Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 8, No. 6, December, 2024

Improving the Reliability of Biometric Authentication Processes Using a Model for Reducing Data Drift

Vladimir Zh. Kuklin [1*], Naur Z. Ivanov [1], Alexander N. Muranov [1], Islam A. Alexandrov [1], Elena Yu. Linskaya [2]

[1] *Institute of Design and Technology Informatics, Russian Academy of Sciences, Russian Federation.*

[2] *Ivannikov Institute for System Programming, Russian Academy of Sciences, Russian Federation.*

Abstract

Modern complexes providing biometric identification face several problems, such as information drift caused by the variability of facial patterns, voice timbres, and current states. Information drift can characteristically exhibit short-term (subjects' states have changed) or long-term changes. Simultaneously, the developed trusted systems should not have the properties of explainable AI to prevent the possibility of intruders, based on understanding the system behavior to perform actions to hack the system. This paper's objective is to improve the reliability of biometric authentication by increasing the informativity of the classified images by transforming the correlations between the information features using the Bayes-Minkowski measure. The paper puts forth the proposition of employing neuroimmune models that are founded upon the principles of both acquired and innate immunity, with an analogy to the natural immune system. In addition, the authors propose to analyze correlations between information features instead of the features themselves. To reduce the influence of data drift, the authors suggest using adaptive learning with a teacher and reinforcement, which helps to work even with small and unrepresentative data samples. The proposed algorithm demonstrates a high degree of accuracy, as evidenced by its equal error rate (EER), and is particularly well-suited to feature recognition tasks due to its adaptive model. The test results have shown that the proposed solutions increase the level of security of personal data and improve the reliability of biometric authentication against fraudulent actions of intruders, including approaches based on adversarial algorithms. The integration of the immune structure into the authentication system enables the algorithm to remain stable even when presented with a limited number of samples. The proposed algorithm mitigates the impact of data drift on the authentication outcome.

Keywords:

Biometric Identification;
Information Drift;
Trusted Artificial Intelligence (AI);
Reliability of Identification Process;
Immune Model.

Article History:

Received:	02	August	2024
Revised:	06	November	2024
Accepted:	19	November	2024
Published:	01	December	2024

1- Introduction

User authentication is one of the most essential and complex aspects of controlling unauthorized access to a system. Authentication is the process through which a system verifies that a user is legally authorized to access the system. It is widely used to protect information technology (IT) systems against unauthorized user activities. Although contemporary authentication systems have the potential to alter their existing authentication methodology, there is a dearth of rigorous examinations of the current advancements in the field, which could inform and influence the development of practical solutions [1].

The authentication and verification of a user can be achieved by employing one or more of three fundamental and broad approaches: knowledge-based (something a user knows), possession-based (something a user has), and biometric-

* **CONTACT**: kuklin_vladimir_ran@mail.ru

DOI: http://dx.doi.org/10.28991/ESJ-2024-08-06-018

based (something a user is). The first two approaches have been widely adopted in most IT systems. However, they are not without their own set of well-known challenges. The biometric-based authentication approach, which employs the physiological and behavioral characteristics of a user, has gained prominence as a reliable solution. Although this approach offers a solution to the shortcomings of the aforementioned approaches, the majority of the solutions employ a single biometric cue, which is applied solely at the point of entry (referred to as static authentication). It can be argued that this limitation is insufficient for providing a verifiably secure system. The use of a single biometric factor has the potential to reduce the accuracy of the authentication system, owing to the presence of poor data quality, overlap between identities, and scarcity of resources for uniquely identifying an individual. Additionally, the use of a single biometric factor with static authentication may render the underlying system susceptible to misuse post-authentication because the verification of the user identity for the session appears to be permanent [2].

Current trends in biometric pattern recognition show the effectiveness of using AI, namely machine learning, to solve such problems. Perhaps the main problem complicating machine learning is the data drift. Data drift refers to alterations in the distribution of features received by a machine-learning model in a production environment. These changes have the potential to reduce the model's performance. Thus, information drift (sensor failure, formation of new information not considered in the learning process, etc.) can be minimized (to consider the list of changes and make a learning forecast). However, it is difficult to eliminate conceptual drift because it is difficult to predict exactly how particular phenomena will change, as discussed in more detail in Kurowski et al. [3].

It is difficult to predict the nature of drifts, even with data on their causes. For example, considering classical biometric samples (fingerprints), it becomes clear that drift can occur in the case of some physical disturbance (e.g., traumatization), while studying any dynamic example shows that these changes are inevitable (e.g., keyboard handwriting changes many times in just one day), as discussed in more detail in Zenisek et al. [4].

