I. J. Computer Network and Information Security, **2021, 6, 1-12**
Published Online December 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2021.06.01

A Biometric Asymmetric Cryptosystem Software Module Based on Convolutional Neural Networks

Ilyenko Anna
National aviation university, Kyiv 03058, Ukraine
E-mail: ilyenko.a.v@nau.edu.ua

Ilyenko Sergii
National aviation university, Kyiv 03058, Ukraine
E-mail: ilyenko.s.s@nau.edu.ua

Herasymenko Marharyta
National aviation university, Kyiv 03058, Ukraine
E-mail: loadlemon@gmail.com

Received: 13 June 2021; Revised: 11 August 2021; Accepted: 21 October 2021; Published: 08 December 2021

Abstract: During the research, the analysis of the existing biometric cryptographic systems was carried out. Some methods that help to generate biometric features were considered and compared with a cryptographic key. For comparing compact vectors of biometric images and cryptographic keys, the following methods are analyzed: designing and training of bidirectional associative memory; designing and training of single-layer and multilayer neural networks. As a result of comparative analysis of algorithms for extracting primary biometric features and comparing the generated image to a private key within the proposed authentication system, it was found that deep convolutional networks and neural network bidirectional associative memory are the most effective approach to process the data. In the research, an approach based on the integration of a biometric system and a cryptographic module was proposed, which allows using of a generated secret cryptographic key based on a biometric sample as the output of a neural network. The RSA algorithm is chosen to generate a private cryptographic key by use of convolutional neural networks and Python libraries. The software authentication module is implemented based on the client-server architecture using various internal Python libraries. Such authentication system should be used in systems where the user data and his valuable information resources are stored or where the user can perform certain valuable operations for which a cryptographic key is required. Proposed software module based on convolutional neural networks will be a perfect tool for ensuring the confidentiality of information and for all information-communication systems, because protecting information system from unauthorized access is one of the most pressing problems. This approach as software module solves the problem of secure generating and storing the secret key and author propose combination of the convolutional neural network with bidirectional associative memory, which is used to recognize the biometric sample, generate the image, and match it with a cryptographic key. The use of this software approach allows today to reduce the probability of errors of the first and second kind in authentication system and absolute number of errors was minimized by an average of 1,5 times. The proportion of correctly recognized images by the comparating together convolutional networks and neural network bidirectional associative memory in the authentication software module increased to 96,97%, which is on average from 1,08 times up to 1,01 times The authors further plan a number of scientific and technical solutions to develop and implement effective methods, tools to meet the requirements, principles and approaches to cybersecurity and cryptosystems for provide integrity and confidentiality of information in experimental computer systems and networks.

Index Terms: Convolutional neural network, Biometric cryptographic systems, Biometric features, Secret key, Authentication.

1. Introduction

One of the most necessary areas of information technology development is information security. Nowadays, the task of creating and using new means of protection in information systems has become very important.

Neurocryptography is a branch of cryptography that studies the use of stochastic algorithms, including neural networks, for encryption and cryptanalysis. Neural networks help solve public key cryptography, key allocation, hashing, and pseudo-random number generation. An artificial neural network is an effective way of parallel processing. This feature of Artificial Neural Networks allows it to be used in the future for a wide range of tasks, but often the complexity of implementing such a system nullifies its practical applicability. The architecture of artificial neural networks can effectively perform the work of pattern recognition and classification of a set of objects on any basis. In addition, due to a well-thought-out algorithm, trained neural networks can achieve extremely high levels of accuracy. These benefits allow the efficient use of artificial neural networks in authentication informstion systems. It can also be used where continuous key generation is required, or to speed up the key exchange process. Authentication is a procedure for verifying the authenticity of data, without which protected information may be compromised. Biometric cryptographic systems are a promising direction in the development of authentication systems. The main efforts in this direction are aimed at the development and improvement of hardware and software that would achieve a simultaneous and significant reduction in the level of errors of the first and second kind, as well as would be protected from threats.

Biometric methods in cryptographic systems in the initial stages were used to protect against unauthorized access. Currently, there are two main areas of application of biometric methods: solving the problem of user authentication and their integration with cryptographic systems. One of the disadvantages of cryptographic systems is the need to ensure secure storage, transfer and management of cryptographic keys. A promising direction to increase the efficiency of authentication systems is the integration of biometric and cryptographic methods with using of neural networks.

Today, when considering biometric authentication procedures, neural networks are increasingly used to process and verify a biometric sample. Biometric samples due to the development of computing capabilities now need to be used as either a secret key (symmetric cipher) or a password or key pair (asymmetric cipher), which means that biometric is relevant to use as a secret information for cryptographic transformations to ensure the confidentiality of information [1-3]. Thus, there is a problem of finding new methods of building secure information systems of cryptographic systems - is the development and implementation of a combination of biometric authentication systems and cryptographic security systems using neural networks. This is a relatively new approach to building information security systems based on ensuring the integrity and confidentiality of information. This approach is aimed at counteracting unauthorized access to the information system and preventing the forgery of biometric samples through the use of cryptographic transformations of biometric data into a cryptographic key and their storage in encrypted form in the database of information system users.

The purpose of this article is to analyze existing biometric cryptographic systems using neural networks and develop an author's advanced approach, which is based on the integration of biometric system and cryptographic module, which allows to use as a neural network output generated on the basis of biometric sample secret cryptographic key. Based on the purpose, the task of this scientific article: 1) to study the existing biometric cryptographic systems using neural networks and to form a requirement for own software module; 2) to develop an authentication algorithm using the neural network conversion of a biometric sample into a cryptographic key; 3) to develop a software implementation of the authentication module using the neural network conversion of a biometric sample into a cryptographic key using the Python programming language; 4) to test and expediency of use of the developed software module. In this paper, the biometric sample is based on the parameters of the user's face, which as a result of using a neural network allows it to be transformed into a cryptographic key and then used to create on its base public key to build an asymmetric cryptographic system.

