КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.196215
UDC 004.052

Mahyar Taj Dini
PhD student, senior lecturer of the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0001-8875-3362
m.tajdini@kubg.edu.ua

BIOMETRICAL AUTHENTICATION SYSTEMS USING ELECTROENCEPHALOGRAPHY

Abstract. There has been a growing movement to connect brain science to medicine, education, and industry in recent years. Personal authentication can be divided into the following types: knowledge authentication, property authentication, and biometric authentication. Authentication by passwords or PINs used to log in to a device falls under knowledge authentication. Property-based authentication is based on a person's property, such as a card or a key. Biometric Authentication is a personal authentication, which uses biometric information, and biometric authentication, such as fingerprints, irises, voiceprints, etc., has been developed. This article consists of eight sections about Biometrical Authentication and a conclusion. After introduction we had an overview on Biometric authentication in section two and then talking about biometric authentication technologies, further we discuss about already available authentication by physical characteristic such as Palm vein, fingerprint , iris recognition in chapter four, then we continue with behavioral authentication like voice authentication and it's problems in chapter five, then in chapter six we explain biometric authentication with feature extraction which means using Machine learning and Artificial intelligence in Authentication systems and by having that in chapter seven we explained performance of authentication by feature extraction and comparing Equal Error Rate and Receiver Operating Characteristics, False Rejection Rate and False Acceptance Rate for performance evaluation and finally in chapter eight we showed how Electroencephalography data by using feature extraction can be used for authentication with *k*-Nearest Neighbor and Support Vector Machine methods. Furthermore, in this study, we used Relaxation EEG, which means brainwave authentication without mental tasks or external stimuli.

Keywords: brain-machine interface; BMI; brain-computer interface; BCI; electroencephalography; EEG; Equal Error Rate; EER.

INTRODUCTION

Based on neuroscience, which is struggling to understand the brain, neurotechnology, which is research to utilize the brain, is developing. Brain Machine Interface (BMI) is divided into two types: invasive BMI, in which metal electrodes for recording neural activity are placed directly in the brain, and non-invasive BMI, in which brain activity is measured indirectly from outside the body. Invasive BMI can obtain highly accurate brain information, but it has problems such as brain damage, infection, and electrode deterioration. On the other hand, non-invasive BMI provides less accurate brain information, but there is no risk of brain damage, making it easier to conduct experiments on healthy subjects. For these reasons, non-invasive BMI is currently the mainstream and is being actively studied [1].

Examples of non-invasive BMIs include electroencephalography (EEG), which measures brain waves transmitted over the scalp, functional magnetic resonance imaging (fMRI), which visualizes the increase or decrease in blood flow, and near-infrared spectroscopy (NIRS), which measures the hemoglobin concentration in the blood using the transmission of near-infrared

light. NIRS (Near Infra-Red Spectroscopy) is a device that measures blood hemoglobin concentration using near-infrared light penetration. In particular, it is a method that healthy people can use safely and efficiently. The development of non-invasive BMI using EEG (electroencephalography) has been vigorously pursued. Currently, research is being conducted in various fields, such as prosthetic hands operated by EEG [2], wheelchair control systems that read EEG and move autonomously [3], and direct communication of EEG from person to person [4]. In addition, there are already commercially available BMI technologies, such as "nekomimi," a device that detects human emotions and moves, and "MindRDR," an application that controls Google Glass using brain waves [5].

As described above, BMI technology for operating devices using brain waves is advancing day by day. Typically, a mouse or keyboard is used to operate a computer, but with the development of BMI technology, it is expected that computer operation using EEG will become possible. P300 Speller, which displays alphanumeric characters on display and randomly lights up examples of characters in a row and a column, analyzes the user's P300 and calculates the sentence to be entered. It analyzes the sentence to identify the characters. In this way, EEG as a substitute for a keyboard has been studied from various points of view, and it is estimated that there is a high demand for computer operations using EEG.

Nowadays, we use personal authentication to log in to devices, which uses passwords and PINs. With the development of EEG keyboards, it will be possible to log into devices by entering passwords and PINs using EEG. However, if we consider computer operation by EEG, it is more reasonable to apply personal authentication using EEG as a "brain print" [6] than personal authentication using passwords or PINs.

Personal authentication can be divided into the following types: knowledge authentication, property authentication, and biometric authentication [7]. Authentication by passwords or PINs used to log in to a device falls under knowledge authentication. Property-based authentication is based on a person's property, such as a card or a key. Biometric Authentication is a personal authentication, which uses biometric information, and biometric authentication, such as fingerprints, irises, voiceprints, etc., has been developed.

AUTHENTICATION OVERVIEW

Knowledge authentication and property authentication are not always meant reliable for security. For example, in knowledge authentication, there is a possibility of forgetting or leaking knowledge information, and in property authentication, there is a problem of loss or theft of property. Biometric authentication, on the other hand, is less likely to be lost because there is no fear of forgetting, and, additionally, it is more secure because it is difficult to steal. Fingerprints, in particular, have high authentication performance and are already in practical use as a login method for devices. However, even biometric authentication systems have been falsified in some cases. One of the reasons for this is that the biometric information required for authentication is constantly exposed to the outside world. For example, it is possible to forge a fingerprint. For example, it is possible to forge fingerprints by making a mold of the fingerprint using silicon and then pouring silicon back into the mold. Biometric authentication using electroencephalogram (EEG), which is one of the internal information, has been devised. The biometric information that can be used for biometric authentication should satisfy the following three conditions: universality, uniqueness, and permanence. In other words, the best biometric information should have characteristics that all people have, no other person has the same characteristics, and the characteristics do not change with time. In terms of universality,

EEG is the most suitable biometric for biometric authentication because it can be used in all situations except brain death. The first is the universality of the biometric because a person's life or death is determined by the cessation of brain functions, except in the brain-dead state. Therefore, as long as a person is alive, they possess an EEG. Unlike biometric data such as fingerprints and iris, EEG is complex internal information requiring a unique measuring device. Therefore, it is highly confidential and less likely to be stolen than other biometric information. In addition, it can be used for other biometric information.

In other words, EEG can be used as a password. Such EEGs are called pass-thoughts [8]. EEG authentication using pass-thoughts is considered a two-factor authentication: knowledge authentication and biometric authentication. Typically, biometric authentication cannot be used for security reasons if the biometric information used for authentication is stolen. However, by using path thinking, the biometric information can be changed periodically, which increases security. There is a need to implement biometric authentication using EEG for these reasons.

Research on EEG authentication has already been conducted in many fields, and it has been shown that EEG gives different characteristics depending on the individual [9]. In addition, various studies have been conducted on the features and classification methods that can be used for EEG authentication, and many effective methods have been proposed [10]. However, the authentication accuracy is not sufficient, and it is not at the stage where it can be put to practical use like fingerprint authentication. The first factor is the lack of accuracy in the authentication of single features. However, studies have shown compelling features, which shows that it is difficult to identify an individual’s EEG with a single feature. The second issue is missing data due to temporary noise. Missing data due to errors in the measurement equipment can be solved by re-measuring the data. However, it is difficult to determine the missing data when temporary noise is introduced into the data. To avoid this problem, it is expected to reduce the probability of false recognition by dividing the measurement data into several parts, processing them, and judging the results comprehensively.

This study uses a multichannel electroencephalograph to obtain more personal characteristics. Since multichannel EEGs are very expensive and require specialized knowledge for measurement, most of the existing EEG studies use EEGs with only one to three channels of electrodes. However, with the development of electroencephalographs, many inexpensive multichannel electroencephalographs that individuals can use daily have become available. The use of multichannel electroencephalography is expected to improve the technology of EEG authentication since more complex EEG information can be obtained.

Therefore, this doctoral thesis proposes a highly accurate authentication system by combining multiple features obtained from a multichannel electroencephalograph and comprehensively judging the results. The performance of the proposed system is evaluated based on the Equal Error Rate (EER) and the classification rate, which is used in biometric authentication. These results are compared with existing research results to examine the efficacy.

