to begin learning process with as low as possible resolution images and then gradually increase to high resolution.

The research objective. This article describes Face Recognition authentication system experimental architecture inside informational system accessible via web interface. The Face Recognition authentication system consists of a camera node, a cloud server and input-output device for interacting with users by means of web interface.

The camera node is as it was previously mentioned - vital for system to exist. Nowadays, almost any device has own web-camera, which is typically placed in front of the users face. Whenever person needs to authenticate or re-authenticate, the camera node will capture a photo, and process it in advance. The camera nodes must be positioned in such way that it has a wide range of vicinity over the subject and therefore detect face approaching the camera from distance. The camera node first has to detect the human face, and then it directly sends data to the cloud for further processing. Cloud runs image processing remotely by using DLib library and TensorFlow installed. For small-sized authentication system even smallest VPS cloud server would be enough for processing data, but for training neural network more powerful cloud server will be required as soon as model learning process requires expensive computation.

Cloud computing is a great advancement of modern days. Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing provides a simple way to access servers, storages, databases and a broad set of application services for research over the internet. Represented system uses two cloud servers to support its functionality. First one is a weak low-powered server only for data processing tasks. Second is as powerful server handling all model training tasks. A face recognition algorithms using CNN requires a lot of computational power machine during functioning process. Cloud computing providers offer a reliable solution at a very low cost for such kind of CPU consumption. Following on the architecture, the first cloud server unit will receive data from the input nodes (most of cases represented by the laptop web camera) and save then push data forward to the second cloud server unit where it will train the data after defined collection period needed to form a suitable dataset. First cloud server unit also interacts with the administrator via web interface utilizing HTTP protocol. The first cloud server has a database with a record of all users being granted authentication permissions. The first cloud server has ability to communicate with the input units on the device using web-socket enabling real-time data processing. Therefore it is obvious that the first cloud server also has a web-based server crawling data from Facebook and saving all data to storage.

The first cloud server has ability to communicate with any smart device accepting direct TCP connection or at least supporting HTTP protocol. Frontend authentication algorithm is running in web and therefore is controlled by the first cloud server. The administrator area of the system allows the owner to control users and also to change their permission level. Based on the granted access level, different users will able to access different sections of any kind of system behind face recognition authentication. This article demonstrates the capabilities of the system using a miniature license management system. Whenever a person is detected via authentication system, data is sent to the first cloud server and it defines access level for this person. If it is a new person - the first cloud server sends an alert to the administrator with access violation notice. The administrator therefore can register the person in the system or take necessary actions in case of any security breach.

To increase stability one can use social network for training face recognition model and also for updating data on current, existing users in the system. This is definitely a new approach in collecting data. Social networks are the largest free, diversified, adaptive dataset with ability to track changes in real-time and online. By using the advantage of Facebooks' Graph API, one can easily detect a face with a tag name, define if this person was registered in the system, authenticate it or send administrator a notice of security violation with additional information about the suspect. Moreover, one can upload all picture with user's faces to the first cloud unit. And most importantly, the facebook developer app is simple and convenient to share between users. That means that one can benefit with additional data collecting faces of already registered users, they only need to log-in with their account and accept the app to collect pictures. The social network node has three collecting interfaces. First is a public application from Facebook developer website, second is from a web-based hosted on the first cloud server, the last one can be application on iOS or Android device. These are simplest way to collect face images with labeled faces of users who are given or not given access.

The statement of basic materials. As it is known - the human brain vision seem very easy functioning. It does not take any difficulty to tell apart a dog and a cat, read a word or recognize a human face. But in difference from human - these tasks are really difficult problems for solving with a computer. Recognition process only seems easy because human brain is really good at perceptions and as a result in understanding images. During last years, machine learning has made great progress in solving these difficult problems. In particular, the model called a deep convolutional neural network can result in reasonable performance on solving difficult visual recognition tasks which are matching or exceeding human performance in some aspects.