The paper proposes an approach based on the integration of a biometric system and a cryptographic module, which allows the use of a secret cryptographic key generated on the basis of a biometric sample as a neural network output by combining convolutional neural network withbidirectional associative memory. This approach solves the problem of secure storage of the secret key. The practical value lies in the creation of an advanced algorithm and software module for biometric authentication using neural networks, which allow to determine with high accuracy the level of coincidence of the input sample with the reference and reduce the level of erroneous operation by using Python libraries. The developed algorithm and software module can be used for any applications or systems that provide authentication and have access to the camera. This approach allows solving the problem of information protection, including stored information, processed and transmitted in modern information networks on the basis of confidentiality.

2. Related Work

Biometric cryptosystems require the storage of public information that depends on biometrics. This information is used to obtain or generate keys and is called helper data [1,2,4]. In paper [5] authors discover three types of biometric cryptosystems, depending on how the auxiliary data is obtained: key release cryptosystems; key binding cryptosystems; key generation cryptosystems.In key release cryptosystems, the cryptographic key is considered secret, and biometric data is used as a key to protect a randomly generated cryptographic key. In key binding systems, auxiliary data is obtained by binding the selected key to a biometric template. In systems with key generation, auxiliary data is obtained only from a biometric template. The keys are generated directly from the auxiliary and this biometric sample. [1,4-7]. The efficiency of the system of biometric cryptosystems is mostly assessed in terms of the coefficient of erroneous deviation and erroneous acceptance. Most biometric cryptosystems are designed to bind or generate keys long enough to be used in a common cryptographic system. To prevent the selection of biometric keys or brute force, they must be of sufficient size and entropy.The second factor that affects the security of biometric cryptosystems is the leakage of confidentiality. Ideally, privacy leaks should be minimized (for a given key length) to avoid fraud with personal data. Key size and privacy leak requirements define a fundamental trade-off in biometric cryptosystem approaches that is rarely evaluated [4,5]. Since both the metrics and the key entropy depend on the allowable levels in the comparison, these three values are very interrelated.

Thus, biometric systems need to be improved by creating integrated systems that take into account several sources of biometric images by using neural networks. Also, it is necessary to use methods that unambiguously identify the pair "biometric image" - "cryptographic key". For the effective recognition of biometric samples, artificial neural networks are often used, which allow to determine with high accuracy the level of coincidence of the input sample with the reference and to reduce the level of false positives [8-11]. A prerequisite for the use of neural networks as a mathematical basis for the creation of new methods of cryptographic protection of information may be their ability to recover distorted signals and recognize objects that have characteristics different from the reference. Biometric authentication systems based on the use of artificial intelligence technologies in most cases approximate the nonlinear functional mapping, allow to assign the recognized biometric image to one of the predefined classes [4,5,12]. The classical algorithm for biometric cryptosystems by using neural network can be divided into five conditional stages in developing the structure of the authentication system with neural network conversion of biometric features input into a cryptographic private key: pre-processing of features; generation of features; creating a biometric samples; comparison images and keys of neural network; key recovery [12-24]. The task of the block of preliminary processing of signs consists in unification of the image of the person of the person and construction of the primary vertor of signs. The key recovery unit is required to transform a compact feature vector into the desired user key. It is worthwhile to say that the system creates a random key that is not used in the system if unauthorized entry is attempted.The generation of features is the projection of the primary vector into a new feature space and the formation of a compact feature vector of each image for further neural network processing. This vector is fed to the neural network block in the form of a binary vector or in the form of an integer vector, which, in turn, generates a private key supplied to the input of the cryptographic system module. This vector is fed to the neural network block in the form of a binary vector or in the form of an integer vector, which, in turn, generates a private key supplied to the input of the cryptographic system module.

Before proceeding to consider the types of neural networks and their possibilities for use in combined systems, consider the mathematical model of the neuron. The mathematical model of the neuron converts the input elements into output using the adder function and the activation function:

- input signals $x_1, x_2, \ldots, x_n$ are data coming from the environment or from other active neurons. Input levels can be discrete from sets [0, 1] or [-1, 1] or take any real values;
- weights $w_1, w_2, \ldots, w_n$ – determine the strength of the connection between neurons;
- b-bias;
- summative function $\sum_{i=1}^{n} w_i \cdot x_i + b$;
- activation function (1) - used to calculate the output value of the signal transmitted to other neurons:

$$Y = f\left(\sum_{i=1}^{n} w_i \cdot x_i + b\right) \tag{1}$$

One of the stages in the development of a neural network is the choice of the activation function of neurons. The type of activation function largely determines the functionality of the neural network and the method of its training.

The activation function is a way to normalize the input data. That is, if there is a large amount of data at the input, then passing them through the activation function, the output will get the desired range.

Linear activation function (2) – a function that translates each element of the definition set into itself:

$$f(x) = x, x \in (-\infty; +\infty) \tag{2}$$

Perceptron activation function (3). Perceptron is one of the first models of neural networks. The activation function of the perceptron has a somewhat similar graph to the Heaviside function. In general, the activation function of the perceptron is a comparison of the adder function with zero:

$$f(x)=\begin{cases}0, x<0\\1, x\geq 0\end{cases}, x\in(0;1) \tag{3}$$

The logistic function or sigmoid (4) is a continuously differentiated monotonic nonlinear S-shaped function that is often used to "smooth" the values of a quantity:

$$f(x)=\frac{1}{1+e^{-x}}, x\in(0;1) \tag{4}$$

Rectified linear unit is the most popular artificial neuron for 2018. He replaced the sigmoid. ReLU has proven itself much better than sigmoids in deep learning (deep learning)

$$f(x)=\begin{cases}0, x<0\\x, x\geq 0\end{cases}, x\in[0,+\infty) \tag{5}$$

Hyperbolic tangent. It makes sense to use the hyperbolic tangent only when the values can be both negative and positive, since the range of the function [-1, 1].