BIOMETRIC AUTHENTICATION TECHNOLOGY

With the development of the Internet of Things (IoT) technology [11], the opportunities to handle various information on the Internet increase every year. Therefore, society's attention is focused on privacy protection. It is crucial to implement a system where only authorized persons can handle the information to protect private information. Therefore, it is necessary to improve authentication techniques for personal identification. There are three types of personal

ISSN 2663 - 4023

authentication: knowledge authentication, property authentication, and biometric authentication, each of which has its advantages and disadvantages. In this doctoral dissertation, we will discuss biometric authentication since EEG is the subject of this dissertation.

Types of Personal Authentication

Personal authentication can be divided into three types depending on the use target. These are knowledge authentication based on the user's knowledge, such as passwords and PINs; property authentication based on the user's possession, such as cards and keys; and biometric authentication based on the user's unique characteristics, such as fingerprints, irises, and handwriting. An overview of each type of personal authentication is given below.

Knowledge authentication is a personal authentication method based on knowledge stored only by the user. The authentication is based on matching the identification information such as user ID and the corresponding password. However, the user can forget passwords and PINs and can be guessed by the name, birthday, phone number, brute force attacks, and dictionary attacks.

Property authentication is a personal authentication method based on objects owned only by the individual.

The authentication can be done using a push card, a contactless IC card for access control, or a hardware token. Compared to knowledge authentication, this method does not require memory or input and can use more specific information, improving security. However, because of problems such as card theft and counterfeiting, it is often used in combination with knowledge authentication.

Biometric authentication is a method of authenticating a person using biometric information. The first application of biometric authentication appeared in criminal investigations, where Bertillon invented the Bertillon anthropometric method [12] in France in 1882. This method identifies criminals by measuring 14 points, such as the height and length of the legs. However, when the number of offenders is large, it has been found that 14 measurements are not enough to identify an individual. Fingerprint authentication was introduced as a new biometric authentication method in the early 20th century.

The biometric information used for biometric authentication has the following three conditions.

The Berthillon anthropometric method does not satisfy the above conditions, and therefore, it is not considered to function as a personal authentication technology. The ideal biometric satisfies all three of these conditions, but there is no such biometric. In the case of biometric authentication, it is necessary to use different biometrics depending on the purpose. In the case of biometric authentication, biometric information such as fingerprints, iris, and veins is not determined by DNA sequence for identical twins. Thus the uniqueness is maintained even when the genes are entirely identical.

Biometric authentication has the following two advantages. First, it can provide a highly convenient method of identification. Since there is no need to recall passwords or prepare IC cards at the time of authentication, there is no possibility of forgetting or losing them. Second, the accuracy of the identification can be adjusted depending on the system. Usually, a person's identity in biometric authentication is determined by the similarity between the registration data and the input data. Therefore, by adjusting the threshold of the similarity, the system can provide security and convenience according to the purpose of the system.

ISSN 2663 - 4023

Typical Biometric Authentication

Biometric authentication is performed using biometric information that includes physical and behavioral characteristics. Physical characteristics are always associated with the person, and behavioral characteristics are the habits of the person. Both of them can be reproduced by the person himself. Authentication based on physical features is more accurate than authentication based on behavioral features. However, since it is difficult to change the template, secure authentication becomes problematic if the biometric information is forged or stolen. On the other hand, behavioral features have lower authentication accuracy than physical features but are relatively secure because the template can be changed even if the information is forged. Although there are many biometric authentication methods in practical use, there is no biometric authentication method that satisfies all the requirements, so it is necessary to use different methods depending on the case.

AUTHENTICATION BY PHYSICAL CHARACTERISTICS

Authentication by physical characteristics refers to authentication using the shape of the body. Typical biometric authentication techniques are fingerprint, vein, iris, face, and hand geometry. In the following, we will introduce each of these authentication techniques.

Fingerprint authentication is the most famous biometric authentication. The history of fingerprint authentication is ancient, and it is thought that it started in the 16th century. Since fingerprints are unique to each individual and remain unchanged throughout their lives, it satisfies uniqueness and permanence. The Meinuysha and frequency analysis methods have been adopted for fingerprint authentication [13]. Figure 1 shows the Meinuysha method and the frequency analysis method. The left figure shows the Meinuysha method, and the correct figure shows the frequency analysis method. A Meinuysha is a feature point, which is a general term for an endpoint where a line ends or a branch point where a line branches. In the Meinuysha method, the number of coincidences of these feature points' position, type, and direction is used for authentication. Because of the image processing complexity, the matching process takes time, but it is possible to authenticate even with rough input. However, there are 1–3% of people whose fingerprints are rejected due to dryness or roughness of the fingers.

In addition, we have developed a method using both the Meinuysha method and the frequency analysis method. There is no rejection of fingerprint registration, and all people can use the method while the processing time is short. On the other hand, the frequency analysis method considers the cross-section of a fingerprint slice as a waveform and uses frequency analysis as the feature value (Fig. 1).

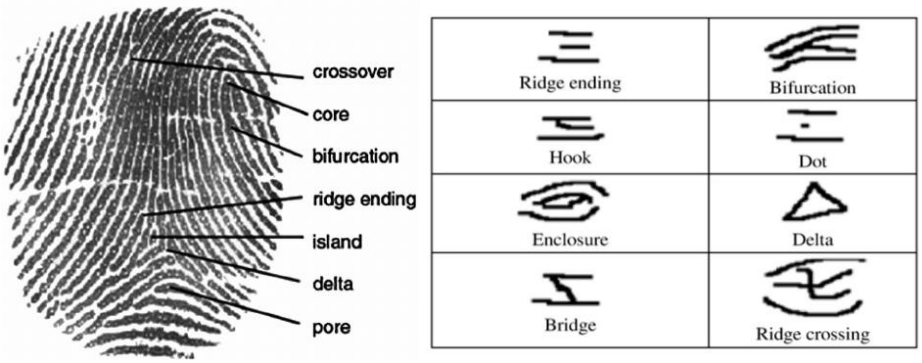

Fig. 1. Fingerprint authentication

ISSN 2663 - 4023

There is an authentication method using a hybrid method [14], which has become the mainstream of fingerprint authentication. Since fingerprint authentication requires only a fingertip, the device can be miniaturized and applied to various devices. In addition, unlike other biometric methods, fingerprints are left on an object when it is touched, which has the advantage that it can be used for authentication when the person is not present, such as in criminal investigations. However, fingerprint authentication makes it possible to use a severed finger for spoofing authentication. Therefore, in addition to fingerprint authentication, a method to determine whether a person is alive or dead by scanning the finger has been developed. In this method, only the finger of a living person can be used for authentication. Examples of the use of fingerprint authentication include PC login systems, cell phone owner authentication, and immigration procedures.

Vein authentication is a general term for authentication using the veins on the back of the hand, the palm, and the finger veins. Since the patterns of veins and arteries are generated randomly, no two people have the same pattern, thus satisfying uniqueness and permanence. In addition, arteries run deep in the body, while veins run on the body's surface and can be collected as images. The near-infrared light is absorbed by hemoglobin in the blood and reflected by the skin so that the veins are raised in the image when irradiated. From the vein images, patterns are extracted, and the positions of the vein branches and other features are used for authentication. The first use of vein authentication was based on the veins on the back of the hand. However, since it is impossible to obtain veins from people with fat or hairy hands, new palm and finger veins methods have been developed. Palm vein authentication is shown in Fig. 2 [15]. The left figure shows the features obtained by palm vein authentication. The obtained vein pattern image is used for pattern matching.