Currently, various image recognition methods and systems based on them are actively developing and therefore successfully solving such tasks as identifying fingerprints, corneas of the eye, analyzing aerospace images, monitoring information flows in a computer network, detecting forgeries, recognizing license plates, handwritten texts, scanned postal, latent, financial and accounting documents. These methods of pattern recognition made it possible to solve complex tasks. In this regard, it is necessary to consider the possibility of applying these methods for authentication purposes.

Researchers have demonstrated reliable methods of computer vision simulation by validating their works on ImageNet [15] - an academic benchmarking system for computer vision algorithms. Subsequent models improve each time to achieve a new bench result: QuocNet [16], AlexNet [17], Inception (GoogleNet), BN-Inception-v2 and Inception-v3 [18]. Inception-v3 was the latest trained model for the ImageNet Large Visual Recognition Challenge from Google. During this work face recognition module was implemented based on the method presented in FaceNet and the training Inception-v3 model in TensorFlow. Instead of using Inception (GoogleNet) model architecture, Inception-3 architecture to train a new model with improved accuracy was used.

Basing on the published architecture and therefore model from the OpenFace and Inception-v3 model a new model with a new database set was trained. Input data is collected by usage of a face detection method and after goes through the deep convolutional neural network to extract an embedding feature. Therefore one can use features for similarity detection and classification.

While processing an image using DLib [19] for face detection one should first define a square around the faces. Each face should then be passed separately into the neural network, which expects a fixed-sized input, currently 1024x1024 pixels, but even 96x96 pixels would be enough as mentioned in FaceNet [12], which is the best size giving the highest accuracy and low training time. But in case and purposes of face authentication one need more detailed analysis therefore accepted reshape of the face in the square was accepted as constant size of 1024x1024 pixels. A potential issue is that faces could be looking in different directions or have some distortions and one have to rotate the images. We use align faces method described in OpenFace by first finding the locations of the eyes and nose with Dlibs' landmark detector, and if the face is undetected or unaligned which will be eliminated before going to the neural network. Finally, an affine transformation is performed on the cropped image to make the eyes and nose appear at about the same place.

Artificial neural networks provide powerful flexible and versatile learning mechanisms, which is their main advantage over the other methods mentioned above. Training eliminates the need to choose key features, their significance and the relationship between features. But, nevertheless, the choice of the original input data significantly affects the quality of the solution. Neural networks have a good generalizing ability, that is, they can successfully spread the experience gained in the final training set to a variety of images.

Neural networks can be trained in a complex structure of images with less memory than is required for classification by structural methods. Training eliminates the need to choose key features and relationships between features. The parallelism of the work of neurons provides fast and high-quality pattern recognition.

Due to a good generalizing ability, artificial neural networks can successfully recognize images that are not shown in training, and also be resistant to noise in the input data.

Neural network is a complex of distributed and parallel computing systems capable of adaptive learning by analyzing the positive and negative effects and simulating simple biological processes occurring in the human brain. The transformative element in such networks is an artificial neuron. (fig. 1) [21].