Let us formulate the base criteria to minimize the negative impact of drift. For example, if data are available for correct learning, even episodic updating of the models will be sufficiently efficient. The above requires weighting the data, assigning a heavy weight to the primary learning sample, and a smaller weight to the samples obtained earlier. Typically, to detect drift in a timely manner, a set of specialized metrics is used to calculate the statistical characteristics of recognition object parameters in dynamics and ensemble classification techniques, as discussed in detail in Chen et al. [5]. However, the most effective approach is the real-time image learning process. Its use eliminates or minimizes the conceptual drift. Many techniques for real-time learning have been extensively studied. However, considering the specifics of biometric systems to control certain changes in biometric images, it is essential to have up-to-date information about each informative biometric parameter, as described in more detail in Jain et al. [6]. Almost any biodynamic pattern (e.g., handwritten character or voice) can change depending on the people's state. A flexible neuroimmune simulation was applied to solve this problem. This paper proposes employing a neuroimmune model, distinguished by a malleable architectural configuration, which integrates the tenets of machine learning and reinforcement learning. This study presents a methodology for investigating the formation of innate immunity and the development of acquired immunity.

2- Literature Review

Enhancing the dependability of highly reliable biometric authentication, which may potentially result in significant adverse consequences if it malfunctions, is of paramount importance. It is necessary to define reliability to form the structure of a trusted AI. The definition of reliability here denotes an increase in the percentage of correctly recognized objects and images using a particular methodology.

Behavioral analysis, a novel form of authentication, seeks to ascertain a user's identity by identifying consistent patterns of behavior. It is now possible to construct personalized behavioral profiles by evaluating user inputs, including typing speed, mouse movements, touchscreen gestures, and the timing of operations. Anomalous and extraordinary actions can be identified through behavioral analysis, which can then alert relevant authorities to potential security breaches. An example of knowledge-based authentication is the presentation of questions to users regarding information they should be aware of, such as their mother's maiden name or their first school. Nevertheless, this approach is not without its inherent limitations, particularly in light of the ease with which sensitive data can be obtained through social engineering or data breaches [7].

One study examined ear recognition methods using machine learning. Studies have demonstrated that ear recognition using traditional machine-learning methods can achieve satisfactory recognition rates with carefully crafted features. To overcome these limitations, the implementation of ear recognition methods based on deep learning has been proposed. Researchers are exploring the potential of deep network architectures, such as CNNs and transfer learning techniques, to improve performance. Because ear image datasets are relatively small and overfitting is a concern, deep learning methods have only recently been applied to ear recognition tasks. Strategies such as aggressive data augmentation, model size reduction, regularization techniques, or transfer learning using pre-trained models from large datasets, such as ImageNet, are crucial to overcoming these limitations [8].

To reduce the number of errors made by the system, it is possible to employ a modified version of the convolutional neural network (CNN) that utilizes the max/average pooling technique, which is referred to as MAP-CNN. This approach ensures the robust extraction of facial features, which is crucial for thermal face recognition. This significantly enhances computational efficiency and model stability for real-time law enforcement applications. The extracted features demonstrated a superior representation of the individuals compared with those obtained through the conventional CNN [9].

With regard to the identification of keystroke biometrics (KB), it is feasible to enhance classification and feature extraction algorithms to attain enhanced accuracy in KB systems. Some studies combine multiple methods to achieve better results, while others utilize platform-dependent features to improve accuracy. Feature engineering remains a relevant area for future work aimed at improving the performance of KB systems. In addition, improving the feature selection and combination methods can enhance the quality of KB systems. Many researchers have not paid attention to the time and space required for training and testing, which may be due to the dramatic increase in processor speed and memory size [10].

Compared to other biometric systems, keystroke authentication represents a highly active area of research. Researchers have conducted limited studies analyzing keystroke authentication systems, and many have used desktops or laptop computers. Some studies have used temporal characteristics and additional characteristics such as pressure, finger area, or their combination [11].

Reviewing a representative subset of simultaneous keyboard search studies led to the following conclusions. The review revealed that the superior outcomes observed in numerous studies were achieved through the use of neural-network-based pattern classification. Although statistical classifiers are the most cost-effective in terms of computational resources, they cannot achieve a high level of classification. Furthermore, the study advises against utilizing the same participants for the assessment of the system in both authorized and unauthorized categories. Additionally, it posits that developing such systems may prove to have considerable potential in the field of cybersecurity, as it is not the case that many identification systems suffer from low recognition accuracy; rather, it is the quality of system security, which is a greater problem [12, 13].

Trusted AI is an essential concept in machine learning. The trusted AI meets the criteria of explainability, transparency, robustness, and security. Neural network architecture rests on several promising research directions to form a high-performance model. Among these directions, it is worth highlighting evolutionary neural networks, deep learning, and artificial information systems, as discussed in detail in Budžys et al. [14] and Alexandrov et al. [15].

The evolutionary process of a classical neural network relies on replicating and optimizing expected results by selecting particular informative characteristics. Evolutionary neural network training uses an algorithm that involves obtaining a training set and creating several neural networks with their topology and a certain weight. The next step is to test them, compare their performances to select the best ones, and combine them. The final neural network becomes a sample of a new AI branch and then repeated tests and other operations until a neural network with the required characteristics is obtained, as detailed in Ding et al. [16].

Using the advantages of the evolutionary approach opens up the possibility of using a learning methodology with learning realized during neural network operations. As a rule, genetic methods should be applied to search for the optimal neural network architectures. Simultaneously, the cost of forming training sets is sufficiently high. Most of these methods focus on working with traditional models of neural elements poorly adapted to interconnected neurons [17, 18].