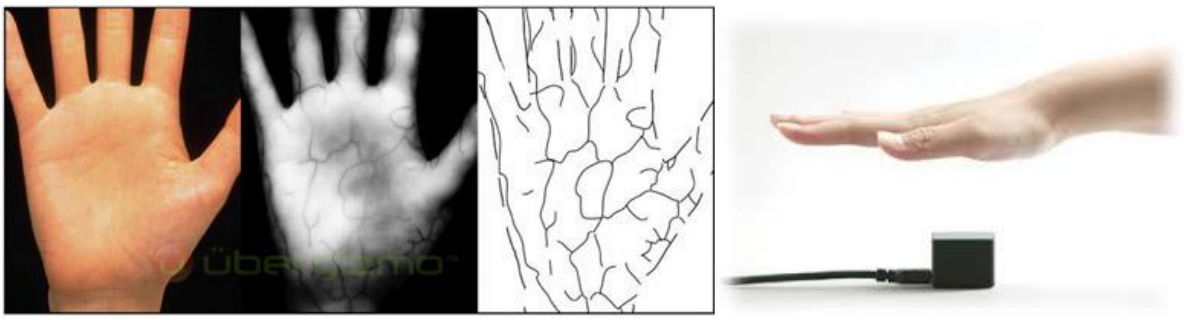

Fig. 2. Palm vein authentication

Next, the finger vein authentication is shown in Fig. 3 [16]. The correct figure shows Fujitsu's palm vein authentication system [15]. Because veins are internal body information, they are highly confidential and are not affected by changes over time or physical conditions, so they can always be authenticated with high accuracy. At the same time, the presence or absence of blood flow can be checked to determine whether a person is alive or dead. Because of the above advantages, this system is mainly used in ATMs of banks. It is also used for access control and PC login systems.

ISSN 2663 - 4023

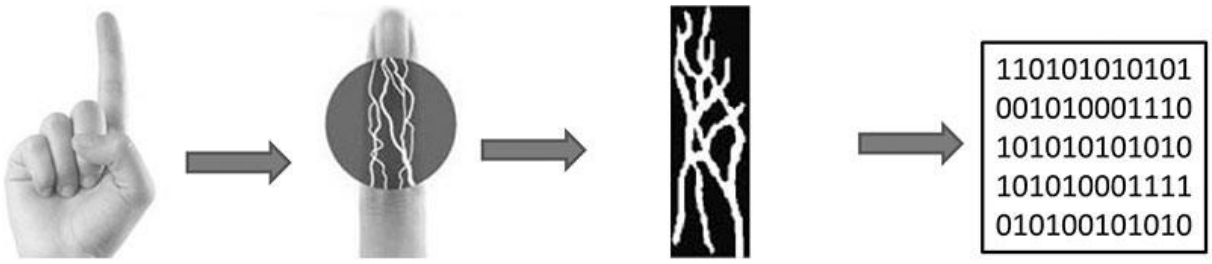

Fig. 3. Finger vein authentication

The first step in the authentication process is to obtain an iris image by irradiating infrared light. The iris is located on the eye's surface, and a random pattern is generated when the child is about two months old. The iris is divided into sections, and the patterns are classified and coded for each section.

Fig. 4. Iris recognition

The authentication is done by comparing these codes. The left figure in Fig. 4 shows the position of the iris in the eye, and the correct figure is an example of the coded iris pattern [17]. As with fingerprints, the iris pattern is used for office access control and immigration procedures. It has been installed in cell phones in recent years for owner authentication. In recent years, mobile phones have been used to authenticate the phone's owner. However, there have been cases where the iris was printed on a contact lens for identity theft due to the inability to determine the survival of the target.

The first large-scale experiment of face-based personal authentication was conducted at the Osaka World Exposition in 1970. There are two main types of face recognition algorithms: the first is a method that extracts features from face images and compares them. The second method is to generate a standardized face image from many face images and compare it with individual face images. For example, there was research on Facebook's face recognition technology “DeepFace” [18] in 2014. By constructing a frontal image from the faces in the image using 3D modeling technology and analyzing the common points using deep learning, the recognition rate is almost the same as that of a human. However, the recognition accuracy may be significantly lower if the facial expression is different, part of the face is hidden, the beard is extended, the person is wearing sunglasses, etc. In addition, face recognition requires re-registration after several years.

There is biometric authentication that uses the shape of the hand. It uses finger length, hand width, and hand thickness as features for authentication. Although there is not much difference in hand shape between individuals, the amount of data required is small, so it is often used in simple systems.

ISSN 2663 - 4023

Other biometric parameters include ear shape, genes, body odor, heart rate, pulse wave, distribution of sweat glands, location of blind spots, and EEG.

AUTHENTICATION BY BEHAVIORAL CHARACTERISTICS

Behavioral authentication refers to authentication using behavioral habits. Typical biometric authentication methods are voice and handwriting. This section introduces each type of authentication.

Voice authentication is a technology that uses the characteristics of the human voice for authentication. In the fixed-text type, a user registers the utterance of a specific word in advance, and the user is authenticated when that word is uttered. In the free text type, the user registers the utterance of various words in advance, and the authentication is performed just by talking. These methods have the possibility of spoofing authentication by recording the voice of the authenticator. However, since the recorded voice is not the same as the spoken voice, it is possible to distinguish between the two strictly. However, if the sound quality of the registered data is poor, it isn't easy to distinguish between them.

For this reason, the "text-specified" method has been developed. In this method, the system specifies the words to be used for authentication on a case-by-case basis, and it isn't easy to record the voice in advance. However, in both methods, the authentication rate may drop significantly when the authenticator has a cold or a lot of noise. In the authentication system, a sound spectrogram, representing a sound signal as a time-frequency distribution, is registered as a pattern and matched to an individual. An example of an application is the access control of an apartment building.

Handwriting recognition is mainly applied to personal authentication at the signature and is widely used in Europe and the United States. The accuracy of handwriting authentication is improved by using the shape of the letters and the speed, pressure, and position of the pen in the air as features of the handwriting.

In addition, authentication technologies using behavioral features such as walking and essential touch are being studied.

BIOMETRIC AUTHENTICATION

The processing procedure for biometric authentication can be generalized. Research has been conducted based on this procedure, and various authentication methods depend on the biometric data used. Therefore, it is necessary to have a method to evaluate the performance of these methods.

Process Steps for Biometric Authentication

The biometric authentication system consists of an enrollment phase and an authentication phase. The procedure of the authentication system is shown in Fig. 5. The following information is the procedure.

ISSN 2663 - 4023

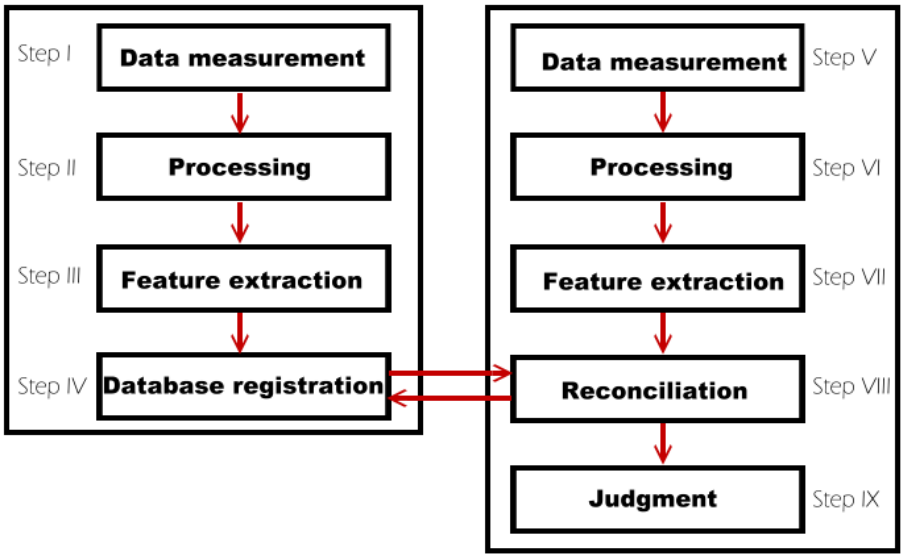

Fig. 5. Biometric authentication procedure

Registration Phase:
Step 1. Data measurement
Step 2. Processing
Step 3. Feature extraction
Step 4. Database registration
Authentication Phase:
Step 5. Data measurement
Step 6. Processing
Step 7. Feature extraction
Step 8. Reconciliation
Step 9. Judgment

In the enrollment phase, the biometric information of the user is registered. In Step 1, biometric data is required for authentication using sensors. In Step 2, we preprocess the measured data. In Step 3, appropriate signal processing is applied to the preprocessed data to extract the person's unique features. The features vary depending on the biometric data used. In Step 4, the extracted features are registered in the database. In this way, it completes the registration phase. These processes are usually performed only once when the authentication system is registered.