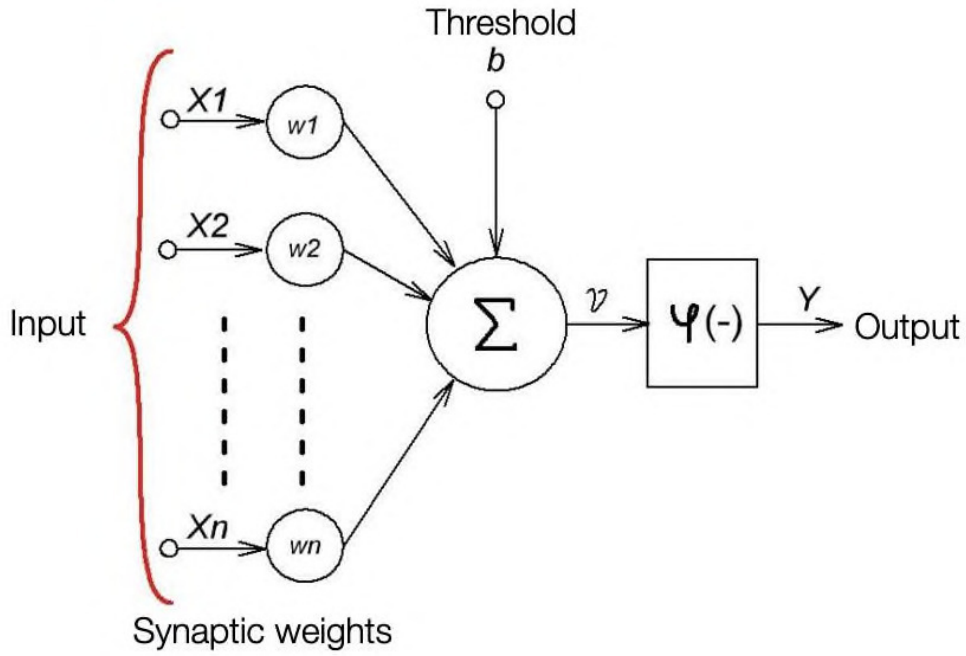

Fig. 1. Artificial neuron model

The functioning of the neuron is described by the following expressions:

$$v = \Sigma_{j=1}^{n} \omega_j x_j, \quad (1)$$

$$y = \varphi(v + b), \quad (2)$$

where xj – input signals;

ωj – synaptic weights;

φ (v+b) is an activation function that limits the amplitude of the output signal of the neuron;

b is the threshold element;

v is a linear combination of input actions;

y is the output of the neuron;

n is the number of inputs.

Our model trained 3400 random people from the Instagram dataset, 523 people from Facebook and 108 students using the security system. As it was mentioned - in order to make the training process easier, we obtain the data from different social network accounts. Images of new users are obtained from photoshoot once the owner requests access for a particular user using the smartphone and new users after using the security system.

It is common that the training data gained from the social media is insufficient for the deep learning model to perform accurately. Therefore as soon as the user is trained with a minimal dataset from the social media, the representation of the user is further improved by fine-tuning the model as the user starts using the system. Sometimes the face recognition system fails to classify the person properly and will have a very low accuracy, in such case system asks help from the administrator. Administrator is sent a request to label the person via his account. After the administrator has labeled, the system will automatically update with the new data and send back to the camera unit to grand the access or other words - authorize user. The test purposed authentication interface is also built in a website with library and an app SDK which can be easily integrated as a login system.

Necessary to mention that the Triplet-loss method mentioned in FaceNet for incremental learning is used by the system. The system has two processing units. The first one is from the camera (in test case represented by the common laptop web-camera). By using application SDK or website JS library for authentication camera is able and will detect and recognize the human face with the current model and data stored in memory in the first cloud server. Giving the access is based on if the system is able to detect and recognize the face with set-up confidence. If the confidence is low or unable to recognize the face, server will respond with refuse in authentication and moreover will take a series of user's photo with different angles and expression to upload in the second cloud server for training purpose. After the training task will be finished in the second cloud server, the updated version of the new model will be pushed to the first cloud server.

First cloud server unit aimed to store the face data and send notifications to the owner asking for labelling the unidentified or unrecognized person. Moreover the Facebook web-based application was built in the first cloud server, which collects the data from social media. Nevertheless the second cloud server will handle the much exhausted computational training tasks instead of first unit. By using the distributed TensorFlow, the model was trained in multiple computing nodes to speed up the training time and also using the incremental learning technique in FaceNet to retrain the model with new data collected from social networks and the security systems after specified time uses.