Algorithms for deep learning have good prospects, but researchers believe that high performance is achievable only in the case of collective learning, which requires large information sets [19, 20]. The fuzzy rough nearest neighbor (FRNN) method is applicable as a nonparametric method for classification and regression. Considering classification tasks using this method, it is possible to conclude that it is advisable to use Equal Error Rate (EER) as a correct estimation of the reliability of its work [21].

The current literature on biometric identification indicates that most subjects involved in the studies were institutions, students, academics, or support staff. Since biometric identification has a robust psychological basis, it cannot represent the entire population. A more nuanced understanding of the behavioral characteristics of individuals from diverse age groups, genders, and backgrounds may enhance the precision of established biometric keystroke systems [22-24].

When working with biometric parameters and their classification or recognition, it is essential to consider such factors as a person's psychophysiological state (PPS). Generally, the PPS is a user's feature describing a set of biological aspects of his adaptation to external conditions analyzed based on his psychophysiological data, as detailed in Berto [25]. Regarding the functional state, it is essential to consider the user's functioning and its characteristics (for example, perception: sensory and intellectual). Simultaneously, any mental state reflects the qualitative features of people's reactions to different situations. There are fundamental differences between the mental state (it is usually long-lasting and shows unique biometric information about behavioral tendencies) and PPS (describes the psychic and physiological characteristics of the user) [26, 27]. Therefore, when changing the PPS, it is practically impossible to predict changes in dynamic bioimages. To solve this issue, it is necessary to use special techniques that enable the model to be trained in real time.

3- Material and Methods

To provide a more detailed and comprehensive representation of the methodology, a flowchart (Figure 1) has been included.

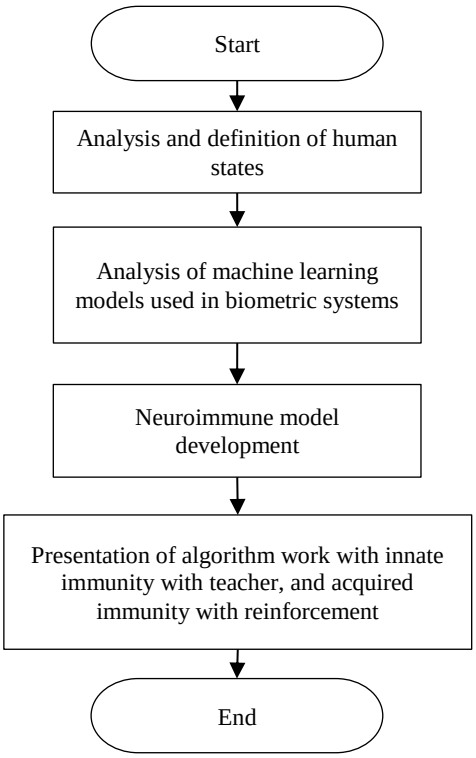

Figure 1. Flowchart of the methodology presented

It is difficult to identify criteria that can accurately determine user states. A particular group of medications can affect the central nervous system (CNS) and change a subject's PPS. Thus, a group of adaptogens provide mild CNS excitation. Caffeine induces excitement and mild euphoria. Natural plant substances, such as mints, can relax a person or become sleepy. This group of substances does not cause addiction, so it is suitable for use in an experiment that will record changes in the work of the heart muscle, as detailed in Borgianni & Maccioni [28]. Based on the results of this study, the following conditions were considered:

1. Stability. In this instance, the individual undergoing the experiment did not exhibit any discernible effect in the morning. The primary condition that the subjects had to follow was to get great rest before the study.
2. Excitement. People attempting to solve responsible tasks usually experience this state. Each participant consumed coffee or herbal adaptogens to ensure mild CNS excitation. The heart muscle beats increased by approximately 8-10%.
3. Fatigue (due to physical exertion). It is necessary to be sensitive to the gender and age of a person in order to consider the factors of fatigue. Furthermore, it should be noted that in this context, the term "fatigue" is used to describe the impact of physical and psychological stressors rather than simply indicating a lack of sleep.
4. Relaxation. In other words, it indicates light sleepiness. Valerian usage to simulate this state decreased the heart muscle beats by approximately 2-5%.
5. Intoxication. An alcoholic beverage was used, calculating the concentration according to the ratio proposed by Widmark: $c = A/m \cdot V$,

where c is the alcohol concentration ‰, A is the weight of the consumed substance (g), m is the participant's weight (kg), V is the index proposed by Widmark (0.7 for males, 0.6 for females), as detailed in Ge et al. [29]. Intoxication considers several stages that characterize a certain PPS of the participants:

5.1. 1st stage. The alcohol content in the blood is 0.2-0.3‰. Some cases record implicit violations detected by testing.

5.2. 2nd stage. The alcohol content in the blood was 0.3-0.5‰. This causes a change in thinking and coordination, difficulty concentrating on something specific, and a slower reaction time. Often, a person experiences slight euphoria, relaxation, joy, or decreased restraint.