In the authentication phase, the system determines whether or not the data applied is that of a user registered in the authentication system. As in the registration phase, data measurement is performed in Step 5, preprocessing is applied in Step 6, and features are extracted in Step 7. In Step 8, the database generated in the registration phase is accessed, and the features obtained in the authentication phase are compared and checked. In Step 9, the person's identity is determined based on the similarity calculated from the matching results.

These processes are performed every time, and only then is an authentication counted as performed. The details of each process are described below.

Data measurement is performed in Steps 1 and 5. Here, the physical or behavioral characteristics of the user using the authentication system are measured using dedicated sensors. The information to be acquired varies depending on the feature value, such as signals, images,

and videos. In addition, different measurement methods may exist even for the same feature. For example, in the case of fingerprint authentication, there is five mainstream methods: optical, thermal, pressure-sensitive, capacitive, and electric field.

Preprocessing is performed in Steps 2 and 6. The data obtained by data measurement usually contains noise. In order to efficiently extract the information necessary for authentication, noise removal is required. There are two types of noise included in biometric data: noise caused by the environment and noise caused by the living body. Environmental noise includes high-frequency noise from digital equipment, low-frequency noise (50/60Hz commercial AC noise), and electrostatic noise generated by rubbing of clothing. The noise originating from the living body is biological information other than the target. These noises can be removed by applying a moving average, median, or bandpass filter to the measurement data.

Feature extraction is performed in Steps 3 and 7. From the preprocessed measurement data, the appropriate features are extracted.

Extraction of Features

Determining feature values is one of the most critical factors in authentication systems. If a feature with high similarity between the user and another person is selected, it becomes tough to determine the user's identity. For this reason, there are multiple methods for feature extraction even when the same biometric information is used, and various methods have been studied to extract better features [10]. For example, the Meinuysha method uses multiple feature points obtained from the fingerprint image in fingerprint authentication. The frequency analysis method considers the cross-sectional view of the fingerprint image as a waveform. Hybrid methods that combine these methods have also been studied.

Database registration is performed in Step 4. The features obtained in Step 3 of the registration phase are stored as the user's template in the database. The user's identity is determined by comparing it with the user's template registered in the database. For this purpose, the template is often created by performing multiple data measurements and using the data with the slightest noise or the average value of the multiple measurements.

The matching is performed in Step 8. The similarity between the template registered in advance and the authentication data measured in Step 5 is calculated. To calculate the similarity, the distance between the features is used. The most commonly used distance is the Euclidean distance. The smaller the Euclidean distance, the higher the similarity, and thus the higher the likelihood that the person is the same as the template.

On the other hand, if the Euclidean distance is significant, the similarity is low, and the possibility that the person is a stranger is high. Some methods use machine learning, such as support vector machines [19] and neural networks [20], to determine the discriminative boundary between classes and match based on the distance from the boundary. Other methods include the Hamming distance obtained by XOR calculation, the Cosine distance, which represents the angle between vectors, and the Effective distance based on the correlation between multiple variables. The Hamming distance is used in iris recognition.

The decision is made in Step 9. Here, a judgment is made as to whether or not the person is the same as the template, based on matching the template with the input data. A threshold value predetermined for each system is used for the judgment. If the similarity result is less than the threshold, the input data is judged to be that of a different person from the template, and the authentication request is rejected. On the other hand, if the result is above the threshold, the

input data is judged to be the same person as the template, and the authentication request is accepted.

PERFORMANCE EVALUATION OF BIOMETRIC AUTHENTICATION

Biometric authentication determines a person's identity based on the degree of similarity between the template registered in the system and the input data. Fig. 6 shows the similarity between the template and the input data.

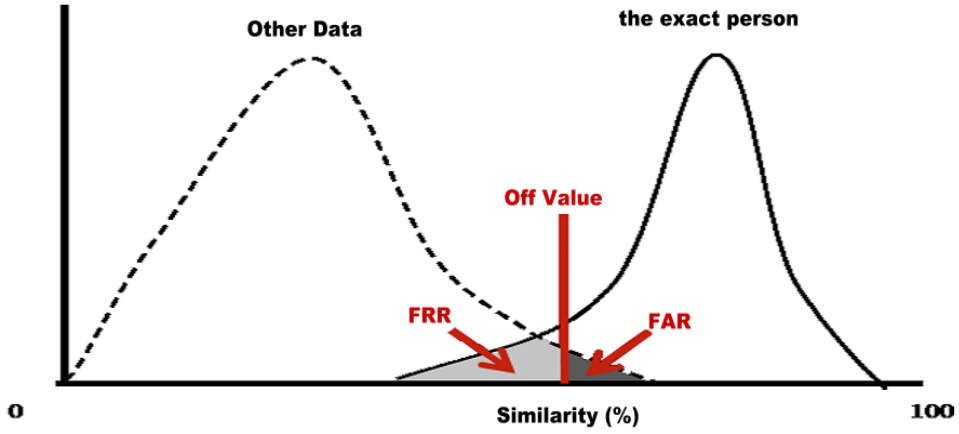

Fig. 6. Distribution of similarity

This figure shows the distribution of similarity. The horizontal axis shows the similarity as a percentage, and the vertical axis shows the frequency of the data. The dotted line graph shows the similarity distribution when the input data is someone else's data. The solid line graph shows the similarity distribution when the input data is the user's data. When the features do not match at all, the similarity is 0%, and when they match perfectly, the similarity is 100%. Even in the case of personal data, it is rare for the feature values to match perfectly. The surrounding environment, such as perspiration and humidity, may degrade the biometric data quality. In addition, other people's data may have a relatively high degree of similarity or may not match at all. It is ideal for drawing a graph that separates the distributions of other people's data and the user's data. However, in many cases, overlaps occur in the boundaries of the graph.

A threshold value is used to determine the similarity between other people's data and users' data. The percentage of personal data with lower similarity than the threshold is defined as the False Rejection Rate (FRR). The percentage of stranger data with higher similarity than the threshold is defined as the False Acceptance Rate (FAR). Fig. 6 shows the range of FRR and FAR, which is supposed to be the person but not the person, and FAR, which is thought to be the person despite being another person, intersects. FRR and FAR are trade-offs. Since there is a trade-off between FRR and FAR, it is essential to set the threshold value according to the system. For example, in the case of financial systems, it is necessary to emphasize security over convenience. Therefore, a threshold value that requires a high degree of similarity should be set for authentication systems.

The performance of biometric authentication is generally evaluated by Equal Error Rate (EER) and Receiver Operating Characteristics (ROC) curves. The evaluation values of both are obtained from FRR and FAR. Fig. 7 shows a graph representing the performance evaluation.