The largest possible problem of deep neural network is viable data. As we mentioned previously, public data to use for training purposes are very small. To compare with Google datasets mentioned in FaceNet paper, they use hundreds of millions of images from Google and Youtube. On the purpose of researching or business, you have to whether pay for a satisfying face dataset or manually collecting the data that will take a while, and the data will also be mostly unlabeled and therefore also insufficient. However, as soon as social media becomes more popular around the world, we proposed a novel method to automatically collect the data from social media. In this paper, we only mentioned Facebook and its child company Instagram since they are the largest social networks today, but actually, one can use this method in other social media networks. By using the graph API for developers, one can extract the tagged face from the users by giving the authentication access. It was also built and published an application on Facebook which is very convenient for all users around the world who can log-in and share their face images.

Firstly, model that has been tested was Face Recognition System model which trained by Instagram dataset on Labeled Faces in the Wild (LFW) datasets and the classification accuracy is 0.9318 ± 0.0140. The ROC of Face Recognition System model is shown in Figure 5 compared with Human and EigenFaces experiments. Unfortunately, the model was unable to reach the accuracy mentioned in the FaceNet paper since it was using much fewer input data to compare with billion photos from Google. Also different methods to preprocess the input data were tested. However, the accuracy is obviously impressed to compare with EigenFaces algorithm used in Jeffrey's and Shankar's security system. The state-of-art Inception-v3 model gave the outstanding result which closes the human gap.

Face authentication was also tested in a real environment by testing 50 people. The highest accuracy was 92.2%. Half of these people were presented as new customers trying to authenticate and as expected system notified for a label from the administrator. The datasets we used to train the neural network model is American, but 90% of test data is European. The result was lower accuracy to compare with LFW dataset and it sometimes failed to distinguish people. That makes collecting data from Social Network advantages because it is able to collect various, diverse people from around the world. The Face Recognition System authentication systems also confused between two people with similar faces, but more face images with different angles and expressions will solve the problem. The light condition is also important, the background should not be over illuminated.

The bottleneck values before training to distinguish different faces were stored. After collection of the data from 200 students and 500 users of Facebook, we knew model was trained with updated data using incremental learning. The result succeeded with improving AUC from 0.9823 to 0.9994. Also, system ability to recognize faces of Asians is increased because of social networks use and ability to updated the data with diverse images of people from different regions. It was not expected that the accuracy will dramatically increase because the collected data was insufficient and also bounded by the algorithm limitations. However, by using incremental learning approach, one can reach the accuracy mentioned in the FaceNet paper. Moreover one can additional improved the accuracy by using the Inception-v3 model. If one focus more on pre-processing the input data by aligning the data and using the TF-Slim libraries with the lightweight package for defining, training and evaluating models, one can even more improve the performance.

The entire system was developed and tested in a miniature informational license management system mimicking the actual one working on the production server. Authentication system was running on the laptop of the imaginary employee. It was constantly running faces detection, then asked server for verification. First and second cloud server are the stack cloud servers. Each of them includes 3 units: 1 controller unit and 2 compute units. Cloud server includes Ubuntu and CentOs operation environments and instances hosted by the QEMU hypervisor [20] on the compute units. The cloud server is able maximum to 8 VCPUs (time slot of the processor) with 32Gb Ram and 200Gb Root Disk. With highly computational power, the cloud server is suitable for neural network training and testing.

iOS app to alert to the owner/administrator via a smartphone was developed. Also was developed a web-based front end running from cloud server i, which is convenient to access anytime, anywhere from any device. Whenever someone tries to access authentication protected area of the licensing system, the new data will be updated in the app and on the website as well as therefore forwarded to the training server. Administrator will receive a notification with ability to label new user or decline / ban this user (face). Therefore administrator can label new users and the system will automatically retrain the classifier model with new users and give them access. As it was mentioned before one can collect the tagged faces with face locations and saved to cloud storage. Also one can assign permission level for different users which will protect privacy. For example, the user do not have access to control other user setting, and another user has no access to license creation tool.

