applied system innovation

MDPI

Article

Human Identification Based on Electroencephalogram Analysis When Entering a Password Phrase on a Keyboard

Alexey Sulavko *,† **and Alexander Samotuga** †

Department of Comprehensive Information Security, Omsk State Technical University, 644050 Omsk, Russia; samotugasashok@mail.ru

* Correspondence: sulavich@mail.ru; Tel.: +79-5339-490-54

† These authors contributed equally to this work.

Abstract: The paper proposes a method for identifying a person based on EEG parameters recorded during the process of entering user password phrases on the keyboard. The method is presented in two versions: for a two-channel EEG (frontal leads only) and a six-channel EEG. A database of EEGs of 95 subjects was formed, who entered a password phrase on the keyboard, including states in an altered psychophysiological state (sleepy and tired). During the experiment, the subjects' EEG data were recorded. The experiment on collecting data in each state was conducted on different days. The signals were segmented in such a way that the time of entering the password phrase corresponded to the time used during the EEG to identify the subject. The EEG signals are processed using two autoencoders trained on EEG data (on spectrograms of the original signals and their autocorrelation functions). The encoder is used to extract signal features. After identifying the features, identification is performed using the Bayesian classifier. The achieved error level was 0.8% for six-channel EEGs and 1.3% for two-channel EEGs. The advantages of the proposed identification method are that the subject does not need to be put into a state of rest, and no additional stimulation is required.

Keywords: electroencephalograms; autoencoder; biometrics; neural networks; signal analysis; neural interfaces

Citation: Sulavko, A.; Samotuga, A. Human Identification Based on Electroencephalogram Analysis When Entering a Password Phrase on a Keyboard. *Appl. Syst. Innov.* **2024**, *7*, 119. https://doi.org/10.3390/asi7060119

Academic Editor: Friedhelm Schwenker

Received: 14 September 2024
Revised: 21 November 2024
Accepted: 25 November 2024
Published: 29 November 2024

1. Introduction

Traditional authentication mechanisms (passwords, qualified and unqualified electronic signatures, and confirmation via phone) are alienable from the owner; therefore, they are subject to the "human factor". These protection methods are unsafe for people with low computer literacy and those who neglect security issues.

The problem of "alienation" of the authenticator is solved by linking keys and passwords to a person's biometric parameters. Many commercial solutions currently available are based on static biometric images (fingerprints, iris patterns, face, etc.). Their fundamental problem is that they are not secret. An intruder can falsify an open biometric image, so the biometric image used for authentication must be secret (combine a password and the user's individual characteristics). Secret biometric images can be formed when reproducing any subconscious movements by a person. For example, a person's keyboard handwriting reflects the characteristics of his hand movements when entering a password phrase or typing arbitrary text [1]. Keyboard handwriting images are considered uninformative and provide a relatively high percentage of incorrect solutions during identification and authentication. All dynamic biometric images, such as voice and handwritten passwords, are subject to this problem to varying degrees [2].

Almost any biometric image can be intercepted: a voice is recorded on a microphone, keyboard handwriting can be secretly tracked using keyloggers, fingerprints are left on objects, images of faces are on photographs, signatures are on paper, etc. Since technologies for generating adversarial examples are constantly being improved—generative neural networks based on the transformer architecture and adversarial learning methods [3] allow

for a targeted enumeration of biometric images and minimize the complexity of an attack on a biometric system—theft of open biometrics is not a problem for a qualified attacker.

There is a need to create an alternative authentication method that is free from the above-mentioned shortcomings. In this paper, it is proposed to use the features of the user's electroencephalogram (EEG) recorded during the process of entering a password (password phrase or text) on the keyboard to recognize the user's identity (Figure 1). EEG is a set of signals characterizing the electrical activity of the brain, recorded non-invasively using electrodes located on the surface of the head. Studies have shown that human EEG parameters are unique [4]. The set of EEG indicators of a subject can be considered as a vector of biometric parameters.

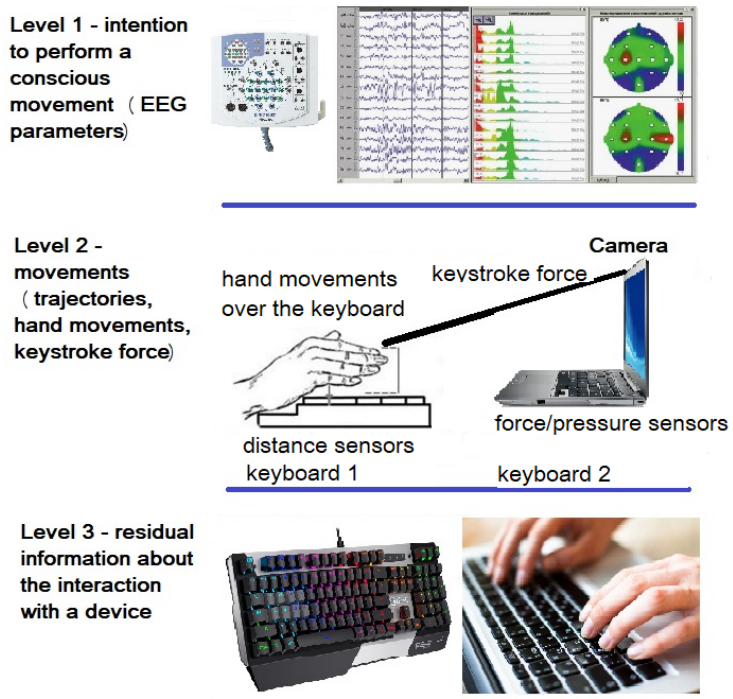

Figure 1. The process scheme of user identification recorded during the process of entering a password.

Biometric EEG images are the most secure against any kind of attack. The falsification of these features is complicated because the EEG signals required for the synthesis and transformation of identifiers are difficult to intercept, and it is impossible to do this remotely or covertly (unlike keyboard handwriting or fingerprints left on objects). The advantages of the method also include the fact that it can be used by people with disabilities, and that the secret biometric image of the EEG can be changed at any time if it somehow has been compromised. Identification requires the human brain to reproduce a stable impulse. For this purpose, the organs of hearing, vision, etc., are stimulated. By changing the stimulus affecting the subject's brain at the time of identification, the nature of the EEG signals changes, so the stimulus plays the role of a password, and the features of the EEG are biometric features that depend on the password.