$$f(x)=\tanh(x)=\frac{e^{x}-e^{-x}}{e^{x}+e^{-x}}, x\in[0;1] \tag{6}$$

Despite the fact that the activation function neuron the hyperbolic tangent is resource-intensive when deploying a neural network, but it is advisable to use it when the values can be both negative and positive and provide faster convergence than the standard logistics function. Therefore, the authors of the work for the implementation of the neural network decided to choose the activation function of the hyperbolic tangent type

It is suggested to use the following approaches to generate signs by biometric cryptosystems by using neural network: Kohonen two-dimensional self-organization map (SOM) [11,17,18,25,26]; probabilistic principal component analysis (PPCA) [27,28]; convolutional neural network (CNN) [29-32]. In case, a user should be added to the system, a compact feature vector is fed to the input of the biometric image creation unit, where the neural network comparison of the private key and the input vector is performed. For comparing compact vectors of biometric images and cryptographic keys, the following methods are analyzed: designing and training of bidirectional associative memory (BAM) [17,18,33,24]; designing and training of single-layer and multilayer neural networks of direct propagation based on perceptrons (MLP) [9-11,25,26,34].

As a result of comparative analysis of algorithms for extracting primary biometric features and comparing the generated image to a private key within the proposed authentication system, it was found that CNN combined with BAM will give the best result during the authentication procedure and will be able to counteract unauthorized access and will be used in proposed software module of authentication.

The authors also conducted a theoretical study of asymmetric cryptographic systems with the possibility of their integration into a biometric cryptographic system. An asymmetric cryptographic system was chosen as the basis for the implementation of the cryptographic system with biometric systems in order to ensure the secret storage of the cryptographic key and conduct a correct authentication procedure. Today cryptographic systems provide secure communication between users. In the present paper we describe existing cryptographic systems such as: systems based on the complexity of factorization of a large integer (RSA); systems based on the complexity of solving a discrete logarithm in finite Galois field (EIGamal, DSA); systems based on the complexity of solving a discrete logarithm in a group of points of an elliptic curve (ECC); lattice-based systems (NTRU). The authors in their work to present biometric samples in the form focused on the RSA algorithm, as it is easy to implement and has wide application in modern information systems and networks.The RSA public key cryptosystem guarantees the integrity and confidentiality of information when transmitting, storing and processing information messages in modern computer systems and networks [35-38].

3. Proposed Software Module of Authentication

The purpose of research is to create a reliable authentication system using neural network conversion of a biometric sample into a cryptographic key. This approach will solve the problem of saving and further use of the cryptographic key by conducting the correct procedure of key generation and authentication based on neural networks.

Functional requirements:

1. At the first time visiting website, the user should be able to sign in to the system if he does not already have an account;
2. The registered user, who have a previously given permission to use the webcam to obtain a biometric sample, has the opportunity to log in;
3. After providing the biometric sample to the user, a message, containing information about the success of the authentication attempt, is displayed (success or failure).

System requirements: the software module is developed in the form of a web page that can be opened in any modern browser. You can also view the page from mobile devices and tablets. The following software development tools were selected to implement the authentication software module: 1) development environment – Visual Studio Code; 2) server-side programming language: Python; 3) eco-system for user interface development (front-end): Angular 7, HTML 5, SCSS, Bootstrap; 4) Database: PostgreSQL – a relative database that has many built-in capabilities and supports complex structures; is also pays considerable attention to maintaining the integrity of data in tables.The architecture type of the software module is client-server because this module is designed for Internet resources.

The cases described above that may occur in the system are shown in the Use case diagram constructed by UML (Fig. 1).

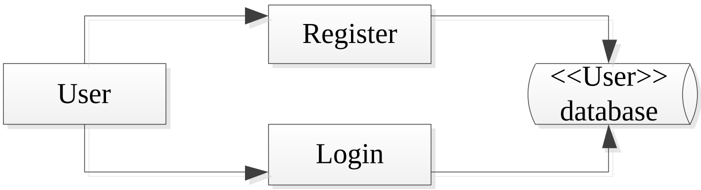

Fig.1. Use case diagram

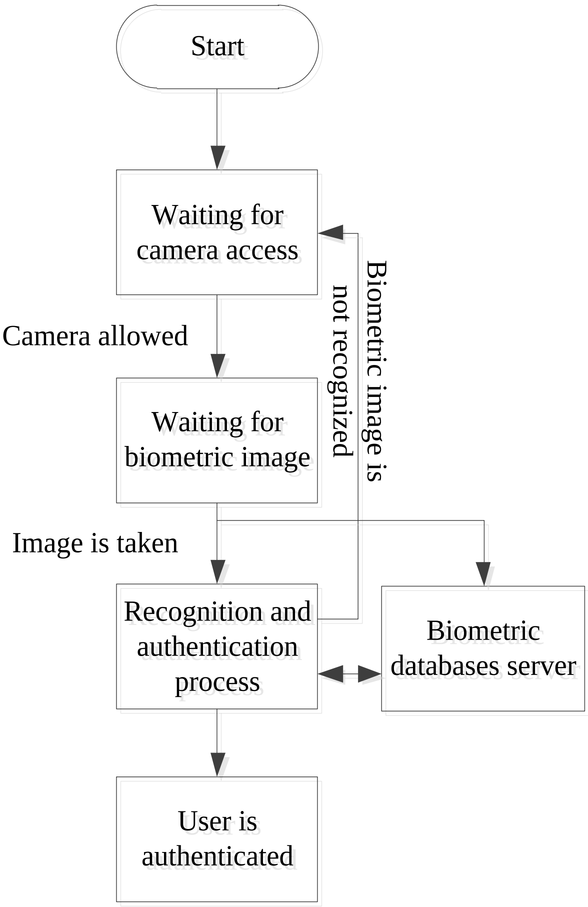
Start
Waiting for camera access
Camera allowed
Waiting for biometric image
Biometric image is not recognized
Image is taken
Recognition and authentication process
Biometric databases server
User is authenticated

Fig.2. State diagram of software module of authentication

Possible states in the system are depicted in the UML stateChart diagram (See Figure 2). Explanation of the stateChart chart: 1) After visiting the home page the user is offered to sign or log in. 2) The system requests permission to use the webcam to obtain a biometric sample. 3) If access to the camera is provided, the system performs the recognition and authentication process. 4) In case of successful authentication, the user enters the system and receives a message.