5.3. 3rd stage (often referred to as "light intoxication"). The alcohol content in the blood was 0.5-1%. It changes the beating of heart muscle variability, dull sensation, perception, and others. The biometric samples for these conditions were collected separately.

The study results show that password phrase entering was 3%-16% slower in an altered state, depending on the specific state. In addition, relatively stable keyboarding times were recorded (37%-203%, Figure 2). In particular, relaxation (170%) and excitement (202%) signs appeared.

Therefore, the specificity of the PPS change supports the assumption that it is virtually impossible to predict the nature and extent of the change in the dynamic biometric image, causing the use of real-time learning.

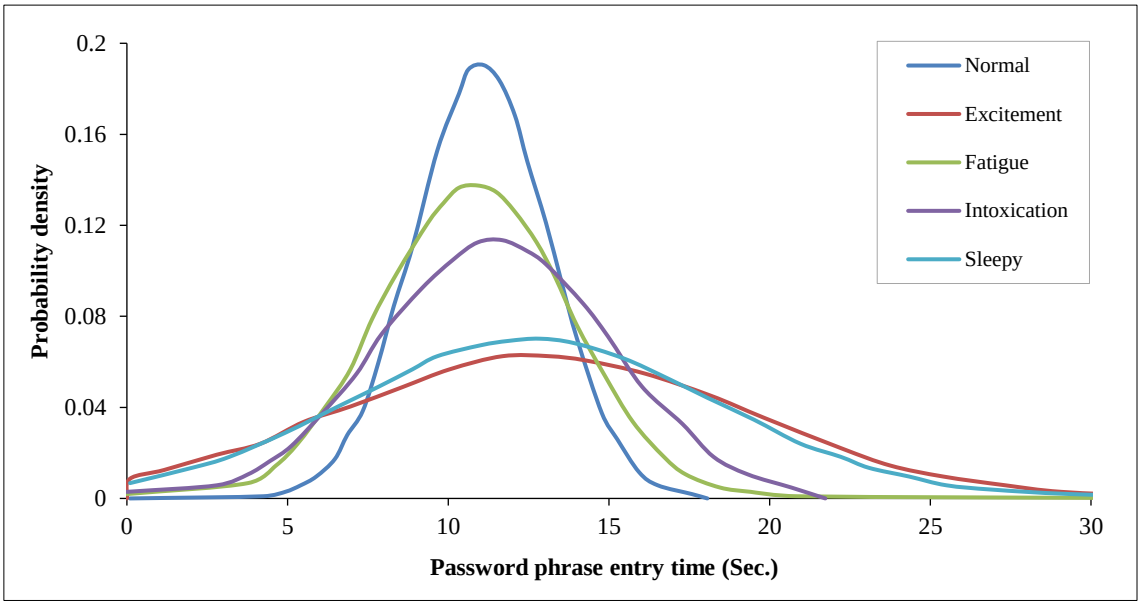

Figure 2. Distribution of the password phrase typing speed, the primary condition of the security system constant improvement. 80 people participated in the experiment

3-1- Formation of the Structure and Function of Detectors and Immune Model Development

As mentioned above, some cells of the immune system identify hostile factors. In this section, the terms "detector" and "sensor" are used to refer to these cells. We normalize the detector response in recognizing a hostile image factor in the interval from 0 to 1, corresponding to a 100% probability of hostility.

Detectors are binary sorters endowed with a particular functional that provides a thorough analysis of a biometric image consisting generally of a gradient of characteristics $\overline{a} = \{a_1, a_2, \ldots, a_n\}$; here, n is the minimum number of image characteristics. Equation 1 is applied to reveal the reaction of i-th sensor to the resulting image $\overline{a}$:

$$u_i = \phi_x(y' = \varphi(y = f_r(\overline{\alpha} = R(\overline{a}, \Psi_i), \overline{g}, \Theta_i), T_i)) \quad (1)$$

Next, we describe in more detail the functionality of the sensors and their parameters.

1. $\overline{\alpha} = R(\overline{a}, \Psi_i)$ is a receptor function that realizes the interaction between the sensors and antigens. This formula allows us to estimate η of n parameters corresponding to $\overline{a}$; in turn, Ψ_i is the set of characteristic indices that the i-th sensor specifies, and gradient $\overline{a} = \{a_1, a_2, \ldots, a_\eta\}$ is a vector with end-to-end element numbering.

2. $y = f_r(\overline{\alpha}, \breve{g}, \Theta_i)$ represents the sensor kernel function that computes a measure of the distance of the gradient $\bar{\alpha}$ from the ideal image; r is a set of functions described by formulas (2)-(11); $\breve{g}$ represents the gradient of parameters that determine the sensitivity of the calculation; $\Theta_i = \{\mu_1, \mu_2, \ldots \mu_\eta, \sigma_1, \sigma_2, \ldots, \sigma_\eta\}$, μ_i, and $\sigma_i$are the characteristics of the j-th features of the gradient $\bar{a}$. Set $\Theta_i$computing uses randomly selected examples of the training sets. To construct a flexible AI model capable of functioning in an unprotected mode, a number of steps must be followed (2.1-2.3):