Conclusion. This paper introduced a new method of obtaining data for training a security systems from social media and human interaction for future use in authentication process in various informational systems. There are several advantages of proposed system which can be described. First of all, one should mention that using of TensorFlow can be adaptive, powerful, and flexible. Moreover, training time is acceptable in comparison with other frameworks and much more faster if one uses distributed TensorFlow. The comparison results represented in Table 1.

Table 1

TensorFlow benchmarks

Library	Class	Time(ms)	Forward(ms)	Backward(ms)
Caffe	ConvLayer	1521	916	1088
Torch	cudnn.Spatial	430	156	1089
TensorFlow	conv2d	349	167	241

There is a range of abundant interesting projects which are leading in Artificial Intelligent and Deep Learning developed in TensorFlow with huge support from Google. In addition, computation in parallel mode will dramatically drop the training time. By using the method mentioned in the FaceNet paper, one can benefit in reaching a swiftness and accuracy comparing with other algorithms as in Table 2.

Table 2

Face recognition for authentication performance

Human , cropped	0.998
FaceNet	0.9983 ± 0.005
EigenFace	0.6162 ± 0.0092
Developed model	0.9718 ± 0.0124

More important, the accuracy has been improved along with use of new data from social media and human interaction. Second, collecting data from social media was also a great move since social media is the largest public data source such as Facebook with around 1.7 billion active users. With the publication of Facebook, one can easily collect the necessary data. One can also collect data from other social networks such as Instagram and many more. One interesting direction for future work is to collect the data from the owner's laptop or other devices such as captured photos and videos and therefore use them to train the network automatically. Another direction for future work is to detect fake-face by using gait speed and eye tracking and depth analysis.

References

1. M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin, et al. TensorFlow: Large-scale machine learning, 2016.

2. P. I. Wilson & J. Fernandez. Facial feature detection using haar classifiers, 2006.

3. R. J. Qian, M. I. Sezan, and K. E. Matthews. A robust real-time face tracking algorithm, 1998.

4. H. M. Do, C. Mouser, M. Liu, and W. Sheng. Humanrobot collaboration in a mobile visual sensor network, 2014.

5. W. Sheng, Y. Ou, D. Tran, E. Tadesse, M. Liu, and G. Yan. An integrated manual and autonomous driving framework based on driver drowsiness detection, 2013.

6. D. Tran, E. Tadesse, W. Sheng, Y. Sun, M. Liu, and S. Zhang. A driver assistance framework based on driver drowsiness detection, 2016.

7. Vivint Smart Home Security Systems. Smart home security solutions, 2016.

8. Protect America. Affordable home security systems for everyone, 2016.

9. K. Denmead. Netatmo is the weather station for the rest of us, 2013.

10. Jeffrey S Coffin and Darryl Ingram. Facial recognition system for security access and identification, 1999.

11. J. Shankar Kartik, K. Ram Kumar, and V.S. Srimadhavan. Security system with face recognition, sms alert and embedded network video monitoring terminal, 2013.

12. F. Schroff, D. Kalenichenko, and J. Philbin. FaceNet: A unified embedding for face recognition and clustering, 2015.

13. G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller. Labeled faces in the wild: A database for studying face recognition in unconstrained environments, 2007.

14. J. Kuzborskij, F. Orabona, and B. Caputo. From n to n+ 1: Multiclass transfer incremental learning, 2013.

15. J. Deng, W. Dong, R. Socher, Li-Jia Li, K. Li, and L. FeiFei. ImageNet: A large-scale hierarchical image database. In Computer Vision and Pattern Recognition, 2009.

16. Q. V. Le. Building high-level features using large scale unsupervised learning, 2013.

17. A. Krizhevsky, I. Sutskever, and G. E. Hinton. ImageNet classification with deep convolutional neural networks, 2012.

18. C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna. Rethinking the inception architecture for computer vision, 2015.