Creating a new account: 1) User enters his data (in this case – username). 2)System shows the user a request to use the camera. 3) If permission is not granted, step 2 repeats. 4)The user takes a picture. 5)The system adds a biometric sample of the user to the database. 6) The system shows the user a message about successful registration.

If the user wants to log in to an existing account: 1) The system shows the user a request to use the camera. 2) If permission is not granted, paragraph 1 repeats.3) The user takes a picture. 4) The system recognizes the user by existing biometric samples in the database. 5) If the user was not recognized – return to step 3. 6) The system shows a user a message about successful login. An unauthorized user has 2 choices: sign in to an existing account or create a new one.

3.1. Description of the software module algorithm

Proposed software module consist of five stages: features pre-processing, feature generation. creating a database of biometric samples, neural network mapping of images and keys, key recovery (fig. 3.). Next, we consider in detail each of the stages and features of their implementation.

Features Pre-Processing. The primary task of features pre-processing is to select the area of interest, i.e. the person for whom we perform authentication. Also, the image should be normalized, scaled, and grayed out to increase the speed. To perform these tasks the OpenCV library was chosen.

OpenCV is an open source library for analyzing, classifying, and processing images. Widely used in languages such as C, C ++, Python and Java.

The process of pre-processing the images is:

```
def faceCrop(pil_im):
   boxScale=1
   faceCascade = cv.Load('haarcascade_frontalface_alt.xml')
   cv_im=pil2cvGrey(pil_im)
      face=DetectFace(cv_im,faceCascade)
      if face:
         croppedImage=imgCrop(pil_im, face[0],boxScale=boxScale)
      else:
         print 'No faces found:', img
```

Here, pil_im is input image, cv_im – image converted to black and white color scheme, faceCascade – prefabricated template used for recognition, face_im – a sequence of rectangular areas returned after recognition, croppedImage – target image.

A method that converts a PIL image into a black and white CV image:

```
def pil2cvGrey(pil_im):
   pil_im = pil_im.convert('L')
   cv_im = cv.CreateImageHeader(pil_im.size, cv.IPL_DEPTH_8U, 1)
   cv.SetData(cv_im, pil_im.tostring(), pil_im.size[0]  )
   return cv_im
```

The method for face recognition is described below. It takes a gray image at the input and highlights the face in this image according to the patterns specified in haarcascade.

```
def DetectFace(image, faceCascade):
   min_size = (20,20)
   haar_scale = 1.1
   min_neighbors = 3
   haar_flags = 0
   cv.EqualizeHist(image, image)
   face = cv.HaarDetectObjects(
         image, faceCascade, cv.CreateMemStorage(0),
         haar_scale, min_neighbors, haar_flags, min_size
      )
    return face
```

The method of histogram alignment was used (cv.EqualizeHist) to increase the contrast of the image and expand the range of intensity.