2.1. The list of relationship-sensitive metrics called measures (once proposed by Minkowski) (2) and the measure variants proposed by Bayes and Minkowski (3)–(5) are expressed as follows:

$$f_1(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sqrt[g]{\sum_{j=1}^{\eta} \left|\frac{(m_j - a_j)}{\sigma_j}\right|^g}, f_1(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sqrt[g]{\sum_{j=1}^{\eta} \left|\frac{(\mu_j - a_j)}{\delta_j}\right|^g} \quad (2)$$

$$f_2(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sum_{j=1}^{\eta} \left| \left| \frac{(m_t - a_t)}{\sigma_t} \right|^g - \left| \frac{(m_j - a_j)}{\sigma_j} \right|^g \right|, f_2(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sum_{j=1}^{\eta} \left| \left| \frac{(\mu_t - a_t)}{\delta_t} \right|^g - \left| \frac{(\mu_j - a_j)}{\delta_j} \right|^g \right| \quad (3)$$

$$f_3(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sqrt[g]{\sum_{j=1}^{\eta} \left| \frac{(m_t - a_t)}{\sigma_t} \right|^g - \left| \frac{(m_j - a_j)}{\sigma_j} \right|^g}, f_3(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sqrt[g]{\sum_{j=1}^{\eta} \left| \frac{(\mu_t - a_t)}{\delta_t} \right|^g - \left| \frac{(\mu_j - a_j)}{\delta_j} \right|^g} \quad (4)$$

$$f_4(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sqrt[g]{\sum_{j=1}^{\eta} \left| \frac{a_t}{\sigma_t} - \frac{a_j}{\sigma_j} \right|^g}, f_4(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \sqrt[g]{\sum_{j=1}^{\eta} \left| \frac{a_t}{\delta_t} - \frac{a_j}{\delta_j} \right|^g} \quad (5)$$

By varying $g \in$ [from 0.01 to 100], it is possible to estimate the remoteness more accurately by considering the degree of interaction between the characteristics. In addition, it is essential to select the characteristic Ψ_i such that the indices describing pairwise interaction $C_{j,t}$ have similar values, that is, the measure proposed by Minkowski $C_{j,t} < 0.5$, and the measure proposed by Bayes-Minkowski $C_{j,t} > 0.5$ [30].

2.2. The list of non-interacting metrics is represented by differential (6) and integral formats (7), and their characterizing criteria (8)–(11). Various detectors can be formed owing to the availability of different functionals. Almost any functional offers multiple measures of remoteness, mainly determined by the variation of the characteristics $\breve{g}$.

$$f_5(\overline{\alpha}, \breve{g} = \{g_1, g_2, \ldots, g_\eta\}, \Theta_i = \prod_{j=1}^{\eta} p_{g_j}(a_j, m_j, \sigma_j) \quad (6)$$

$$f_6(\overline{\alpha}, \breve{g} = \{g_1, g_2, \ldots, g_\eta\}, \Theta_i = \prod_{j=1}^{\eta} P_{g_j}(a_j, m_j, \sigma_j) \quad (7)$$

Here, $P_g(a, m, \sigma)$ and $p_g(a, m, \sigma)$ are the current values of the dependences describing the distribution, considering a_j and the characteristics $m_j$and σ_j. This distribution, which depends on characteristic g_j, determines the behavior of these dependencies. In this study, three probability distributions were considered: normal, lognormal, and Laplace. These distributions describe the predominant morphological characteristics [31].

To ensure that any meaningful image is identified, the distribution can be extended. Thus, with respect to

– The normal distribution (g_j= one):

$$p_1(a_j, m_j, \sigma_j) = \frac{1}{\sigma_j \sqrt{2\pi}} e^{-\frac{(a_j - m_j)^2}{2\sigma_j^2}}$$

$$P_1(a_j, m_j, \sigma_j) = \frac{1}{\sigma_j \sqrt{2\pi}} \int_{m_j - 5\sigma_j}^{a_j} e^{-\frac{(\vartheta - m_j)^2}{2\sigma_j^2}} d\vartheta$$

here, m_j and σ_j are averaged deviations of *j*-th characteristics;

– The lognormal distribution (g_j= two):

$$p_2(a_j, m_j, \sigma_j) = \frac{1}{a_j \sigma_j \sqrt{2\pi}} e^{-\frac{(Ln(\vartheta) - m_j)^2}{2\sigma_j^2}}$$

$$P_2(a_j, m_j, \sigma_j) = \frac{1}{a_j \sigma_j \sqrt{2\pi}} \int_{m_j - 5\sigma_j}^{a_j} e^{-\frac{(Ln(\vartheta) - m_j)^2}{2\sigma_j^2}} d\vartheta$$

here, m_j and σ_j characterize the scale and formats;