The study of the brain is an area of active research; as a result of which, EEG recording equipment is constantly being modernized. There are various types of electrodes (dry, bridge, cup), each of which can operate in different conditions. The element base is being improved, due to which the cost of electroencephalographs is decreasing. In addition, artificial intelligence and big data analysis methods are actively developing. These prerequisites allow us to consider the subject's EEG images as an alternative to traditional passwords and biometric features seriously in the near future.

To date, the methods of identification and authentication by EEG are usually based on visual stimulation or recording of the EEG of the subject at rest, which may be difficult in practice. This work is devoted to the development of a method that allows recognizing

the identity of a computer user in real conditions when working on a computer (without additional stimulation). The purpose of the study is to develop a method for identifying a person by the electrical activity of the brain during the process of entering a password phrase on a computer.

The proposed method, unlike those that existed before, is relatively stable to changes in the user's state, allows for real-time user recognition without "plunging" into a state of rest, and can be integrated with the keystroke dynamics control method (if the user enters an incorrect phrase, access will be denied). The novelty of this study is that we used the subconscious movements of the user typing a learned phrase on the keyboard as a stimulus for the formation of evoked potentials. Thus, for the first time, a method for identifying a person by keystroke dynamics has been proposed that uses the parameters of evoked potentials of the EEG as biometric features instead of the parameters of time delays, pressing force, or other characteristics used in this task by other researchers.

2. State of the Art

In their works, the authors use various types of stimuli or tasks to evoke potentials (to provoke the brain to produce certain reactions that are then analyzed in order to identify individual characteristics of the EEG of subjects). The following stimuli (tasks) were used in well-known works:

1. Breathing task. Subjects close their eyes and focus on their breathing for several seconds (minutes) [5,6].
2. Imagining movements of body parts (without actually moving them) or reproducing movements for several seconds (minutes) [7].
3. Audio stimulation [8]:
    - Mentally singing or pronouncing individual words (phrases). Subjects imagine singing (in silence) for several seconds (minutes);
    - Listening to sounds. Subjects close their eyes and listen to a sound tone (or music) for several seconds (minutes).
4. Visual stimulation. This method is the most common and is found in most publications. Many experiments of varying complexity are based on the principle of visual stimulation. It is believed that the occipital areas of the brain are responsible for visual processing (the strongest visually evoked potential (VEP)) [9]. Many studies have focused on evoking the P300 potential (this is a positive deviation with an amplitude of 2–5 μV with a delay of 300–600 ms after the stimulus is applied) [10]. Analysis of the P300 potential was used to create interfaces for mental password entry by focusing the gaze on symbols (pass-thought). Typically, P300 is measured by analyzing signals from the Fz, Cz, and Pz electrodes of the standard 10–20 arrangement. To detect P300, the signal accumulation principle is used. Before averaging, the EEG signal must be passed through a bandpass filter (usually with a passband of 1–20 Hz) and artifacts (eye movements, etc.) must be removed. Also analyzed are N1 (N100) waves—negative deviations that peak between 90 and 200 ms after the presentation of an unexpected stimulus. Sometimes subjects are asked to imagine an object or abstraction.

Each type of stimulus or task activates different areas of the brain (cortex). Therefore, analysis of data from the corresponding electrodes allows us to identify features that characterize a person (either their condition or the action being performed).

The cerebral cortex is divided into zones—Brodmann cytoarchitectonic areas (52 fields are identified). A more detailed brain map containing about 180 functional zones was compiled in 2016 by David van Essen [11]. The EEG signal is usually described by the concept of rhythmic activity, which is usually classified by frequency, dividing into alpha (8–13 Hz), beta (14–40 Hz), gamma (30–100 Hz), theta (4–8 Hz) and delta (1–4 Hz) rhythms (waves, ranges) [12]. To remove uninformative frequencies, (frequency) filters (Butterworth,

Welch) are often used. To highlight EEG features, spectral, correlation and wavelet analysis methods [13], as well as artificial neural networks, are actively used.

There are publicly available EEG databases (DEAP, GrazIIIa, Alcoholism, PhysioNet and others) [10,14]. They contain EEGs obtained under the influence of strictly defined types of stimuli. When developing new methods of identification (authentication) by EEG, these data may not be applicable.

In the work [15], a method of identification of the person by parameters of EEG called CEREBRE (Cognitive Event-RElated Biometric REcognition) was proposed. The principle of its work consists of the assessment of individual reactions to various stimuli (for example, primary visual perception, recognition of familiar faces, taste). A test set of 400 images of the corresponding theme was prepared. A total of 50 volunteers who were asked to choose a visual image password took part in the experiment. The participants were placed in front of the screen in a sound isolation chamber protected from electromagnetic influences. While the stimuli were shown to subjects, a 26-channel EEG and a 3-channel electrooculogram were recorded. The obtained data were used for training. At the testing stage, the subjects were shown the same images in random order, but when a "black label" appeared before the image, the subjects presented the image password. The system identified the subjects without errors even 514 days after training. The disadvantage of this method is the lengthy training procedure, as well as the need to create ideal conditions for use, imposing significant restrictions on the application of the method in real practice.

The authors of the work [16] claim that using the spectral power of brain gamma waves as features increases the accuracy of biometric authentication by EEG. An experiment in which EEG data from 109 subjects from the PhysioNet database were used (subjects were in a calm state with open eyes and closed eyes) was conducted. The obtained recognition reliability estimate was EER = 0.0196.

Multifactorial identification systems are known that use EEG and eye blink data [17]. The accuracy of the two-factor procedure for subject recognition has been obtained from 92.4% to 97.6%.

In [18], wavelet analysis and deconvolutional neural network (DNN) were used to recognize EEG images; as a result, a subject recognition accuracy of 94% was achieved.

The issues of creating models for generating cryptographic keys or passwords based on EEG data, which are subsequently used for authentication, are covered quite widely in the literature. Various authors consider the possibility of using schemes based on fuzzy extractor, fuzzy vault, and fuzzy commitment. In particular, the work [19] presents the results of an experiment on assessing the reliability of key generation involving 42 subjects (the probability of errors was 0.024). Some authors have assessed the influence of a person's emotional state on the stability of key generation using EEG data [20]. The subjects' emotional state was changed by various influences. The results showed that the EEG features used depend to a significant extent on the subject's state, which affects the reliability of key generation (the probability of error increases).