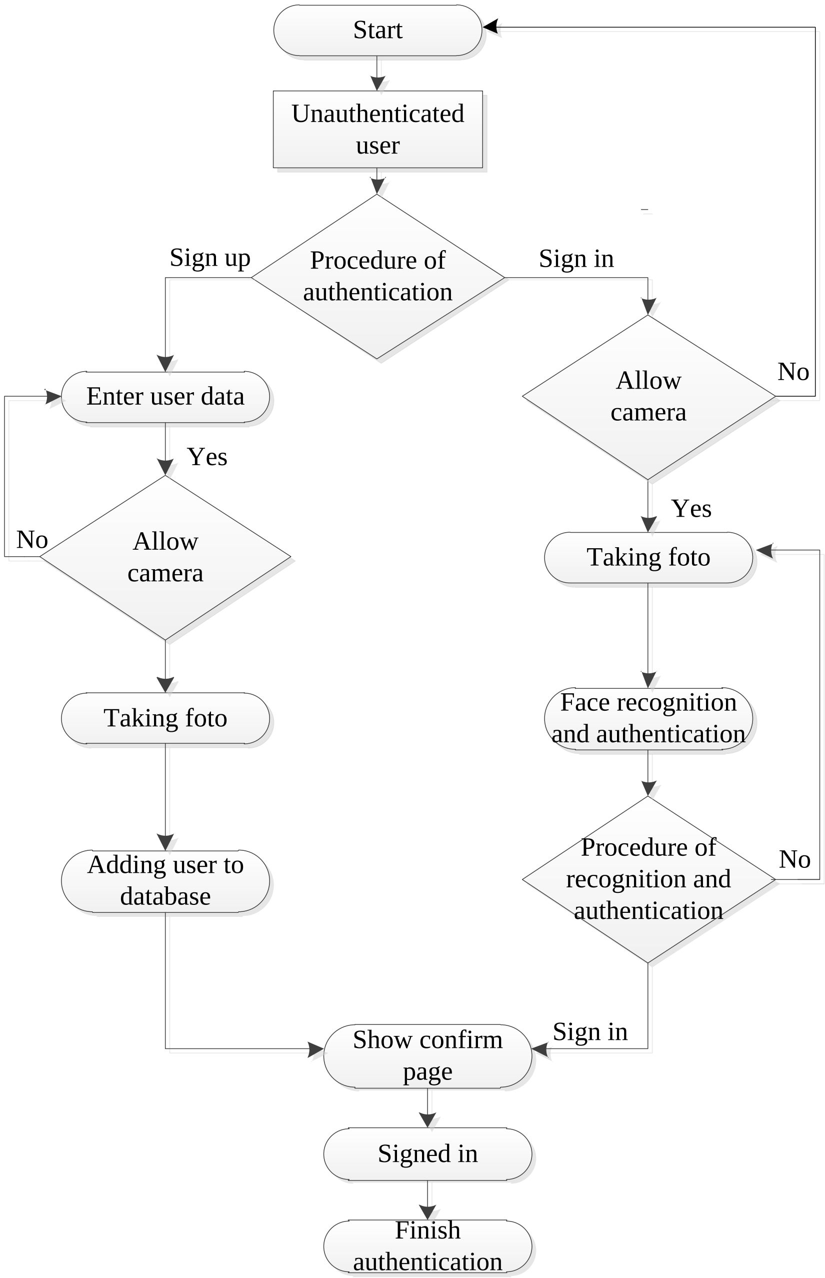

Fig.3. Diagram of activities for proposed software module of authentication

The cv.HaarDetectObjects function finds rectangular areas in this image that may contain faces and returns these areas as a sequence of rectangles.

Feature Generation. The approach of using the convolution network was chosen to generate biometric features.

Implementation begins with the import of the following libraries:

1. TensorFlow: An open source platform for the implementation, training and deployment of machine learning models.
2. Keras: An open source library used to implement neural network architectures running on both CPUs and GPUs.
3. Matplotlib: Python visualization tool used to illustrate interactive diagrams and images.

The network is trained on a pre-prepared data set. To reference image class names during the rendering phase, the list containing the classes is initialized with the name of the CLASS_NAMES variable: CLASS_NAMES= ['face', 'other']. The data set is divided into 50,000 training data and 10,000 test data. The last section of the dataset we need is validation data. Validation data is taken from the last 5,000 images in the training data.

validation_images, validation_labels = train_images[:5000], train_labels[:5000]

```
train_images, train_labels = train_images[5000:], train_labels[5000:]
```

TensorFlow provides a set of functions and operations that allow easily process and modify data using a specific input pipeline. To access these methods and procedures, data set should be into an efficient representation of the data that TensorFlow is familiar with. This is achieved using the tf.data.Dataset API.

Along with a brief description here are the types of layers which the CNN architecture consists of: 1) convolutional layer; 2) packet normalization layer; 3) maxpooling layer; 4) smoothing layer; 5) dense layer.

There are some other operations and methods used in CNN that are worth mentioning: 1) activation function; 2) rectified linear unit activation function (ReLU); 3) Softmax Activation Function; 4) prolapse.

Creating a Database of Biometric Samples. If a new user registers in the system, system must first add this user and his biometric data to the database. The needed data is the username and image. In addition, using the Crypto.PublicKey library, a private RSA key for the user is generated from biometric sample.

As a biometric sample for the experiment, a photograph from the camera was taken during the identification procedure with a size of 640*480 in the ratio 4:3. This biometric sample is then converted into a cryptographic key using an asymmetric cryptographic algorithm and stored in the server database. A person who is identified and authorized in the system can use the key, both to authenticate any actions on the system and to carry out procedures for encryption and formation / verification of electronic digital signature. This approach is multi-tasking and solves the issue of secret storage and combating cryptographic key compromise.

RSA is the most common and widely used public key algorithm. Its security is based on the difficulty of decomposing large integers. The algorithm can be used for both confidentiality (encryption) and authentication (digital signature). It is worth to note that signing and decryption are much slower than verification and encryption. The cryptographic force is mainly related to the length of n module. 1024 bits are considered as a sufficient length for encryption secret information.

```
from Crypto.PublicKey import RSA
def generateKey(compactVector):
key = RSA.generate(1024)
privatekey = key.exportKey(passphrase=compactvector, pkcs=8)
publickey = key.publickey().exportKey()
return privatekey, publickey
```

User data is stored in a database. To do this, the psycopg2 library is used. Psycopg is the most popular PostgreSQL database adapter for the Python programming language. Its main features are the full implementation of the Python DB API 2.0 specification and thread security (multiple threads can have a common connection). It was designed for multithreaded applications that create and destroy multiple cursors and make a large number of simultaneous INSERT or UPDATE.

Key Recovery. In case, the system finds a user who has a matching biometric sample, it returns the key generated for that user. Otherwise – generate a random RSA key and return it. With this key, the system will not be able to perform any actions.

```
from Crypto.PublicKey import RSA
def getUserKey(user):
  if (user)
    return user.getKey()
  else
    return RSA.generate(1024)
```

The user.getKey () method does not take the key from the database but generates it again, based on the compact vector of the biometric sample stored in the database, which belongs to the user. In general the interface part of the program contains three main pages: main.html (home page), signup.html (registration page), login.html (login page). On the main page, two links are placed: to the registration page and the login page, respectively. The registration page contains a form, where the user enters the username, and a continue button, when after clicking a modal window appears in which you can take a photo and confirm registration.

This script contains 3 functions:

1) gotoSnapshot is a function that activates when you press the Continue button and hides the block with the input field and instead shows the user the block for taking a photo.

2) takesnapshot is a function that takes a picture of the face. It is activated after pressing the Take snapshot button.

3) registerUser is a function that sends data received from the user to the server and processes the response. If the

answer has a status “200”, it displays a message to the user about successful registration, otherwise – shows an error.