ISSN 2663 - 4023

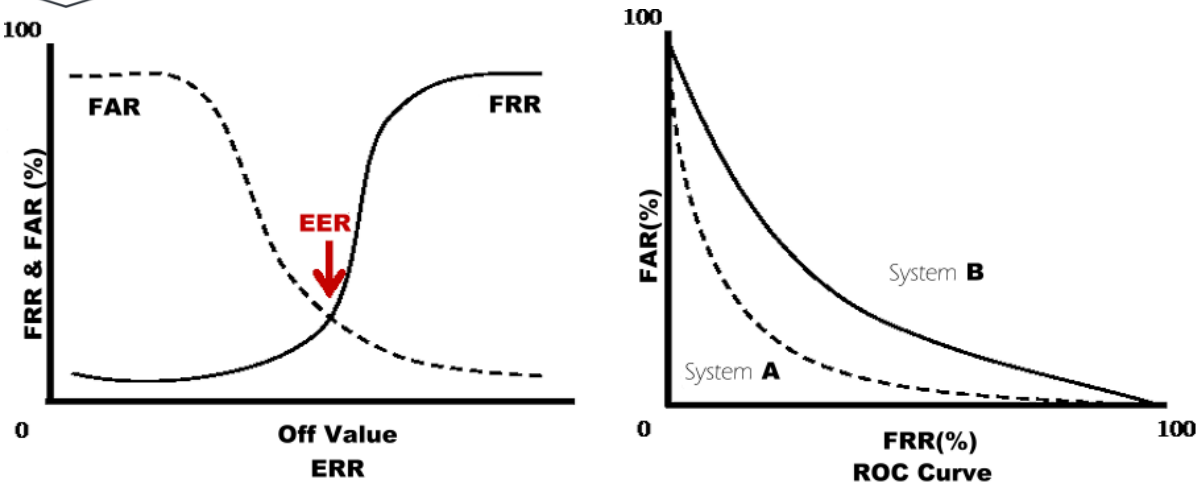

Fig. 7. Performance evaluation method

A graph for calculating the EER is on the left in Fig. 7. The horizontal axis shows the threshold value, and the vertical axis shows the FAR and FRR values as percentages. The dotted line graphs show the FAR and FRR values when the threshold is changed, respectively. The FAR decreases as the threshold value increases, while the FRR increases as the threshold value increases. The intersection of these two graphs is the EER, which is used as the evaluation value of the system.

Next, the ROC curve representing the authentication accuracy of systems A and B is shown in Fig. 7. The horizontal axis represents FRR, and the vertical axis represents FAR. The ROC curve is obtained by plotting the value of FAR corresponding to FRR. When comparing Systems A and B, System A has lower values for both FRR and FAR, which indicates higher authentication accuracy.

According to the ROC curve, when FRR > FAR, the system is used for systems requiring a high-security level. When FAR > FRR, the system is used for criminal investigations where the probability of missing a person is reduced.

ELECTROENCEPHALOGRAPHY DATA

The EEG is not always constant but changes with various internal and external stimuli. For this reason, EEG authentication in all measurement conditions has been studied. The EEGs used for authentication are mainly classified into resting and task EEGs.

The method of using resting EEG has been used in the literature [21,22]. Resting EEG refers to EEG measured in a relaxed state, and these EEGs are used for authentication. The resting EEG often shows strong alpha waves, the background EEG. The alpha waves are more easily observed with closed eyes and suppressed by opening the eyes. In addition, body movements such as walking cause noise in the EEG, so it is often measured in a sitting position. The advantage of using resting EEG is that it does not require any stimulus or a task, so authentication is easy and quick.

The disadvantage is that the EEG of the authenticated person is used as it is. This is the same as for authentication using physical characteristics other than EEG. The disadvantage is that since the EEG of the authenticator at rest is used as it is, even if the authenticator is forged, the authenticator's registration data cannot be changed.

The first is a method that uses EEG during mental tasks. Mental tasks include calculation, writing, reading, and imagery. The first is a method that uses brain waves during mental tasks. The second method uses EEGs for external stimuli such as images and sounds. For authentication, evoked potentials such as visual evoked potentials and event-related potentials are used. In the case of using EEG during a task, it is possible to change the enrollment data of the authenticator by changing the task, even if it has been forged once. However, it takes extra time to perform the task than the resting EEG authentication. Furthermore, using EEG during external stimulation requires a device for stimulus presentation.

In addition to the classification of resting EEG and task EEG, studies of EEG authentication have differed in the number of electrodes of the EEG machine used. So far, EEG authentication has been divided into two categories: studies using electroencephalographs with three or fewer installed electrodes [21,23] and studies using electroencephalographs with more than three installed electrodes [24,25]. Most of the studies were conducted on the condition with a small number of electrodes. This may be because at that time, multichannel electroencephalography was expensive and specialized, used only in the medical field, and needed to be worn and measured by specialists. However, many multichannel electroencephalographs that can be used daily have been developed, increasing the number of channels.

It is expected that more research will be conducted on EEG. A 32-channel electrode can be applied in five minutes, while a 256-channel electrode can be applied in 15 minutes. The use of a multichannel electroencephalograph will help to improve the accuracy of authentication because more features can be obtained. It is necessary to develop an authentication method that utilizes multichannel EEG in EEG authentication.

Electroencephalography Feature Extraction

In EEG authentication, extraction methods of features obtained from EEG data have been studied. The proposed feature extraction methods are categorized into spectral information, correlation information, and others [21]. Fig. 8 shows a graph of the literature's frequency of use of existing feature extraction methods [10].

Since spectral information is the feature that represents the most characteristic of EEG, it was the central study in this paper.

In the existing studies, it has been used in [21–23,25–27]. Spectral information can be obtained from frequency analysis such as Fourier transform and wavelet transform. The Fourier transform is a method of representing time series data in the frequency domain. The wavelet transform is a frequency analysis method that considers the time domain, which the Fourier transform cannot represent using wavelets. The features used as spectral information are mainly power spectrum, amplitude spectrum, phase spectrum, and energy spectrum. These spectra are obtained from the EEG data of each channel, and the differences between the left and right hemispheres are also used as features.

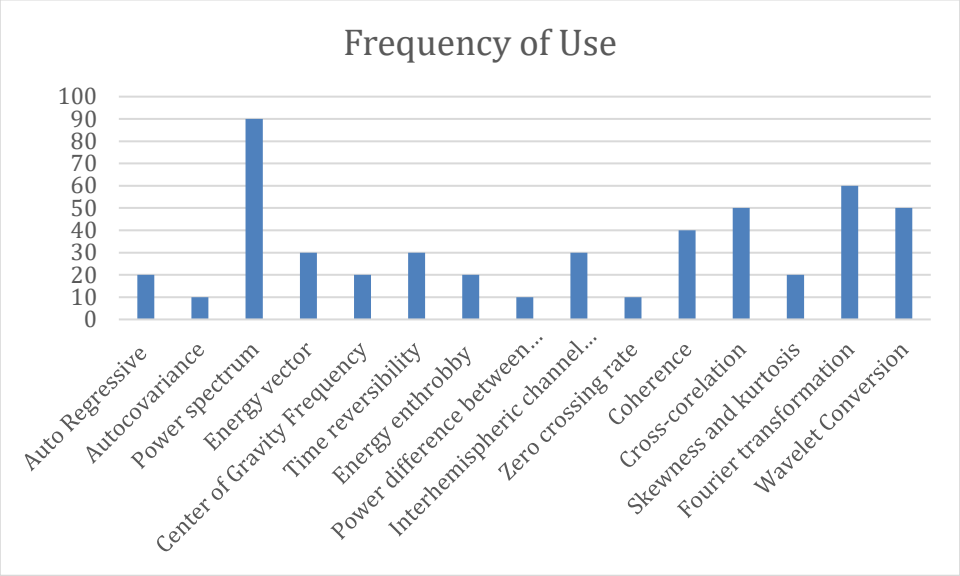

Fig. 8. Feature extraction methods frequency of use

Correlation information is a feature that represents the correlation between two-time series data. In the case of authentication using a multichannel electroencephalograph (EEG), many studies have been conducted using the correlation information of the EEG data obtained from two electrodes as the feature value. The existing studies are used in the literature [21,22]. Correlation information includes coherence, cross-correlation coefficient, and mutual information. Coherence is a feature that describes the relationship of phase and amplitude between data. Cross-correlation coefficients and mutual information are the methods to evaluate the similarity between data. The cross-correlation coefficient is a feature that evaluates linear relationships, and the mutual information quantity is a feature that evaluates the dependency between data based on information theory.