In [21], an EEG-based identification method using code-modulated visual-evolved potentials (c-VEPs) was proposed. The authors recorded two data sessions for each individual on different days to measure the performance of intra-session and cross-session identification. State-of-the-art VEP detection algorithms in brain–computer interfaces (BCIs) were used to build the template-matching-based identification framework. For cross-session identification, the error rate was 99.43% using 10.5-second EEG signals.

It is evident from the presented materials that research in this area is actively developing and is promising. Many researchers report high accuracy of human identification by EEG. However, in such cases, a small volume of test samples or a small number of subjects are usually used, or the method was tested under ideal conditions (as in the case of "error-free" recognition based on the CEREBRE method [15]). In addition, the training or identification procedure takes a lot of time. Nevertheless, the uniqueness of EEG indicators is very high. The method proposed in this paper is more practice-oriented and belongs to the second of the listed categories based on movement incentives.

3. Materials and Methods

3.1. About the Reproduction of Subconscious Movements When Typing Text on a Keyboard

3.1.1. The Connection Between Keyboard Handwriting and the Peculiarities of Brain Function

Let us consider three stages of reproducing a password on the keyboard, at which the peculiarities of the computer user's keyboard handwriting appear:

1. First of all, there is an intention to perform some action; the brain gives a command to perform conscious movements. A person cannot immediately perform complex movements, such as typing on a keyboard. In the process of learning, successful solutions to the task are selected and remembered through multiple repetitions (training). Muscle control programs are remembered in the subconscious and are implemented automatically. The features of the electrical activity of the brain in the process of entering a phrase on the keyboard are individual. By recording and analyzing the EEG, it is possible to identify biometric parameters—features that characterize a specific person. The identified features can be very informative if the EEG recording is long enough. These features can also characterize the selected password phrase, and the psychophysiological and emotional state of the operator.
2. At the second level, the operator's movement patterns are revealed. It is known that the operator interacts with the keyboard using 20 shoulder girdle muscles on each arm. The operator's individual characteristics can be identified by analyzing the trajectories of hand movements when typing a phrase on the keyboard using special sensors (a rangefinder, and for a smartphone, an accelerometer [22] and a gyroscope [23]). Additionally, keyboard handwriting can be judged by the force of pressing the keys [24] and the vibration level of the keyboard.
3. The last level of keyboard dynamics is the data on time delays between pressing keys and the time they are held [1]. These features can be registered on any keyboard, but they contain significantly less information about the user than those described above. In addition, these features depend on the keyboard used, the operator's state, the time of day, and they also change significantly over time. For these reasons, this type of keyboard dynamics features is almost never used in real practice for the purposes of access control to computer resources, although the method is very easy to implement programmatically.

3.1.2. Areas of the Brain Involved in Reproducing Movements When Working with a Keyboard

The problem of the hierarchical organization of human movements was considered in the works of the Russian physiologist N.A. Bernstein. In the same work, a theory of the levels of movement construction was presented. The levels are understood as morphological sections of the nervous system, each of which corresponds to its own type of movement. Five levels were identified (Figure 2) [25]:

- The A level is responsible for muscle tone. A typical independent manifestation of this level is the body trembling from cold or fear.
- At the B level, the work of "temporary ensembles" (synergies) is organized. This level takes part in the formation of movements of a more complex type without taking into account the characteristics of external space (stretching, involuntary facial expressions, and simple reflexes).
- At the C level, information about external space coming from the senses is taken into account. This level is responsible for constructing movements adapted to the spatial properties of objects—running, waving arms, etc.
- The D level is responsible for organizing interaction with objects. At this level, data on the main physical characteristics of surrounding objects are taken into account, and the motor programs used are made up of flexible, interchangeable links.
- At the E level, "intellectual" motor acts are formed (for example, speech or writing). Moreover, it can be called "objectless" because movements are determined by an

abstract meaning (when a person writes a letter, he thinks about the meaning of the letter, and not about the mechanical process of writing itself).

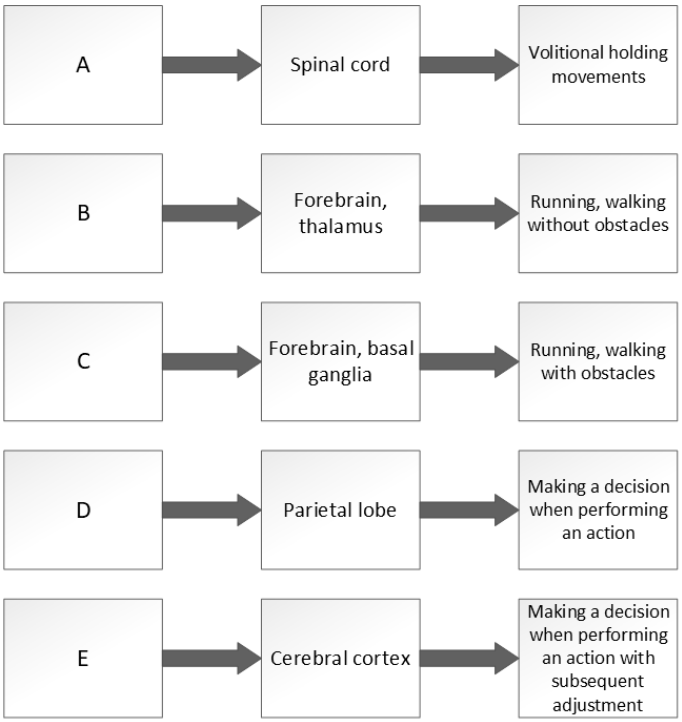

Figure 2. Levels of movements and the involvement of different parts of the brain in their reproduction.