A script that takes a photo and sends a request with user data to the server and processes the response:

The login page contains a block where you can take a photo, and as soon as the user takes a photo, a request is sent to the server. Applied styles to the login page are identical to those ones, which are applied to the login page, but do not contain input field settings. A script that takes a photo and sends a request with user data to the server and processes the response.

This script contains 3 functions:

1) takesnapshot is a function that takes a picture of the face. It is activated after pressing the Take snapshot button.

2) loginUser is a function that sends data received from the user to the server and processes the response. If the answer has a status “200”, it displays a message to the user about successful registration, otherwise – shows an error.

Thus, the proposed software module differs from existing approaches in that it combines the procedure of both authentication and the procedure of generating a cryptographic key based on the use of biometric images presented as a photo of the user when accessing the information system. The main feature of the software module is the use of the stages creating a database of biometric samples and neural network mapping of images and keys on the basis of special libraries of the Python programming language. database of biometric samples. Special is that biometric samples for authorized users are stored in the database of the information system not in the open, but also additionally hashed using the algorithm SHA-256. This allows you to further provide a procedure for storing identifying information. Next, we consider the process of evaluating the effectiveness of the implementation of the authentication procedure in combination with cryptographic transformations based on neural networks.

4. Performance evaluation and prospects for the practical implementation

To evaluate the effectiveness of the implementation of the authentication software module, we conducted an experiment in which different methods of generating biometric images and their comparison with a cryptographic key were compared. As a result of comparative analysis of algorithms for extracting primary biometric features and comparing the generated image with a private key within the proposed authentication system, it was found that the most effective test data are the approach using deep convolutional networks and neural network bidirectional associative memory. The procedure of testing the software module was performed on a PC with the following technical characteristics: processor - Intel (R) Core ™ i7-6700HQ 2.60GHz; installed RAM - 8.00 GB; GPU video card - NVIDIA GTX960M; system type - 64-bit operating system; operating system - Windows 10 Pro.

The main parameters of the experiment include the following: 1) original image – JPEG image obtained from the user's camera size 640 * 480 in the ratio 4: 3; 2) type of neural network – a combination of convolutional network and bidirectional associative memory; 3) the activation function of the hyperbolic tangent type; 4) symmetric threshold activation function. Note that all the percentage distribution of all samples was as follows: the training sample was 10%, and the test - 90%. The use of this software approach allows today to reduce the probability of errors of the first and second kind in authentication system and absolute number of errors was minimized by an average of 1,5 times (fig.4).

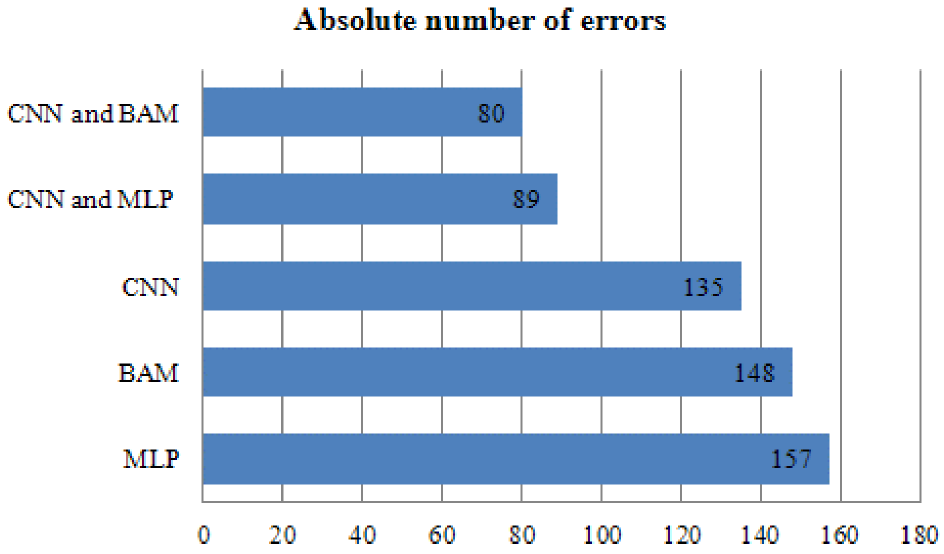

Fig.4. Absolute number of errors for different kinds of neural network

The use of associative memory, based on the BAM neural network, showed good results of comparison and the the capacity of such a network allowed to increase to 1500 samples. The proportion of correctly recognized images by the comparating together convolutional networks and neural network bidirectional associative memory in the authentication software module increased to 96,97 %, which is on average from 1,08 times up to 1,01 times (fig.5).

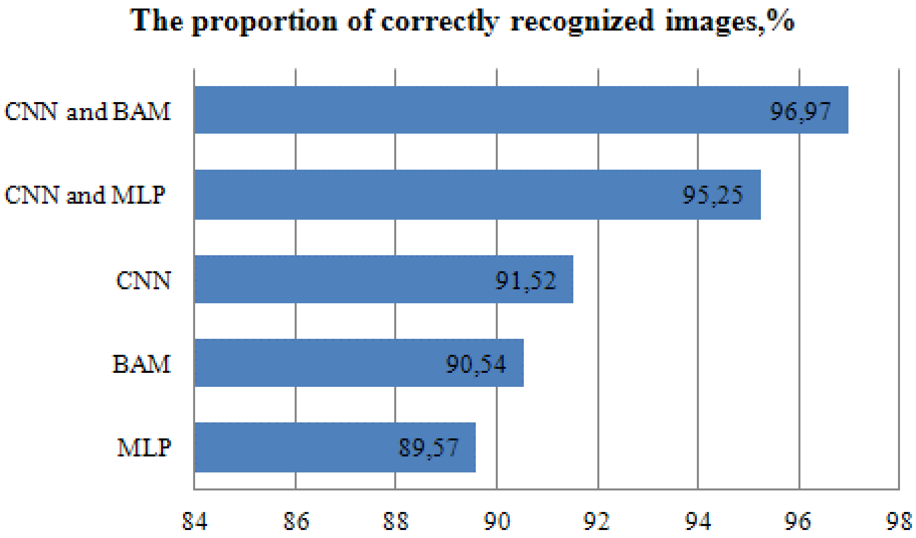

Fig.5. Proportion of correctly recognized images for different kinds of neural network