19. D. E. King. Dlib-ml: A machine learning toolkit, 2009.

20. F. Bellard. Qemu-open source processor emulator, 2016.

21. Kryvoruchko O., Khorolska K., Chubaevskyi V., Usage of neural networks in image recognition. (2019). Зовнішня торгівля: економіка, фінанси, право, 3, 83–92. DOI: 10.31617/zt.knute.2019(104)07

22. Reddy, N., Kulkarni, S., & Hariharan, S. (n.d.). Facial Image Based Mood Recognition Using Committee Neural Networks. Intelligent Engineering Systems through Artificial Neural Networks Volume 18, 277–284. DOI: 10.1115/1.802823.paper35.

УДК 004.8:67

Олена Криворучко, Богдан Бебешко, Карина Хорольська,
Альона Десятко, Наталія Котенко

ВИКОРИСТАННЯ СИСТЕМИ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ДЛЯ АВТОРИЗАЦІЇ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Актуальність теми дослідження. *Технічний прогрес веде до величезного збільшення числа кіберзлочинів. Майже кожна людина у світі має цифрові облікові записи, які містять конфіденційну особисту інформацію, яка насправді захищена простим паролем. Тому системи безпеки відіграють велику й важливу роль у захисті конфіденційності. Необхідно мати надійну систему, яка може розрізняти людей і діяти по-різному в залежності від їх прав.На відміну від аутентифікації по розпізнаванню обличчя та інших рішень для ідентифікації, таких як паролі, перевірка електронної пошти або ідентифікація за відбитками пальців, біометричний розпізнавання осіб використовує унікальні математичні та динамічні шаблони, які роблять таку систему однією з найбільш безпечних та ефективних.*

Постановка проблеми*. Аутентифікація з розпізнавання обличчя скоро стане однією з найстабільніших. Є методи, доступні для виявлення та обробки обличчя з використанням різних рівнів складності. Підводячи підсумки, можна стверджувати, що розпізнавання обличчя з метою аутентифікації може посилити безпеку. Згорткові нейронні мережі (CNN) перевершують будь-який можливий рівень розпізнавання людини. Однак такі системи повинні постійно поліпшуватися вручну. Інша проблема, пов'язана з такими системами, полягає в тому, що для їх підготовки повинен бути точно підготовка даних, перш ніж вони будуть розгорнуті. Дуже важливо, щоб система була досить швидкою, щоб розпізнавати людей, і щоб навчання проходило без особливих труднощів, а також швидко.*

Аналіз досліджень і публікацій. *Алгоритми розпізнавання обличчя були розглянуті в ряді наукових робіт, таких як каскади Хаара, фільтр Калмана і застосовані в різних сферах. Серед дослідницьких робіт є ряд систем безпеки, які використовують технологію розпізнавання осіб. Підхід розпізнавання осіб для безпечного доступу і аутентифікації, представлений Джеффрі С. Коффіна, використовує користувальницький метод VLSI Hardware і метод Eigenspaces. Системи, надані Shankar Kartik, також використовують метод Eigenfaces для ідентифікації обличчя, який фактично дає слабкі результати з помірною точністю.*

Виділення недосліджених частин загальної проблеми. *Швидкість окремих систем розпізнавання обличчя великою мірою залежить від змін умов освітлення, експресії, щільності камери й часткової блокування особи. Кілька наукових робіт вже запропонували певні підходи до розпізнавання обличчя в неприємних умовах, але насправді не багато з них працюють.*

Метою статті *є опис експериментальної архітектури системи аутентифікації системи розпізнавання обличчя всередині інформаційної системи, доступної через веб-інтерфейс. Система аутентифікації Face Recognition System складається з вузла камери, хмарного сервера і пристрої введення-виведення для взаємодії з користувачами за допомогою веб-інтерфейсу.*

У зв'язку з розвитком Інтернету і хмарних обчислень ця стаття являє собою розробку системи аутентифікації на основі системи розпізнавання осіб. Використовуючи систему Google наступного покоління, TensorFlow з платформою глибокого навчання на борту. TensorFlow – це гнучкий, стерпний проєкт із відкритим вихідним кодом.