When typing on a keyboard, the extrapyramidal system conducts nerve impulses to support the position of the back, arms and shoulders to allow typing. The pyramidal system conducts motor impulses for coordinated and independent movements of the fingers. Learned voluntary movements are activated by pyramidal cells in the motor area on the opposite side of the cerebral cortex and by impulses from the cerebellum. Movement intentions are translated into specific programs by areas of the premotor and association cortex (frontal and parietal areas), the basal ganglia, and lateral part of the cerebellum. The thought to initiate a specific movement is translated into detailed neural programs by the basal ganglia, premotor cortical areas (Brodmann areas 5, 6, 7, as seen in Figure 3), and the lateral cerebellum. In the primary motor cortex (Brodmann area 4, as seen in Figure 3), these instructions are decoded and executed. This area of the cerebral cortex contains centers that control muscle groups belonging to the opposite side of the body. The intermediate zones of the cerebellar hemispheres receive two types of information: at the start of the movement from the motor cortex about the sequence of the movement plan, and from the peripheral parts of the body (limbs) about the nature of the movement being performed. After comparing this information, the cells of the deep intermediate nucleus send corrective signals to the motor cortex. There are several feedback loops for controlling voluntary movements. One of them is the visual system. When typing, individual zones of the frontal lobe, supplementary motor area, parietal area, and other regions are activated. Movements that include rapid sequences of muscle contractions cause an increase in blood flow in the supplementary motor cortex [26].

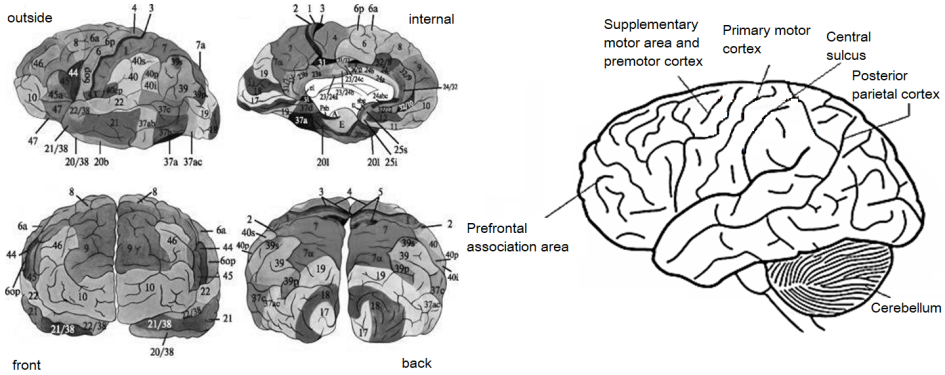

Figure 3. Map of Brodmann's areas of the cerebral cortex, with numbers indicating surfaces (**left**) and topography of motor areas of the brain (**right**).

3.2. Dataset Description

To analyze the brain activity of an operator when entering text on the keyboard, it is sufficient to take readings from the following electrodes (based on the previously presented information) installed in accordance with the 10–20 scheme (monopolar installation), Fp1, Fp2, Fz, F3, F4, and Cz, as well as reference electrodes A1 and A2 (Figure 4). The 10–20 scheme is a standard method of electrode placement used to collect EEG data, including in modern neurophysiological studies. The letter designations of the 10–20 system indicate the zones of the cerebral cortex where the corresponding electrodes are located (F—frontal, T—temporal, C—central, P—parietal, and O—occipital).

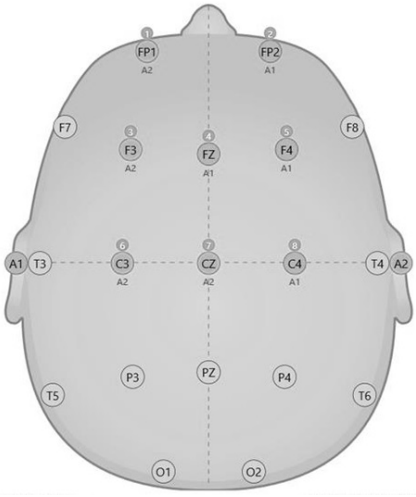

Figure 4. Connections of electrodes for recording electrical activity of the brain when the subject types on the keyboard (electrodes used in the experiment: Fp1, Fp2, Fz, F3, F4, Cz, A1, A2, and monopolar fastening).

An experiment to collect EEG data from 95 subjects was carried out. The subjects were asked to enter a phrase consisting of several words (30–50 characters on average) on a keyboard with a plastic case. Each subject entered their own unique secret phrase at least 50 times. At the same time, the EEG of the brain was recorded using a 19-channel Mitsar-EEG-201 electroencephalograph (with a noise level of less than 2 μV from peak to peak and a signal quantization frequency of 250 Hz per channel). All subjects underwent a series of experiments four times on different days (to identify stable, robust features and exclude features with a high degree of variability over time). During the first two days, the subjects entered data from the keyboard in a normal psychophysiological state; on the third day, the subjects were put into a sleepy state (they were asked to take two motherwort tablets of 200 mg each, after which the subjects sat in a chair for 20 min in a quiet and dark

room immediately before the start of the EEG recording). On the fourth day, they were put into a state of fatigue (the subjects were subjected to physical exertion, the volume of which was determined by the Martinet method and then varied depending on the physical capabilities of the subject).

3.3. EEG Image Processing

First, let us look at how the signal is generated in the brain that triggers a chain of subconscious movements for typing on the keyboard. Next, we will describe collecting EEG data and the methods for processing the data.

3.3.1. Preprocessing of EEG Data

A notch filter (45–55 Hz) was applied to the EEG signals to eliminate interference caused by power lines. The EEG images were then divided into fragments corresponding in time to periods of correct and incorrect password entry.

Visual analysis of the fragments showed that the subjects' EEGs generally have distinctive features. For some subjects, the moments between the end of the next phrase input and the beginning of the next one are clearly visible (Figure 5). For each subject, a different level of correlation is observed between the fragments of signals from different electrodes (cross-correlation). Autocorrelation functions also have features. In particular, the average number of zero crossings (sign change frequency) and extrema for autocorrelation functions differ for different subjects. Individual features of human EEGs are quite unstable, but they can be observed in large samples by constructing empirical probability densities of the values of the parameters under study.