– Laplace distribution (g_j= three):

$$p_3(a_j, m_j, \sigma_j) = \frac{\sigma_j}{2} e^{-\sigma_j |a_j - m_j|}$$

$$P_3(a_j, m_j, \sigma_j) = \begin{cases} 0{,}5e^{\sigma_j (a_j - m_j)}, a_j \le m_j \\ 1 - 0{,}5e^{\sigma_j (a_j - m_j)}, a_j > m_j \end{cases}$$

here, m_j and σ_j are indicators describing the scale and shift;

$$f_7(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \int_{-5}^{5} \sqrt[g]{|P_1(\vartheta, m_{\dot{a}}, \sigma_{\dot{a}} - P_1(v, 0{,}1)|^g} \cdot d\vartheta \quad (8)$$

$$f_8(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \int_{-5}^{5} \sqrt[g]{|p_1(\vartheta, m_{\dot{a}}, \sigma_{\dot{a}} - p_1(\vartheta, 0,1)|^g} \cdot d\vartheta \quad (9)$$

$$f_9(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \int_{-5}^{5} \sqrt[g]{|P_1(\vartheta, m_{\dot{a}}, \sigma_{\dot{a}} \cdot (1 - P_1(\vartheta, 0,1))|^g} \cdot d\vartheta \quad (10)$$

$$f_{10}(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i) = \int_{-5}^{5} \sqrt[g]{|p_1(\vartheta, m_{\dot{a}}, \sigma_{\dot{a}} \cdot p_1(\vartheta, 0,1)|^g} \cdot d\vartheta \quad (11)$$

Functionals (8)–(11) are modifications of the indicators describing the agreement that allows us to compare the considered dependencies describing the distribution concerning the ideal $\mathring{a}$. In this case, it is assumed that the distribution is normal, so $\mathring{a}$ is the normalized value of the current characteristic, $\mu_{\dot{a}}$and $\sigma_{\dot{a}}$describe the mathematical expectation and average deviation value, respectively. In addition, they allow the calculation of the average geometric probability and Gini index [32]. The distinction (when set $a_j$is a random variable $\mathring{a}$) considered the value $\Theta_i$according to the following formula: $\dot{a} = \frac{a_j - m_j}{\sigma_j}$

The characteristics of the distribution $\mathring{a}$ in the class "Friend" are typical ($\mu_{\dot{a}}$≈1 and $\sigma_{\dot{a}}$≈1). The same ones in the class "Foe" have deviations ($\mu_{\dot{a}}$≠0 and/or >1).

2.3. The subsequent phase of the process involves applying the set of functions (12) to the protected mode, thereby establishing a robust foundation for the forthcoming detector. As previously stated, these relationships can be represented as follows:

$$f_{11}(\overline{\alpha}, \breve{g} = \{g\}, \Theta_i = \sqrt[g_1]{\frac{1}{\eta}\sum_{j^*=1}^{n'} w_{j*}(a'_{j*} - m')^{g2}} = \sqrt[g_1]{\frac{1}{\eta}\sum_{t=1}^{\eta} w_t(a'_t - m')^{g2}}$$
$$m' = \frac{1}{\eta}\sum_{t=1}^{\eta} a'_t, a'_t, = a'_{t,j} = f(a_t, a_j) = \left|\left|\frac{a_t}{\delta_t}\right|^{g_3} - \left|\frac{a_j}{\delta_j}\right|^{g_3}\right| \quad (12)$$

3. $y' = \varphi(y, T_i)$ represents a normalization of the dependence responses y with respect to the threshold values calculated during the tuning of the *i*-th detectors. The following formula describes the normalization process:

$$\varphi(y, T_i) = y/T_i$$

here, *y* is the distance from $\overline{\alpha}$ to the "Friend" ideal; the T_i value represents the correlation of the kernels of *i*-th detectors when it is affected by the training image "Friend," or:

$$\varphi(y, T_i) = T_i/y$$

here, *y* represents the probability of a situation occurring when $\bar{\alpha}$ will correspond to the category "Friend". The value of *y* is contingent upon the dependence of the detector kernels.

4. $u_i = \phi_\chi(y'_i)$ - the extent of nonlinearity in the sensor response is contingent upon the specific activation function employed, which ultimately affects the overall system functionality. Since the final solution in the range [0, 1] is determined by the detectors, the choice of activation function is of utmost importance. The most universal option is the sigmoid function; however, various alternative options are possible, as presented above.

An important theoretical concept in the field of trusted authentication systems is distance [33]. However, in the case under consideration, the detectors estimate the distance using an original method and are programmed to adapt to changing tasks, that is, they ensure that a solution is found when learning using various AI models.

We proposed a classification of the entire population of detectors, distinguishing between those with innate and acquired immunity. This classification is then presented to several committees of sorters who are capable of learning using different techniques.

This ratio can be used to determine the outcome of the collegial decisions made by *N* detectors:

$$\ddot{u} = \Phi(\overline{D}^* = \{D_1^*, \ldots, D_n^*\}, \overline{a}) = \frac{1}{N}\sum_{i=1}^{N} \phi(D_i^*, \overline{a}) = \frac{1}{N}\sum_{i=1}^{N} u_i$$

Innate immunity is genetically transmitted from the beginning of its onset. In this study, immunocompetent sensors play the role of innate immunity, whose final structure is determined by their developmental trajectory (especially in the early stages). Iterative learning based on the validation and training sets generates the type of immunity under consideration (Figure 3). The initial option pertains to the assessment of the dependability of each determination rendered by the model in response to alterations in the sensor generation.