5. Conclusion

As a result of the research, an algorithm was developed and a software module of biometric authentication was implemented using the neural network conversion of a biometric sample into a cryptographic key. Author’s propose an approach based on the integration of a biometric system and a cryptographic module by using neural networks, namely the convolutional network and bidirectional associative memory, to recognize the biometric sample, generate the image, and match it with a cryptographic key. The practical significance of the proposed software module is to create a biometric authentication algorithm using neural networks, which allow to determine with high accuracy the level of coincidence of the input sample with the reference and reduce the level of erroneous work using Python libraries.The software authentication module is implemented based on the client-server architecture. The server part is implemented using various internal Python libraries (TensorFlow and Keras), which greatly simplify the construction and training of neural networks. The TensorFlow libraries (an open source platform for implementing, learning, and deploying machine learning models) and Keras (an open source library used to implement neural network architectures running on both core and GPUs). The RSA algorithm is chosen to generate a private cryptographic key. The following stack of tools was used for software implementation: Python –server part; PostrgeSQL – database; psycopg2 for database queries; Angular 7, HTML 5, SCSS – for the client side. Such authentication system should be used in systems where the user data and his valuable information resources are stored or where the user can perform certain valuable operations for which a cryptographic key is required. In the research, an approach based on the integration of a biometric system and a cryptographic module was proposed, which allows using of a generated secret cryptographic key based on a biometric sample as the output of a neural network.

The proposed sortware module allows at first to reduce the probability of errors of the first and second kind in authentication system and absolute number of errors was minimized by an average of 1,5 time; second increase to 96,97 % the proportion of correctly recognized images by the comparating together convolutional networks and neural network bidirectional associative memory and third solve the problem of secure storing the secret key. As a result of using this approach of converting biometric characteristics into a cryptographic key, the issue of interception and unauthorized use of the key during its transmission over an open communication channel is removed and the proper level of confidentiality of both the cryptographic key and the entire information system is provided. Such authentication system should be used in systems where the user data and his valuable information resources are stored or where the user can perform certain valuable operations for which a cryptographic key is required. On the basis of the conducted researches the authors have selected further perspective directions of improvement of the given algorithm of combination of biometric and cryptographic systems on the basis of neural networks, namely at first neural networks should be taught to distinguish a real user from a fabricated one, which will provide protection against imitation of a legitimate user and second it is possible to save not only the image of your face as a biometric sample but also a certain gesture or facial expression, thus, increasing the reliability of the system. This software module can be further integrated into websites, mobile and desktop applications, as well as any other systems that require user authentication and have access to the webcamera. In the future, the authors plan to expand the possibilities of using not only the RSA algorithm, but also faster encryption and cryptographic key generation based on the use of elliptic curves.

References

[1] Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. Proceedings of the IEEE, 92(6), 948-960.

[2] Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP Journal on advances in signal processing, 2008, 1-17.

[3] Jain, A. K., Ross, A., & Uludag, U. (2005, September). Biometric template security: Challenges and solutions. In 2005 13th European signal processing conference (pp. 1-4). IEEE.

[4] Biometrics: definition, use cases and latest news. [Online]. – Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[5] Maček, N., Franc, I., Gnjatović, M., Trenkić, B., Bogdanoski, M., & Aleksić, A. Biometric Cryptosystems–Approaches to Biometric Key-Binding and Key-Generation. Univerzitet Metropolitan Beograd 20. oktobar 2018. godine, 16.

[6] Juels, A., & Wattenberg, M. (1999, November). A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security (pp. 28-36).

[7] Bodo, A. (1994). Method for producing a digital signature with aid of a biometric feature. German patent DE, 42(43), 908.

[8] Nandakumar, K., Jain, A. K., & Pankanti, S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. IEEE transactions on information forensics and security, 2(4), 744-757.

[9] Gu, J., Wang, Z., Kuen, J., Ma, L., Shahroudy, A., Shuai, B., & Chen, T. (2018). Recent advances in convolutional neural networks. Pattern Recognition, 77, 354-377.

[10] Montavon, G., Samek, W., & Müller, K. R. (2018). Methods for interpreting and understanding deep neural networks. Digital Signal Processing, 73, 1-15.

[11] Minhas, R. A., Javed, A., Irtaza, A., Mahmood, M. T., & Joo, Y. B. (2019). Shot classification of field sports videos using AlexNet Convolutional Neural Network. Applied Sciences, 9(3), 483.

[12] Ding, S., Li, H., Su, C., Yu, J., & Jin, F. (2013). Evolutionary artificial neural networks: a review. Artificial Intelligence Review, 39(3), 251-260.

[13] Dodis, Y., Katz, J., Reyzin, L., & Smith, A. (2006, August). Robust fuzzy extractors and authenticated key agreement from close secrets. In Annual International Cryptology Conference (pp. 232-250). Springer, Berlin, Heidelberg.

[14] Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., & Smith, A. (2005, May). Secure remote authentication using biometric data. In annual international conference on the theory and applications of cryptographic techniques (pp. 147-163). Springer, Berlin, Heidelberg.

[15] Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In Annual international conference on the theory and applications of cryptographic techniques (pp. 457-473). Springer, Berlin, Heidelberg.

[16] Baek, J., Susilo, W., & Zhou, J. (2007, March). New constructions of fuzzy identity-based encryption. In Proceedings of the 2nd ACM symposium on Information, computer and communications security (pp. 368-370).