Figure 5. EEG during the entry of the password phrase by the subject

The EEG records were divided into fragments corresponding to the periods of phrase input. The average fragment duration was 7.5 s (1875 reports). Then, from each fragment, a signal spectrogram and a spectrogram of its autocorrelation function were calculated for each channel, Fp1, Fp2, Fz, F3, F4, and Cz (a total of 6 channels), with a window width of 64 and a step of 4. In this case, 4 types of window functions were used when calculating the spectrograms—rectangular, Hamming, Bartlett and Gauss. The output was 48 spectrograms (2 types of function—original and autocorrelation, 4 types of windows and 6 channels). This technique with several types of window functions was used to augment the training sample of the autoencoder, which was then used to transform the spectrogram into a feature vector.

All spectrograms after their construction were interpolated along the time scale to bring them to a fixed dimension of 32×256 (where the first dimension is associated with the frequency scale of the spectrogram; the second is associated with the time scale).

3.3.2. Feature Extraction

To extract features, we used an autoencoder with the architecture presented in Table 1. This is a neural network architecture that consists of two segments—an encoder and a decoder. The encoder compresses the data into a compact representation, and the decoder reconstructs it. The network is trained as a single whole, while the same data, that are feature vectors, are supplied to the input and output. Autoencoders are often used to extract features [27]. In total, 12 autoencoder architectures were tested, differing in the number of layers, convolution kernels and the size of the kernel of the first convolutional layer, the number of fully connected layers and neurons in each of them.

Table 1. Architecture of the autoencoder for feature extraction.

Layer Type	Layer Parameters
Encoder	
Input	dimension is 32 × 256
ConvL (2D)	number of filters—2, convolution window—3.3, convolution step—2.2, activation function—ReLU
ConvL (2D)	number of filters—4, convolution window—3.3, convolution step—2.2, activation function—ReLU
	Batch normalization
ConvL (2D)	number of filters—8, convolution window—3.3, convolution step—2.2, activation function—ReLU
ConvL (2D)	number of filters—16, convolution window—3.3, convolution step—2.2, activation function—ReLU
	Batch normalization
ConvL (2D)	number of filters—32, convolution window—3.3, convolution step—2.2, activation function—ReLU
ConvL (1D)	number of filters—64, convolution window—3.3, convolution step—2.2, activation function—ReLU
	Batch normalization
ConvL (1D)	number of filters—128, convolution window—1.3, convolution step—1.2, activation function—ReLU
ConvL (1D)	number of filters—256, convolution window—1.3, convolution step—1.2, activation function—ReLU
	Batch normalization
Fully connected layer	number of neurons—256, activation function – linear
Decoder	
Input	dimension is 256
TConvL (2D)	number of filters—128, window—3.3, step—2.2, activation function—ReLU
TConvL (2D)	number of filters—64, window—3.3, step—2.2, activation function—ReLU
	Batch normalization
TConvL (2D)	number of filters—32, window—3.3, step—2.2, activation function—ReLU
TConvL (2D)	number of filters—16, window—3.3, step—2.2, activation function—ReLU
	Batch normalization
TConvL (2D)	number of filters—16, window—3.3, step—2.2, activation function—ReLU
TConvL (1D)	number of filters—4, window —— 1.3, step—1.2, activation function—ReLU
	Batch normalization
TConvL (1D)	number of filters—2, window—1.3, step—1.2, activation function—ReLU
TConvL (1D)	number of filters—1, window—1.3, step—1.2, activation function—sigmoid

Each autoencoder received one spectrogram as input and 256 features as output. The autoencoders were trained using data from 30 subjects. A total of 2 autoencoders with identical architecture were created: the first was trained using spectrograms of the original signal and the second was trained using spectrograms of the autocorrelation function. The training sample size was over 36,000 (30 subjects, at least 50 examples, 6 channels, and 4 types of window functions) images for each autoencoder. The number of epochs was 200; the Adam optimizer was used.

After training, the decoder was removed and only the encoder was used. To extract features, 6 spectrograms were extracted from the original signal and the autocorrelation function (based only on the Hamming window, since it is noise-reducing). Spectrograms were sent to the corresponding encoders (Figure 6), which extracted features. Thus, each EEG image was transformed into a vector of 3072 features (Figure 7).

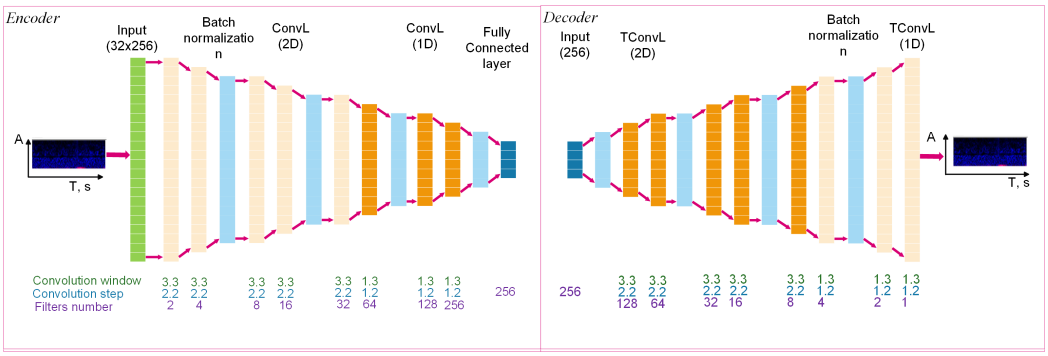

Figure 6. Diagram of the autoencoder for feature extraction architecture.

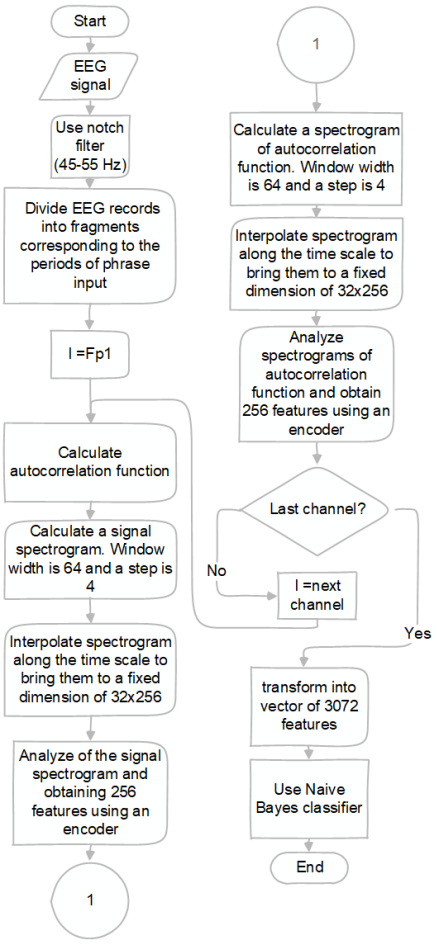

Figure 7. Data-preprocessing flow chart.