Виклад основного матеріалу. *Як відомо, зір людського мозку здається дуже легко функціонуючим. Неважко розгледіти собаку й кішку, прочитати слово або дізнатися людське обличчя. Але на відміну від людини ці завдання дійсно складні для вирішення за допомогою комп'ютера. Процес розпізнавання здається простим, тому що людський мозок дійсно хороший у сприйнятті і, в результаті, в розумінні зображень. В останні роки машинне навчання домоглося великих успіхів у вирішенні цих складних завдань. Зокрема, модель, звана глибоко сверточное нейронною мережею, може привести до розумної продуктивності при вирішенні складних завдань візуального розпізнавання, які в деяких аспектах відповідають або перевершують можливості людини.*

Висновки відповідно до статті. *У цій статті представлено новий метод отримання даних для навчання систем безпеки з соціальних мереж і взаємодії з людиною для майбутнього використання в процесі аутентифікації в різних інформаційних системах. Існує кілька переваг пропонованої системи, які можна описати. Насамперед треба зазначити, що використання TensorFlow може бути адаптивним, потужним і гнучким. Більш того, час навчання прийнятно в порівнянні з іншими середовищами і набагато швидше, якщо використовувати розподілений TensorFlow.*

Ключові слова: *штучний інтелект; розпізнавання обличчя; нейронна мережа; інформаційні системи; аутентифікація.*

Рис.: 1. Табл.: 2. Библ.: 22.

Kryvoruchko Olena – Doctor of Technical Sciences, Professor, Head of the Department of Software Engineering and Information Systems, Kyiv National University of Trade and Economics (19 Kioto Str., 02156 Kyiv, Ukraine).
Криворучко Олена Володимирівна – доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет (вул. Кіото 19, м. Київ, 02156, Україна).
E-mail: kryvoruchko_ev@knute.edu.ua
ORCID: http://orcid.org//0000-0002-7661-9227

Bohdan Bebeshko – Senior Software Engineer, Softorino Ltd. (Marshall Islands, Ajeltake Road, Majuro, MH 9696, USA).
Бебешко Богдан Тарасович – Senior Software Engineer, Softorino Ltd. (Marshall Islands, Ajeltake Road, Majuro, MH 9696, USA).
E-mail: thismushroom@gmail.com
ORCID: https://orcid.org/0000-0001-6599-0808

Khorolska Karyna – assistant of the Department of Software Engineering and Information Systems, Kyiv National University of Trade and Economics (19 Kioto Str., 02156 Kyiv, Ukraine).
Хорольська Карина Вікторівна – асистент кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет (вул. Кіото 19, м. Київ, 02156, Україна).
E-mail: k.khorolska@knute.edu.ua
ORCID: https://orcid.org/0000-0003-3270-4494

Desiatko Alona – Senior Lecturer of the Department of Software Engineering and Information Systems, Kyiv National University of Trade and Economics (19 Kioto Str., 02156 Kyiv, Ukraine).
Десятко Альона Миколаївна – старший викладач кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет (вул. Кіото 19, м. Київ, 02156, Україна).
E-mail: desyatko@knute.edu.ua
ORCID: https://orcid.org/0000-0002-2284-3218

Kotenko Nataliia – PhD in Pedagogical Sciences, Senior Lecturer of the Department of Software Engineering and Information Systems, Kyiv National University of Trade and Economics (19 Kioto Str., 02156 Kyiv, Ukraine).
Котенко Наталія Олексіївна – кандидат педагогічних наук, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки, Київський національний торговельно-економічний університет (вул. Кіото 19, м. Київ, 02156, Україна).
E-mail: kotenko@ukr.net
ORCID: http://orcid.org/0000-0002-2675-6514

Kryvoruchko, O., Bebeshko, B., Khorolska, K., Desiatko, A., Kotenko, N. (2020). Artificial intelligence face recognition for authentication. *Technical Sciences and Technologies*, 2 (20), 139-148.