As for other information, many studies use Auto-Regressive (AR) models. The AR model is used to analyze time-series data, and it represents the current data by adding weights to the past data. It is assumed that the EEG data of each channel is generated from the AR model, and the obtained AR coefficients are used as features. References [21] can be found among the existing studies. Other features used in existing studies include autocovariance, which represents the variability of time-difference data; center-of-gravity frequency, which represents the position of the center of gravity of the integrals obtained from frequency analysis; time inversion, which represents the asymmetry of interelectrode data; zero-crossing property, which is a measure of periodicity and whiteness of data; and skewness and kurtosis, which represent the shape of the probability distribution of data. Skewness and kurtosis, which describe the shape of the probability distribution of the data, have been investigated [10].

Electroencephalography Matching

This section describes EEG matching methods. The existing methods for EEG authentication often use class classification methods for matching. The most common feature classification methods use machine learning to classify the input data. Supervised learning methods such as k-nearest neighbor methods, discriminant analysis, neural networks, and support vector machines are the most common machine learning methods used for authentication.

In the following, we introduce each learning method separately. The *k* Nearest Neighbor algorithm (kNN) [28] is the most straightforward machine learning algorithm. kNN classifies the test data by majority voting using the *k* data closest to the test data schematic diagram shown in Fig. 9. The test data is classified into class 1 if $k = 3$ but into class 2 if $k = 7$. The procedure of the algorithm is shown below.

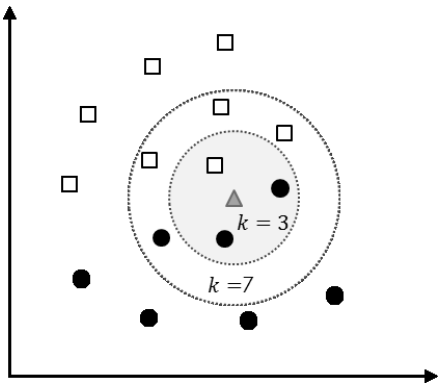

Fig. 9. k-schematic diagram of the nearest neighbor method

Procedure k1. Determination of parameter *k* value.
Procedure k2. Similarity calculation procedure using each feature of training and test data.
Procedure k3. Sorting of the training data based on the similarity.
Procedure k4. Selection of *k* neighboring training data.
Procedure k5. Vote by the majority for the selected training data class.
Procedure k6. Classify the most classes as test data classes.

Find *k* that minimizes the generalization error by cross-validation or other methods. In Procedure k1, it is necessary to select the optimal *k* value. In Procedure k2, we calculate the similarity between the features extracted from the training and test data. To calculate the similarity, mainly Euclidean distance, and Manhattan distance are used.

In Procedure k3, the test data and the training data are sorted in order of increasing similarity. In Procedure k4, the k training data with the highest similarity to the test data are selected. In Procedure k5, we perform majority voting on the classes of the training data selected in Procedure k4. Finally, in Procedure k6, the test data is classified into the training data class with the highest number of votes in Procedure k5.

Discriminant Analysis (DA) [29] is an analytical method for classifying multivariate data and is the most classical pattern recognition method. Discriminant analysis is also called multiple discriminant analysis or canonical discriminant analysis. There are two types of discriminant analysis: discriminant analysis by discriminant function and discriminant analysis by distance. Discriminant analysis by discriminant function is divided into discriminant analysis by a linear function and a non-linear function. When the boundary of a class is a straight line or a hyperplane, linear discriminant analysis (LDA) uses a linear function. Equivariance is required for linear discriminant analysis. When the boundary of a class cannot be expressed by a linear function, such as a curve or hypersurface, quadratic discriminant analysis (QDA) is used to discriminate using a quadratic function such as an ellipse. For discriminant analysis by distance, the Effective distance is the mainstream method. This section describes Fisher's linear analysis [30], a type of linear discriminant analysis. In linear discriminant analysis, the feature vector $\boldsymbol{x}$ is multiplied by the weight vector, and the value $z = \boldsymbol{wx}$ is used to find the $\boldsymbol{w}$ that separates the two classes the most. $z = \boldsymbol{wx}$. For this purpose, the within-class variance-covariance matrix *Swc* and the between-class variance-covariance matrix.

ISSN 2663 - 4023

The method of determining $\boldsymbol{w}$ that maximizes Sbc/Swc, the ratio of Sbc, which maximizes the ratio Sbc/Swc, is Fisher's linear analysis.

First, calculate the within-class variance-covariance matrix Swc and between-class variance-covariance matrix Sbc of the training data.

To maximize Sbc/Swc, find the maximum eigenvalue of Swc -1 to find the maximum eigenvalue of Sbc. The eigenvector at that time is $\boldsymbol{w}$

A neural network (NN) [20] is a method that models the brain's neurons. There are multiple nerve cells called neurons in the brain, and information is processed by sending and receiving signals between neurons. A neural network is a method of reproducing this mechanism in a computer. Backpropagation, also called error backpropagation, is a feed-forward model consisting of an input layer, an intermediate layer, and an output layer. A schematic diagram is shown in Fig. 10. Backpropagation is a method of learning parameters. The error between the output and target values given as supervisory data is minimized. The procedure is as follows. First, initialize all the weights and put the input values of the supervised data into the input layer. The resulting input layer

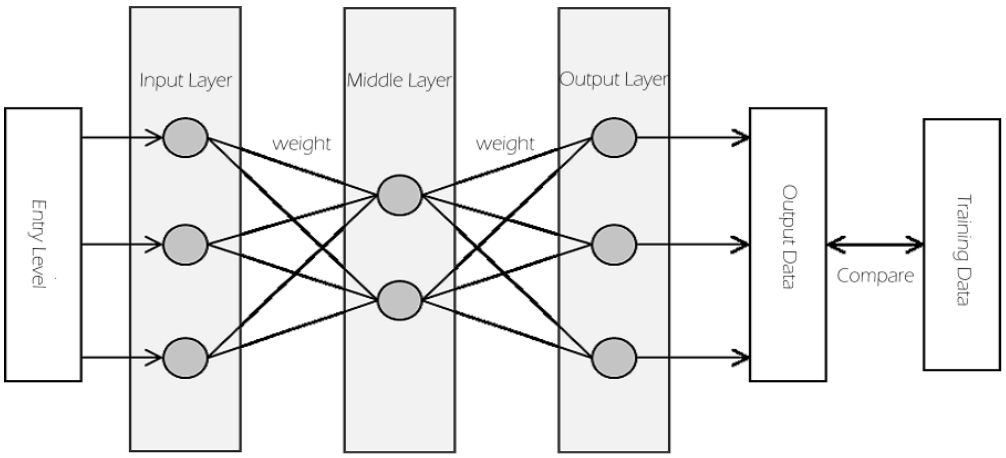

Fig. 10. Schematic diagram of backpropagation

To obtain the value of the middle layer. Similarly, the values of the intermediate layer are weighted to obtain the values of the output layer. In this case, the sigmoid function is mainly used as the output function of the intermediate layer and the output layer. Next, the error of the output layer is calculated from the target value of the training data and the value of the output layer. The error of the intermediate layer is calculated from the error of the output layer and the value of the intermediate layer. The weights and thresholds are updated from these errors in the output and intermediate layers. The above process is repeated for all the training data, and learning is completed when the mean square error is minimized. Neural networks have been applied to pattern recognition and data mining. Research using neural networks can be found in the literature [23,25].