4. Results

Each subject must first create a biometric template—train the recognition system. The training sample of the subject included EEG samples obtained on the first day of the experiment. The remaining EEG data of the subject were assigned to the test sample. According to this principle, the training and test sample of 65 subjects was compiled.

For each feature and subject, probability densities were constructed based on the training set, based on the hypothesis of a normal distribution of features (which was confirmed by the chi-square method). It was decided to build a classifier based on a "naive" Bayesian classifier. Each subject template is assigned a hypothesis. The method calculates the a posteriori probabilities of hypotheses for a certain number of steps equal to the number of features entering the identification process. At each step, the a posteriori probabilities of hypotheses are calculated using formula (1), taking into account the value of the next feature, while the a posteriori probability of a hypothesis calculated at the previous step is taken as the a priori probability. In the first step, all hypotheses are equally probable $P(H_i|A_0) = n^{-1}$, where n is the number of hypotheses, i.e., identified subjects. In the last step, preference is given to the hypothesis with the maximum a posteriori probability.

$$P(H_i|A_j) = \frac{P(H_i|A_{j-1})P(A_j|H_i)}{\sum_{i=1}^{n} P(H_i|A_{j-1})P(A_j|H_i)} \quad (1)$$

where $P(H_i|A_j)$ is the posterior probability of the i-th hypothesis calculated at the j-th step, and $P(A_j|H_i)$ is the conditional probability of the i-th hypothesis, equal to the probability density of the j-th feature for the i-th template. In this version, the Bayesian classifier is often called "naive", since it is assumed that the features are statistically independent (which in practice is most often not the case). To create a user standard (i.e., to train the Bayesian classifier by calculating the probability density functions of each feature), at least 50 EEG examples of each user were used, equal to the number of attempts to enter the password phrase.

Using the created templates and test sample, a computational experiment was conducted to identify subjects. The result of experiment is presented in Figure 8. First, single EEG samples were fed to the input of the method. Then, several samples were combined into one of greater duration—the dimension of the feature vector gradually increased from 3072 to 12,288.

As can be seen from Table 2, the reliability of subject recognition for the proposed method is quite high and corresponds to the world level.

An additional series of experiments were also conducted. During the mentioned experiments, EEG data corresponding to the altered state of the subject (fatigue, sleepy) were used for testing, provided that the subject standard was created in a normal state (according to the recordings obtained on only the first, as well as on the first and second days of the experiment).

In addition to using all the specified electrodes, we also tested the use of only the frontal branches Fp1 and Fp2, for which dry electrodes can be used in practice. Dry electrodes do not work well through hair, so we separately tested the use of only the frontal branches Fp1 and Fp2.

As can be seen from Table 2, the reliability of subject recognition for the proposed method is quite high and corresponds to the world level. We see that for a two-channel EEG, the accuracy decreases, but is still at an acceptable level (98.7%; error probability 0.013). It can also be seen that the state of fatigue of the subject greatly affects the identification results, in contrast to the sleepy state. Apparently, fewer artifact amounts appear on the EEG in the sleepy state. However, if we use data from the normal state obtained on different days as a training sample, we can increase the system's resistance to changes in the subject's state.

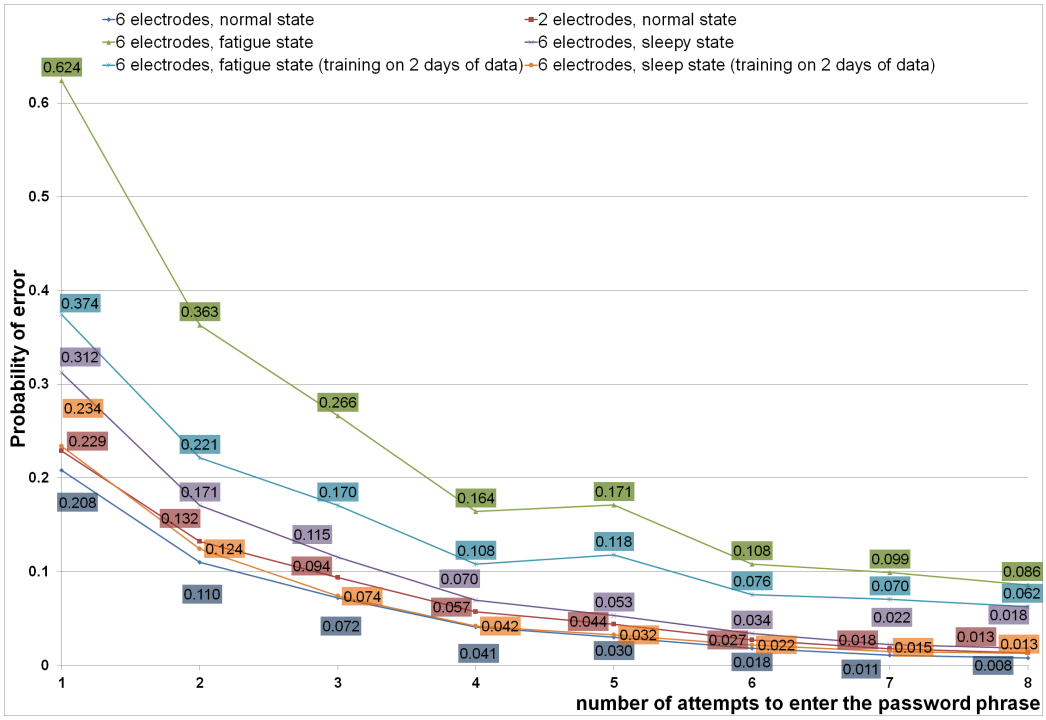

Figure 8. Probability of subject identification error as a result of performing a computational experiment.