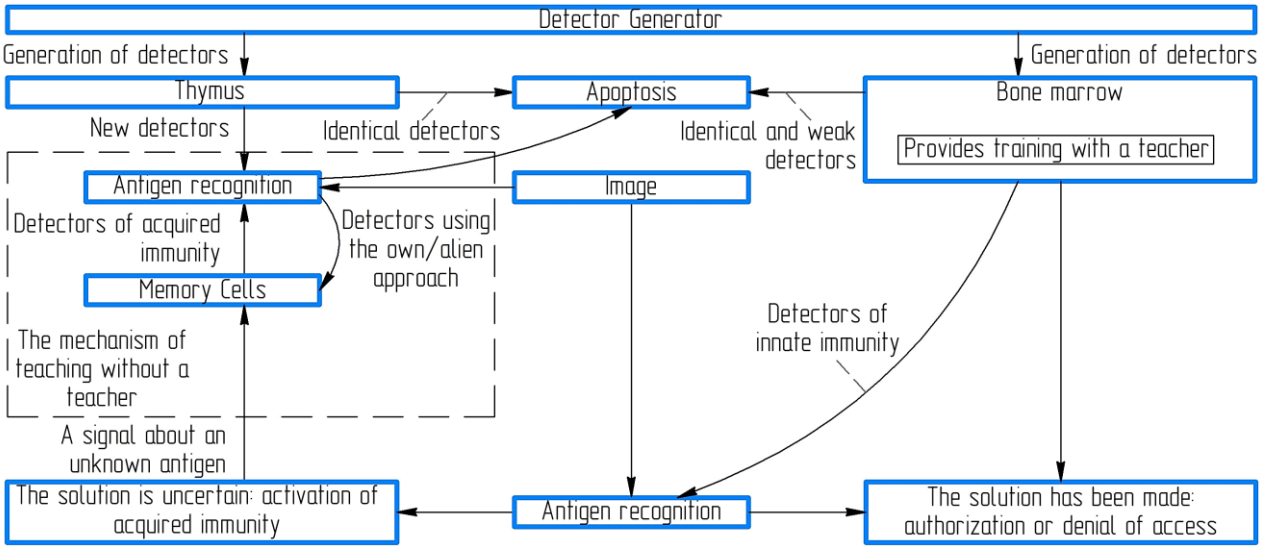

Figure 3. Adaptive neuroimmune model based on the immune approach

Acquired immunity develops throughout its function. It is more effective not for typical negative factors but for specialized ones. The immune model considered in this study was designed to select immunocompetent sensors based on the validation sampling. The formation of immunologic cells, specifically memory cells, is contingent on the presence of an immune response. In our case, these cells served as detectors. It can be reasonably deduced that the aforementioned type of immunity will manifest as a result of the image operation. When an individual is presented with a visual stimulus and is required to attribute it to one of two categories "Friend" and "Foe", a dual-process decision-making mechanism may be initiated, which subsequently gives rise to the generation of novel immune-competent detector cells.

He proposed the concept that with an increase in the number of opinions of different specialists, the overall ability of the ensemble tends to 1, provided that the opinions are independent [34]. Even if the value of each opinion is less than 0.5, the decisions of the detectors can be inverted, that is, the problem of making the opposite decision will be solved.

Detector generator involves determining a random number of detectors and selecting features of mutual correlation within certain set limits. If there are no features with a given level of correlation, the feature number generation is repeated, resulting in the selection of a Minkowski proximity measure and the subsequent selection of a random activation function. If the generated detector is an exact match for one of the innate or acquired immunity detectors, the generation process is repeated.

Accordingly, a number of indicators that influence the decision-making processes of all detectors to the optimal level can be identified:

- N – full set of detectors for decision-making;
- RD is a matrix of Pearson pairwise correlations $C(\overline{u}_i, \overline{u}_l)$, in which $\overline{u}_i$is the gradient of the responses of the i-th detector to each “Foe” sample obtained from the training sets;
- Δu is the combined strength of the response to "Friend" and "Foe" (13):

$$\Delta u = \mu_u^{(FO)} - \mu_u^{(FR)}, \mu_u^{(FO)} > \mu_u^{(FR)} \quad (13)$$

here, μ_u represents the performance evaluation of the detector. The aforementioned strategy principles were designed with the objective of reducing the interrelations between the decisions of experts. However, this approach has been demonstrated to be insufficient in terms of efficiency. The analysis of characteristic $C(\overline{u}_i, \overline{u}_l)$ showed that this method is quite costly. Furthermore, there is a dearth of consensus regarding the methodology employed for image customization. It can be reasonably deduced that the training period was excessively protracted, and in the majority of cases, did not yield a favorable outcome. It was thus resolved to augment the number of sensors, given that they were not homogeneous. A deficiency in the number of sensors would result in cell death, which would then lead to the destruction of the aforementioned defective cells (Figure 3).