Support Vector Machine (SVM) [19] is considered the best pattern discriminator of the two classes. Support Vector Machines are characterized by margin maximization and kernel trick. Margin maximization makes it possible to construct a discriminator with high discriminative performance even for untrained data. In addition, the kernel trick can be used for problems where linear separation is not possible. The main kernels are the linear kernel, the polynomial kernel, the radial basis function kernel, and the hyperbolic tangent kernel. Furthermore, by extending the two-class classification, multi-class classification can be supported. Research using support vector machines can be found in [22].

CONCLUSION AND FUTURE WORK

After reviewing available authentication methods and technologies, we proposed brain wave authentication based on EEG signals by using feature extraction and machine learning.

As described in the article, many studies using EEG have been conducted worldwide. However, EEG authentication technology has not been established at present, and the accuracy of authentication is not sufficient. In this study, we aim to improve the accuracy of EEG authentication to establish the technology. This article proposes an EEG authentication system to improve authentication accuracy. In this study, we aim to improve the accuracy of the EEG authentication technology to establish it. The following two factors have contributed to the low authentication accuracy in existing research results:

1. Lack of authentication accuracy for single features.
2. Missing test data due to temporary noise, etc.

The first is that the authentication accuracy of a single feature is insufficient. Although various features that are effective for EEG authentication have been studied in existing research, the accuracy of authentication using a single feature is low. In this paper, we propose a method to improve the accuracy of EEG authentication by combining multiple features. We propose a matching method.

The second factor is the degradation of authentication accuracy due to missing measurement data. Apparent missing data, such as a malfunction of a measuring instrument, can be solved by requesting another measurement. However, it is challenging to determine insufficient data due to temporary noise contamination as missing data. For this reason, it is possible to use insufficient data that contains noise for authentication. In this case, there is a high possibility that the noise will interfere with the feature extraction, and the data will be judged as not being the person's data, even though it is the person's data. We propose a method to reduce the probability of false recognition due to temporary noise by comprehensively judging the results of all the split data. Therefore, we split the measurement data into several parts and perform authentication using each part of the data.

The solution derived from these two factors related to the degradation of authentication accuracy is as follows:

1. Combining multiple features by ensemble learning.
2. Comprehensive judgment by dividing the measurement data.

The proposed authentication system, which aims to improve the accuracy of EEG authentication, is based on the above two solutions. In addition, our goal is to make the EEG measurement required for authentication as short as possible. In order to achieve this goal, we will use resting EEG, which does not require mental tasks or external stimuli, to perform authentication.

REFERENCES

1 Kawato, M. (2008). Brain-Network Interface. Journal of the Institute of Electronics. *Information and Communication Engineers*, 91(2), 123–130.

2 Hotson, G., et al. (2016). Individual Finger Control of a Modular Prosthetic Limb using High-Density Electrocorticography in a Human Subject. *Journal of Neural Engineering*, 13(2), 026017. doi:10.1088/1741-2560/13/2/026017

3 Tanaka, K. (2012). Development of a Wheelchair Moved by Brain Wave Commands (Special Issue on the Forefront of Robotics for Supporting People). *Journal of the Japan Society for Precision Engineering*, 178(81), 662–665.

4 Rao, R. P. N., et al. (2014). A Direct Brain-to-Brain Interface in Humans. *PLoS ONE*, 9(11), e111332. doi:10.1371/journal.pone.0111332
5 This Place. MindRDR. http://mindrdr.thisplace.com/static/index.html
6 Armstrong, B. C., et al. (2015). Brainprint: Assessing the Uniqueness, Collectability, and Permanence of a Novel Method for ERP Biometrics. *Neurocomputing*, 166, 59–67. doi:10.1016/j.neucom.2015.04.025
7 Komatsu, N., Uchida, K., Ikeno, S., and Sakano, S. (2008). The Story of Biometrics, Japanese Standards Association.
8 Thorpe, J., van Oorschot, P. C., and Somayaji, A. (2005). Pass-thoughts. Proceedings of the 2005 Workshop on New Security Paradigms—NSPW'05. doi:10.1145/1146269.1146282
9 Ito, S., Mitsukura, Y., Fukumi, M., and Akamtsu, N. (2004). Proposal of the EEG Analysis Method Using the Individual Characteristic of the EEG. *IEEJ Transactions on Electronics, Information and Systems*, 124(6), 1259–1266. doi:10.1541/ieejeiss.124.1259
10 Kumari, P., and Vaish, A. (2014). Brainwave based Authentication System: Research Issues and Challenges, *International Journal of Computer Engineering and Applications*, IV(I&II), 89–108.
11 Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A Survey. *Computer Networks*, 54(15), 2787–2805.
12 Watanabe, K. (2003). The Birth of Judicial Identity: Individual Identification and Registration in Civil Society, Kotososha.
13 Hoshino, Y. (2005). Fingerprint Authentication Technology—Biometric Security, Tokyo Denki University Press.
14 Toshiba. Fingerprint Authentication. http://www.it-serve.co.jp/products/security/fingerprint_attest.htm
15 Fujimori. Palm Vein Certification. http://www.fujitsu.com/jp/group/frontech/solutions/business-technology/security/palmsecure/
16 Hitachi. Finger Vein Authentication. http://www.hitachi-ics.co.jp/product/virsecur/vein/secure_sol.html
17 Fushidori. Iris Certification. http://atfe.fmworld.net/at/report/?id=320
18 Taigman, Y., Yang, M., Ranzato, M., and Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. 2014 IEEE Conference on Computer Vision and Pattern Recognition. doi:10.1109/cvpr.2014.220
19 Cristianini, N. and Shawe-Taylor, J. (2005). Introduction to Support Vector Machines, Kyoritsu Publishing Co.
20 Kumazawa, I. (1998). Learning and Neural Networks, Morikita Publishing Co.
21 Riera, A., et al. (2007). Unobtrusive Biometric System Based on Electroencephalogram Analysis. *EURASIP Journal on Advances in Signal Processing*, 2008 (1). doi:10.1155/2008/143728
22 Ishikawa, Y., et al. (2015). A Personal Classification Method Using Spatial Information of Multi-channel EEG. International Conference on Parallel and Distributed Processing International Conference on Parallel and Distributed Processing Techniques and Applications, 1, 229–235.
23 Hema, C. R., Paulraj, M. P., and Kaur, H. (2008). Brain Signatures: A Modality for Biometric Authentication. 2008 International Conference on Electronic Design. doi:10.1109/iced.2008.4786753
24 Marcel, S., and R. Millan, J. (2007). Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 743–752. doi:10.1109/tpami.2007.1012
25 Palaniappan, R., and Mandic, D. P. (2007). Biometrics from Brain Electrical Activity: A Machine Learning Approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 738–742. doi:10.1109/tpami.2007.1013
26 Nakanishi, I., Fukuda, H., and Li, S. (2013). Biometric verification using brain waves toward on-demand user management systems. Proceedings of the 6th International Conference on Security of Information and Networks—SIN'13. doi:10.1145/2523514.2523536
27 Ishikawa, Y., Yoshida, C., Takata, M., and Joe, K. (2014). Validation of EEG Personal Authentication with Multi-channels and Multi-tasks. International Conference on Parallel and Distributed Processing International Conference on Parallel and Distributed Processing Techniques and Applications, 2, 182–188.
28 Kanamori, T., Takenouchi, T., and Murata, N. (2009). Pattern Recognition, Kyoritsu Publication.
29 Nagata, Y., and Munechika, M. (2001). Introduction to Multivariate Analysis Methods, Science, Inc.
30 Fisher, R. A. (1936). The Use of Multiple Measurements in Taxonomic Problems. *Annals of Eugenics*, 7(2), 179–188. doi:10.1111/j.1469-1809.1936.tb02137.x
31 Karayama, H. (2014). Outdoor EEG Personal Authentication for Wearable BMI Operation. *Intelligence and Information*, 26(2), 606–616.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

УДК 004.052

Махіяр Таджіні
аспірант, старший викладач кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка
ORCID ID: 0000-0001-8875-3362
m.tajdini@kubg.edu.ua