In real practice, it is necessary to ensure protection of biometric templates from compromise. For this purpose, an approach based on fuzzy extractors [19] or shallow artificial neural networks with automatic robust learning [28] is used at the stage of image classification.

Table 2. Comparison of the obtained results with the results achieved in other studies.

Brief Information About the Method	Dataset	Accuracy, %
Authentication technique based on simple cross-correlation values of PSD features extracted from 19 EEG channels during eyes-closed and eyes-open rest-state conditions.	EEG of 109 subjects from the PhysioNet database	98.04 [16]
Deep neural network (DNN) is used to classify the data. Optimization and regularization methods are employed to improve the accuracy of the results.	109 individuals	99.19 [29]
EEG-based cryptographic key generation systems.	The EEG data of 80 subjects from AEEG dataset	97.42 [13]
Automatic channel selection, wavelet feature extraction and deep neural network (DNN) classifier.	DEAP multimodal dataset	94 [18]
Biometric authentication method based on the discrete logarithm problem and Bose–Chaudhuri–Hocquenghem (BCH) codes.	42 subjects	97.6 [19]
EEG-based cryptographic key generation.	16 channels selected from the DEAP dataset	97.88 [20]
EEG-based identification method using code-modulated visual echo potentials (c-VEPs).	25 subjects	99.43 [21]
Proposed method	95 subjects	99.2

5. Conclusions

Before the subject starts typing, the brain initiates a sequence of actions that are subsequently adjusted when analyzing information coming from the peripheral parts of the body. The performed movements have features that affect the time delays between pressing the keys and holding them down. Together, these delays are called keyboard handwriting. Thus, the individual style of working with the keyboard is initially formed in the cerebral cortex.

Experiments have shown that the EEG images of the operator performing the keyboard input are unique. The achieved percentage of erroneous decisions in identifying 65 subjects was 0.8%, which corresponds to the world level in this area of research. The advantages of the proposed identification method are that the subject does not need to be put into a state of rest (most methods are efficient if the user is in a calm state and immobilized, preferably sitting with eyes closed), and no additional stimulation (visual, sound) is required. Unlike previous existing methods, the proposed method can be used for continuous identification of the operator in the process of professional activity and can be combined with methods of identification by keyboard handwriting.

At the moment, the specified percentage of erroneous decisions is achieved based on an average of 1 min of monitoring, which corresponds to entering the password phrase eight times. When using a single entry, the error is too high—more than 20%. For practice, you need to use at least four entry attempts (an average of 30 s), which corresponds to 4.1% of errors.

It has been established that if the user was in different psychophysiological states during the training and operation of the system, the identification accuracy drops (from 3 to 11 times in a tired state, or from 2 to 3 times in a sleepy state). To eliminate or reduce this negative effect, it is proposed to train the system on user data obtained on different days. This will level out random outliers and data bias related to the installation of electrodes and the user's emotional background.

Further research will be aimed at improving the identification accuracy, reducing the transit time, and protecting biometric templates. In the future, using hierarchical deep learning neural networks [30] is planned for feature extraction and using the c-neuro-extractor model proposed in [31] is planned for building a classifier.

Author Contributions: A.S. (Alexey Sulavko): Conceptualization, methodology, software, validation, formal analysis, investigation, resources, writing—original draft preparation, writing—review and editing, supervision, project administration, and funding acquisition; A.S. (Alexander Samotuga): validation, formal analysis, investigation, data curation, writing—original draft preparation, writing—review and editing, and visualization. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the state assignment of Ministry of Science and Higher Education of the Russian Federation grant number theme No. FSGF-2023-0004.

Informed Consent Statement: Written informed consent has been obtained from the research participants to publish this paper.

Data Availability Statement: Data that were used in the present research, such as datasets from aiconstructor, are partially available to download on the following link http://en.aiconstructor.ru/page40799810.html (accessed on 14 Septemer 2024).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Sulavko, A. An abstract model of an artificial immune network based on a classifier committee for biometric pattern recognition by the example of keystroke dynamics. *Comput. Opt.* **2020**, *44*, 830–842. [CrossRef]
2. Sulavko, A. Highly reliable two-factor biometric authentication based on handwritten and voice passwords using flexible neural networks. *Comput. Opt.* **2020**, *44*, 82–91. [CrossRef]
3. Ren, H.; Yan, A.; Ren, X.; Ye, P.G.; Gao, C.Z.; Zhou, Z.; Li, J. GanFinger: GAN-Based Fingerprint Generation for Deep Neural Network Ownership Verification. *arXiv* **2023**, arXiv:cs.CR/2312.15617.