[17] Vihar Kurama, Samhita Alla, Rohith Vishnu K, " Image Semantic Segmentation Using Deep Learning", International Journal of Image, Graphics and Signal Processing, Vol.10, No.12, pp. 1-10, 2018.

[18] Priya Gupta, Nidhi Saxena, Meetika Sharma, Jagriti Tripathi,"Deep Neural Network for Human Face Recognition", International Journal of Engineering and Manufacturing, Vol.8, No.1, pp.63-71, 2018.

[19] Kalid A.Smadi, Takialddin Al Smadi,"Automatic System Recognition of License Plates using Neural Networks", International Journal of Engineering and Manufacturing, Vol.7, No.4, pp.26-35, 2017.

[20] Safiia Mohammed, Michael Hegarty,"Evaluation of Voice & Ear Biometrics Authentication System", International Journal of Education and Management Engineering, Vol.7, No.4, pp.29-40, 2017.

[21] Vanaja Roselin.E.Chirchi, Laxman.M.Waghmare,"Iris Biometric Authentication used for Security Systems", International Journal of Image, Graphics and Signal Processing, vol.6, no.9, pp.54-60, 2014.

[22] Jyoti Malik,Dhiraj Girdhar,Ratna Dahiya,G. Sainarayanan, "Reference Threshold Calculation for Biometric Authentication", International Journal of Image, Graphics and Signal Processing, vol.6, no.2, pp.46-53, 2014.

[23] K.Usha, M.Ezhilarasan,"A Hybrid Model for Biometric Authentication using Finger Back Knuckle Surface based on Angular Geometric Analysis", International Journal of Image, Graphics and Signal Processing, vol.5, no.10, pp.45-54, 2013.

[24] Anouar Ben Khalifa,Najoua Essoukri BenAmara,"Contribution to the Fusion of Biometric Modalities by the Choquet Integral", International Journal of Image, Graphics and Signal Processing, vol.4, no.10, pp.1-7, 2012.

[25] Yamashita, R., Nishio, M., Do, R. K. G., & Togashi, K. (2018). Convolutional neural networks: an overview and application in radiology. Insights into imaging, 9(4), 611-629.

[26] Gatys, L. A., Ecker, A. S., & Bethge, M. (2016). Image style transfer using convolutional neural networks. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 2414-2423).

[27] Sylvester, J. J. (1889). On the reduction of a bilinear quantic of the nth order to the form of a sum of n products by a double orthogonal substitution. Messenger of Mathematics, 19(6), 42-46.

[28] Pearson, K. (1901). LIII. On lines and planes of closest fit to systems of points in space. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 2(11), 559-572.

[29] The convolutional neural network. [Online]. – Available: https://intellect.ml/svertochnaya-nejronnaya-set-convolutional-neural-network-cnn-6013

[30] The Complete Beginner’s Guide to Deep Learning: Convolutional Neural Networks and Image Classification. [Online]. – Available: https://towardsdatascience.com/wtf-is-image-classification-8e78a8235acb

[31] Convolutional Neural Networks as a modern approach in AI. [Online]. – Available: https://svitla.com/blog/convolutional-

neural-networks-as-a-modern-approach-in-ai

[32] Convolutional_neural_network. [Online]. – Available: https://en.wikipedia.org/wiki/Convolutional_neural_network

[33] Kosko, B. (1988). Bidirectional associative memories. IEEE Transactions on Systems, man, and Cybernetics, 18(1), 49-60.

[34] Feng, C., & Plamondon, R. (2001). On the stability analysis of delayed neural networks systems. Neural networks, 14(9), 1181-1188.

[35] Kazmirchuk, S., Anna, I., & Sergii, I. (2019, January). Digital signature authentication scheme with message recovery based on the use of elliptic curves. In International Conference on Computer Science, Engineering and Education Applications (pp. 279-288). Springer, Cham.

[36] Ilyenko, A., Ilyenko, S., & Prokopenko, O. (2020). The improvement of ntruencrypt public key cryptosystem:design and performance evaluation. Cybersecurity: education, science, technique, 2(10), 123-134. https://doi.org/10.28925/2663-4023.2020.10.123134

[37] Kazmirchuk, S., Ilyenko, A., Ilyenko, S., Olesya, Y., Herasymenko, M., & Iavich, M. (2020). Improved Gentry's Fully Homomorphic Encryption Scheme: Design, Implementation and Performance Evaluation.

[38] Kazmirchuk, S., Ilyenko, A., Ilyenko, S., Prokopenko, O., & Mazur, Y. (2020, January). The Improvement of Digital Signature Algorithm Based on Elliptic Curve Cryptography. In International Conference on Computer Science, Engineering and Education Applications (pp. 327-337). Springer, Cham.

Authors' Profiles

Ilyenko Anna

Candidate of Technical Sciences, assistant professor, assistant professor of Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine

She has 12 years of experience in teaching. Total number of research publications are more 100. Areas of scientific interests: applied cryptography and cybersecurity.

ORCID ID: 0000-0001-8565-1117

Ilyenko Sergii

Candidate of Technical Sciences, assistant professor, assistant professor of Automation and Energy Management Department National Aviation University of Kyiv, Aerospace Faculty, Ukraine

He has 12 years of teaching experience. Total number of research publications are 82. Areas of scientific interests: aviation, cybersecurity.

ORCID ID: 0000-0002-0437-0995

Marharyta Herasymenko

Student Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine

Areas of scientific interests: neural networks, applied cryptography and cybersecurity.

ORCID ID: 0000-0003-1142-0572

How to cite this paper: Ilyenko Anna, Ilyenko Sergii, Herasymenko Marharyta, "A Biometric Asymmetric Cryptosystem Software Module Based on Convolutional Neural Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.6, pp.1-12, 2021. DOI: 10.5815/ijcnis.2021.06.01