СИСТЕМИ БІОМЕТРИЧНОЇ АУТЕНТИКАЦІЇ З ВИКОРИСТАННЯМ ЕЛЕКТРОЕНЦЕФАЛОГРАФІЇ

Abstract. Останніми роками зростає рух, спрямований на поєднання науки про мозок з медициною, освітою та промисловістю. Особисту автентифікацію можна розділити на такі види: автентифікація знань, автентифікація властивостей та біометрична автентифікація. Аутентифікація за допомогою паролів або PIN-кодів, які використовуються для входу на пристрій, підпадає під аутентифікацію знань. Аутентифікація на основі власності базується на власності особи, наприклад картці або ключі. Біометрична аутентифікація — це особиста аутентифікація, яка використовує біометричну інформацію, а також розроблена біометрична аутентифікація, наприклад, відбитки пальців, райдужки, відбитки голосу тощо. Ця стаття складається з восьми розділів про біометричну аутентифікацію та висновку. Огляд біометричної аутентифікації знаходиться у другому розділі, а потім говоримо про технології біометричної аутентифікації, далі ми обговорюємо вже доступну аутентифікацію за фізичними характеристиками, такими як вена долоні, відбиток пальця, розпізнавання райдужної оболонки ока, у четвертому розділі, потім ми продовжимо поведінкову аутентифікацію, як-от голосова аутентифікація та її проблеми в п’ятому розділі, потім у шостому ми пояснюємо біометричну автентифікацію з вилученням функцій, що означає використання машинного навчання та штучного інтелекту в системах аутентифікації, і, маючи це в сьомому розділі, ми пояснили ефективність автентифікації шляхом вилучення функцій і порівняння рівня помилок, операційні характеристики швидкості та приймача, коефіцієнт помилкового відхилення та коефіцієнт помилкового прийняття для оцінки продуктивності, і, нарешті, у восьмому розділі ми показали, як дані електроенцефалографії за допомогою вилучення ознак можна використовувати для аутентифікації за допомогою *k*-найближчого сусіда та метод опорного вектору. Крім того, у цьому дослідженні ми використовували релаксаційну електроенцефалографія, що означає аутентифікацію мозкової хвилі без розумових завдань або зовнішніх подразників.

Keywords: нейромашинний інтерфейс; BMI; нейрокомп’ютерний інтерфейс; BCI; електроенцефалографія; ЕЕГ; рівень помилок; EER.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Kawato, M. (2008). Brain-Network Interface. Journal of the Institute of Electronics. *Information and Communication Engineers*, 91(2), 123–130.
2 Hotson, G., et al. (2016). Individual Finger Control of a Modular Prosthetic Limb using High-Density Electrocorticography in a Human Subject. *Journal of Neural Engineering*, 13(2), 026017. doi:10.1088/1741-2560/13/2/026017
3 Tanaka, K. (2012). Development of a Wheelchair Moved by Brain Wave Commands (Special Issue on the Forefront of Robotics for Supporting People). *Journal of the Japan Society for Precision Engineering*, 178(81), 662–665.
4 Rao, R. P. N., et al. (2014). A Direct Brain-to-Brain Interface in Humans. *PLoS ONE*, 9(11), e111332. doi:10.1371/journal.pone.0111332
5 This Place. MindRDR. http://mindrdr.thisplace.com/static/index.html
6 Armstrong, B. C., et al. (2015). Brainprint: Assessing the Uniqueness, Collectability, and Permanence of a Novel Method for ERP Biometrics. *Neurocomputing*, 166, 59–67. doi:10.1016/j.neucom.2015.04.025
7 Komatsu, N., Uchida, K., Ikeno, S., and Sakano, S. (2008). The Story of Biometrics, Japanese Standards Association.

8 Thorpe, J., van Oorschot, P. C., and Somayaji, A. (2005). Pass-thoughts. Proceedings of the 2005 Workshop on New Security Paradigms—NSPW'05. doi:10.1145/1146269.1146282
9 Ito, S., Mitsukura, Y., Fukumi, M., and Akamtsu, N. (2004). Proposal of the EEG Analysis Method Using the Individual Characteristic of the EEG. *IEEJ Transactions on Electronics, Information and Systems*, 124(6), 1259–1266. doi:10.1541/ieejeiss.124.1259
10 Kumari, P., and Vaish, A. (2014). Brainwave based Authentication System: Research Issues and Challenges, *International Journal of Computer Engineering and Applications*, IV(I&II), 89–108.
11 Atzori, L., Iera, A., and Morabito, G. (2010). The Internet of Things: A Survey. *Computer Networks*, 54(15), 2787–2805.
12 Watanabe, K. (2003). The Birth of Judicial Identity: Individual Identification and Registration in Civil Society, Kotososha.
13 Hoshino, Y. (2005). Fingerprint Authentication Technology—Biometric Security, Tokyo Denki University Press.
14 Toshiba. Fingerprint Authentication. http://www.it-serve.co.jp/products/security/fingerprint_attest.htm
15 Fujimori. Palm Vein Certification. http://www.fujitsu.com/jp/group/frontech/solutions/business-technology/security/palmsecure/
16 Hitachi. Finger Vein Authentication. http://www.hitachi-ics.co.jp/product/virsecur/vein/secure_sol.html
17 Fushidori. Iris Certification. http://atfe.fmworld.net/at/report/?id=320
18 Taigman, Y., Yang, M., Ranzato, M., and Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. 2014 IEEE Conference on Computer Vision and Pattern Recognition. doi:10.1109/cvpr.2014.220
19 Cristianini, N. and Shawe-Taylor, J. (2005). Introduction to Support Vector Machines, Kyoritsu Publishing Co.
20 Kumazawa, I. (1998). Learning and Neural Networks, Morikita Publishing Co.
21 Riera, A., et al. (2007). Unobtrusive Biometric System Based on Electroencephalogram Analysis. *EURASIP Journal on Advances in Signal Processing*, 2008 (1). doi:10.1155/2008/143728
22 Ishikawa, Y., et al. (2015). A Personal Classification Method Using Spatial Information of Multi-channel EEG. International Conference on Parallel and Distributed Processing International Conference on Parallel and Distributed Processing Techniques and Applications, 1, 229–235.
23 Hema, C. R., Paulraj, M. P., and Kaur, H. (2008). Brain Signatures: A Modality for Biometric Authentication. 2008 International Conference on Electronic Design. doi:10.1109/iced.2008.4786753
24 Marcel, S., and R. Millan, J. (2007). Person Authentication Using Brainwaves (EEG) and Maximum A Posteriori Model Adaptation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 743–752. doi:10.1109/tpami.2007.1012
25 Palaniappan, R., and Mandic, D. P. (2007). Biometrics from Brain Electrical Activity: A Machine Learning Approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 738–742. doi:10.1109/tpami.2007.1013
26 Nakanishi, I., Fukuda, H., and Li, S. (2013). Biometric verification using brain waves toward on-demand user management systems. Proceedings of the 6th International Conference on Security of Information and Networks—SIN'13. doi:10.1145/2523514.2523536
27 Ishikawa, Y., Yoshida, C., Takata, M., and Joe, K. (2014). Validation of EEG Personal Authentication with Multi-channels and Multi-tasks. International Conference on Parallel and Distributed Processing International Conference on Parallel and Distributed Processing Techniques and Applications, 2, 182–188.
28 Kanamori, T., Takenouchi, T., and Murata, N. (2009). Pattern Recognition, Kyoritsu Publication.
29 Nagata, Y., and Munechika, M. (2001). Introduction to Multivariate Analysis Methods, Science, Inc.
30 Fisher, R. A. (1936). The Use of Multiple Measurements in Taxonomic Problems. *Annals of Eugenics*, 7(2), 179–188. doi:10.1111/j.1469-1809.1936.tb02137.x
31 Karayama, H. (2014). Outdoor EEG Personal Authentication for Wearable BMI Operation. *Intelligence and Information*, 26(2), 606–616.