4. Sulavko, A.; Lozhnikov, P.; Choban, A.; Stadnikov, D.; Nigrey, A.; Inivatov, D. Evaluation of EEG identification potential using statistical approach and convolutional neural networks. *Inf. Control. Syst.* **2020**, *6*, 37–49. [CrossRef]
5. Hong, Y.G.; Kim, H.K.; Son, Y.D.; Kang, C.K. Identification of Breathing Patterns through EEG Signal Analysis Using Machine Learning. *Brain Sci.* **2021**, *11*, 293. [CrossRef]
6. Xia, Q.; Bai, X.; Zhang, J.; Cui, S.; Wang, G.; Baruah, A. Machine Learning Technology is Used to Classify Respiratory Patterns According to EEG Signals. In *Lecture Notes on Data Engineering and Communications Technologies*; Springer Nature: Singapore, 2023; pp. 703–708. [CrossRef]
7. Giannopulu, I.; Mizutani, H. Neural Kinesthetic Contribution to Motor Imagery of Body Parts: Tongue, Hands, and Feet. *Front. Hum. Neurosci.* **2021**, *15*, 602723. [CrossRef]
8. Ramirez-Aristizabal, A.G.; Ebrahimpour, M.K.; Kello, C.T. Image-based eeg classification of brain responses to song recordings. *arXiv* **2022**, arXiv:2202.03265. [CrossRef]
9. Martínez-Cagigal, V.; Thielen, J.; Santamaría-Vázquez, E.; Pérez-Velasco, S.; Desain, P.; Hornero, R. Brain–computer interfaces based on code-modulated visual evoked potentials (c-VEP): A literature review. *J. Neural Eng.* **2021**, *18*, 061002. [CrossRef]
10. Won, K.; Kwon, M.; Ahn, M.; Jun, S.C. EEG Dataset for RSVP and P300 Speller Brain-Computer Interfaces. *Sci. Data* **2022**, *9*. [CrossRef]
11. Glasser, M.F.; Coalson, T.S.; Robinson, E.C.; Hacker, C.D.; Harwell, J.; Yacoub, E.; Ugurbil, K.; Andersson, J.; Beckmann, C.F.; Jenkinson, M.; et al. A multi-modal parcellation of human cerebral cortex. *Nature* **2016**, *536*, 171–178. [CrossRef]
12. Nigrey, A.A.; Sulavko, A.E.; Samotuga, A.E.; Inivatov, D.P. On the person and psychophysiological state identification using electroencephalogram parameters. *J. Physics Conf. Ser.* **2020**, *1546*, 012092. [CrossRef]
13. Nguyen, D.; Tran, D.; Sharma, D.; Ma, W. On the Study of Impacts of Brain Conditions on EEG-based Cryptographic Key Generation Systems. *Procedia Comput. Sci.* **2018**, *126*, 713–722. [CrossRef]
14. DelPozo-Banos, M.; Travieso, C.M.; Weidemann, C.T.; Alonso, J.B. EEG biometric identification: A thorough exploration of the time-frequency domain. *J. Neural Eng.* **2015**, *12*, 056019. [CrossRef] [PubMed]
15. Ruiz-Blondet, M.V.; Jin, Z.; Laszlo, S. Permanence of the CEREBRE brain biometric protocol. *Pattern Recognit. Lett.* **2017**, *95*, 37–43. [CrossRef]
16. Thomas, K.P.; Vinod, A.P. EEG-Based Biometric Authentication Using Gamma Band Power During Rest State. *Circuits Syst. Signal Process.* **2017**, *37*, 277–289. [CrossRef]
17. Wu, Q.; Zeng, Y.; Zhang, C.; Tong, L.; Yan, B. An EEG-Based Person Authentication System with Open-Set Capability Combining Eye Blinking Signals. *Sensors* **2018**, *18*, 335. [CrossRef]
18. Li, Y.; Zhao, Y.; Tan, T.; Liu, N.; Fang, Y. Personal Identification Based on Content-Independent EEG Signal Analysis. In *Lecture Notes in Computer Science*; Springer International Publishing: Cham, Switzerland, 2017; pp. 537–544. [CrossRef]
19. Damaševičius, R.; Maskeliūnas, R.; Kazanavičius, E.; Woźniak, M. Combining Cryptography with EEG Biometrics. *Comput. Intell. Neurosci.* **2018**, *2018*, 1867548. [CrossRef]
20. Nguyen, D.; Tran, D.; Sharma, D.; Ma, W. Emotional Influences on Cryptographic Key Generation Systems using EEG signals. *Procedia Comput. Sci.* **2018**, *126*, 703–712. [CrossRef]
21. Zhao, H.; Wang, Y.; Liu, Z.; Pei, W.; Chen, H. Individual Identification Based on Code-Modulated Visual-Evoked Potentials. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3206–3216. [CrossRef]
22. Ning, E.; Cladek, A.T.; Ross, M.K.; Kabir, S.; Barve, A.; Kennelly, E.; Hussain, F.; Duffecy, J.; Langenecker, S.L.; Nguyen, T.; et al. Smartphone-derived Virtual Keyboard Dynamics Coupled with Accelerometer Data as a Window into Understanding Brain Health. In Proceedings of the CHI '23: CHI Conference on Human Factors in Computing Systems, Hamburg, Germany, 23–28 April 2023; ACM: New York, NY, USA, 2023; pp. 1–15. [CrossRef]
23. Senarath, D.; Tharinda, S.; Vishvajith, M.; Rasnayaka, S.; Wickramanayake, S.; Meedeniya, D. BehaveFormer: A Framework with Spatio-Temporal Dual Attention Transformers for IMU-Enhanced Keystroke Dynamics. In Proceedings of the 2023 IEEE International Joint Conference on Biometrics (IJCB), Ljubljana, Slovenia, 25–28 September 2023; IEEE: Piscataway, NJ, USA, 2023; Volume 9, pp. 1–9. [CrossRef]
24. Shekhawat, K.; Bhatt, D.P. A novel approach for user authentication using keystroke dynamics. *J. Discret. Math. Sci. Cryptogr.* **2022**, *25*, 2015–2027. [CrossRef]
25. Profeta, V.L.; Turvey, M.T. Bernstein's levels of movement construction: A contemporary perspective. *Hum. Mov. Sci.* **2018**, *57*, 111–133. [CrossRef] [PubMed]
26. Lu, F.M.; Wang, Y.F.; Zhang, J.; Chen, H.F.; Yuan, Z. Optical mapping of the dominant frequency of brain signal oscillations in motor systems. *Sci. Rep.* **2017**, *7*, 14703 . [CrossRef] [PubMed]
27. Michelucci, U. An Introduction to Autoencoders. *arXiv* **2022**, arXiv:2201.03898.
28. Sulavko, A.; Panfilova, I.; Samotuga, A.; Zhumazanova, S. Biometric Authentication Using Face Thermal Images Based on Neural Fuzzy Extractor. In Proceedings of the 2023 Intelligent Methods, Systems, and Applications (IMSA), Giza, Egypt, 15–16 July 2023; IEEE: Piscataway, NJ, USA, 2023; Volume 1, pp. 80–85. [CrossRef]
29. Akbarnia, Y.; Daliri, M.R. EEG-based identification system using deep neural networks with frequency features. *Heliyon* **2024**, *10*, e25999. [CrossRef]

30. Zhang, L.; Cheng, L.; Li, H.; Gao, J.; Yu, C.; Domel, R.; Yang, Y.; Tang, S.; Liu, W.K. Hierarchical deep-learning neural networks: Finite elements and beyond. *Comput. Mech.* **2020**, *67*, 207–230. [CrossRef]
31. Sulavko, A. Biometric-Based Key Generation and User Authentication Using Acoustic Characteristics of the Outer Ear and a Network of Correlation Neurons. *Sensors* **2022**, *22*, 9551. [CrossRef]