It is imperative that no solitary decision made by a sensor indicates its interconnectivity; rather, each decision should be independent of the others. The corresponding twin was subsequently removed, and a new sensor was created.

The greater the number of distinguishing characteristics D_i and D_l are, the fewer the number of interconnected decisions of *i*-th and *l*-th sensors.

The described model relies on a random sampling idea, but unlike the "random forest" Ψ_i, it generates rules for random attributes. Thus, sensor tuning involves a threshold T_i calculation and "ideal" feature description Θ_i (μ_j and σ_j). After tuning, the detectors can be described as $D_i^* = \{\Psi_i, \breve{g}, r, \chi, \Theta_i, T_i\}$ and the dependence (1) – as $\phi(D_i^*)$.

3-2- Collaborative Development of Adaptable Neuroimmune Artificial Intelligence Models with the Teacher

The proposed methodology comprises a series of iterative cycles, whereby novel detectors are generated using multiple training examples, followed by an estimation of their efficacy (Figure 4). The elimination of suboptimal detectors occurs in accordance with the outcomes of the verification process, forming a new, more productive generation. The value Δu (13) expresses the sensor learning. Estimates $\mu_u^{(FR)}$ and $\mu_u^{(FO)}$ regarding a particular innate immunity sensor decision are calculated. The obtained characteristics allowed us to construct an interval of uncertain decisions $[\mu_u^{(FR)}; \mu_u^{(FO)}]$.

Each training cycle formed a set of new "Foe" images (Figure 4). For this purpose, training examples poorly categorized by strong "Foe," giving minimal responses $\ddot{u}$, are crossed, as expressed by the following relation:

$$a_{k,j} = \frac{K_{syn} + 1 - k}{K_{syn} + 1} \cdot a_{k,j} + \frac{k}{K_{syn} + 1} \cdot a_{z,j}$$

here, K_{syn} is the number of artificial samples formed by "strong Foe" classified as the previous generation (in our case, K_{syn} = one), *k* is the index of the regular artificial sample, and *j* is the index of the current characteristic. The considered variant of the strong "Foe" detector formation is sufficiently productive with the characteristics distributed according to the patterns close to normal.

Artificial examples were entered into the training sets. Each detector is tuned on the artificial samples to better classify the "Foe" examples while close to the "Friend" examples. Consequently, the models underwent training to create images of a strong "Foe" and its identification.

Figure 4 shows the productivity of the training methodology. The most significant characteristics in learning are I_{II}– the number of training cycles; N_{II}– the number of sensors remaining at the end of learning; N_{gen}– the number of sensors generated at each stage of their generation; N_{valid}– the number of dropouts; Q – the number of sensors that are strong "Foe" (each cycle generates $K_{syn} \cdot Q \cdot (Q-1)/2$ samples).

The base characteristics of this methodology include training ($K_G^{(T)}$ and $K_I^{(T)}$) sets and validation ($K_G^{(V)}$ and $K_I^{(V)}$) sets, considering the dimensionality of the training sets with combined "Friend" and "Foe" ($K_G^{(F)}$ and $K_I^{(F)}$). In this case, the training sets were $K_I^{(F)} = K_I^{(T)}/3, K_G^{(F)} = 2 \cdot K_G^{(T)}/3$. The dimensionality of the training sets employed in the "Foe" classification task is not constant. Rather, it underwent an incremental increase with the introduction of artificial samples into the training set. In contrast, the dimensionality of the validation set remained constant across all instances.

3-3- The Development of Adaptive AI Neuroimmune Systems Through Reinforcement Learning

In instances where the training sets do not align with the intended purpose and objectives of the study, the observed productivity of the innate immunity components typically fails to align with the proposed Δu (13). In this case, it cannot be guaranteed that detectors with low sensitivity levels will surpass the obstacles presented by Condorcet. (For such sensors, analysis using test sets is performed according to the expression $\mu_{u,i}^{(FO)} < \mu_{u,i}^{(FR)}$). Overcoming this barrier is possible in the presence of acquired immunity voting, resulting in the development of collegial decisions.

In accordance with this rule, lying in the interval $\mu_i > \mu_u^{(FO)}$ or $\mu_i < \mu_{u,i}^{(FR)}$ where decisions D_i^* are definite, and when $\mu_u^{(FR)} < u_i < \mu_u^{(FO)}$, they are indefinite. When decisions of innate immunity by external features are indefinite during the identification of images, acquired immunity comes into operation (Figure 5).

Then, the formation of new sensors customized to other samples contained in the validation datasets occurs. For these, the calculation of the standard response u_i takes place. Note that the collegial decision only considers sensors with a definite response analogous to memory. Sensors with indefinite responses were eliminated.

The duration and productivity of the methodology responsible for additional training (Figure 5) will depend on: I_{AI}– the number of training cycles, $N_{AI}^{(max)}$– and the maximum number of sensors for acquired immunity.

Using I_{AI}realizes a stop function, that is, infinite learning cycles are impossible. Thus, the methodology assumes reinforcement learning. Staying in the interval $[\mu_u^{(FR)}; \mu_u^{(FO)}]$ is a type of reinforcement signal, that is, a reaction to each decision.

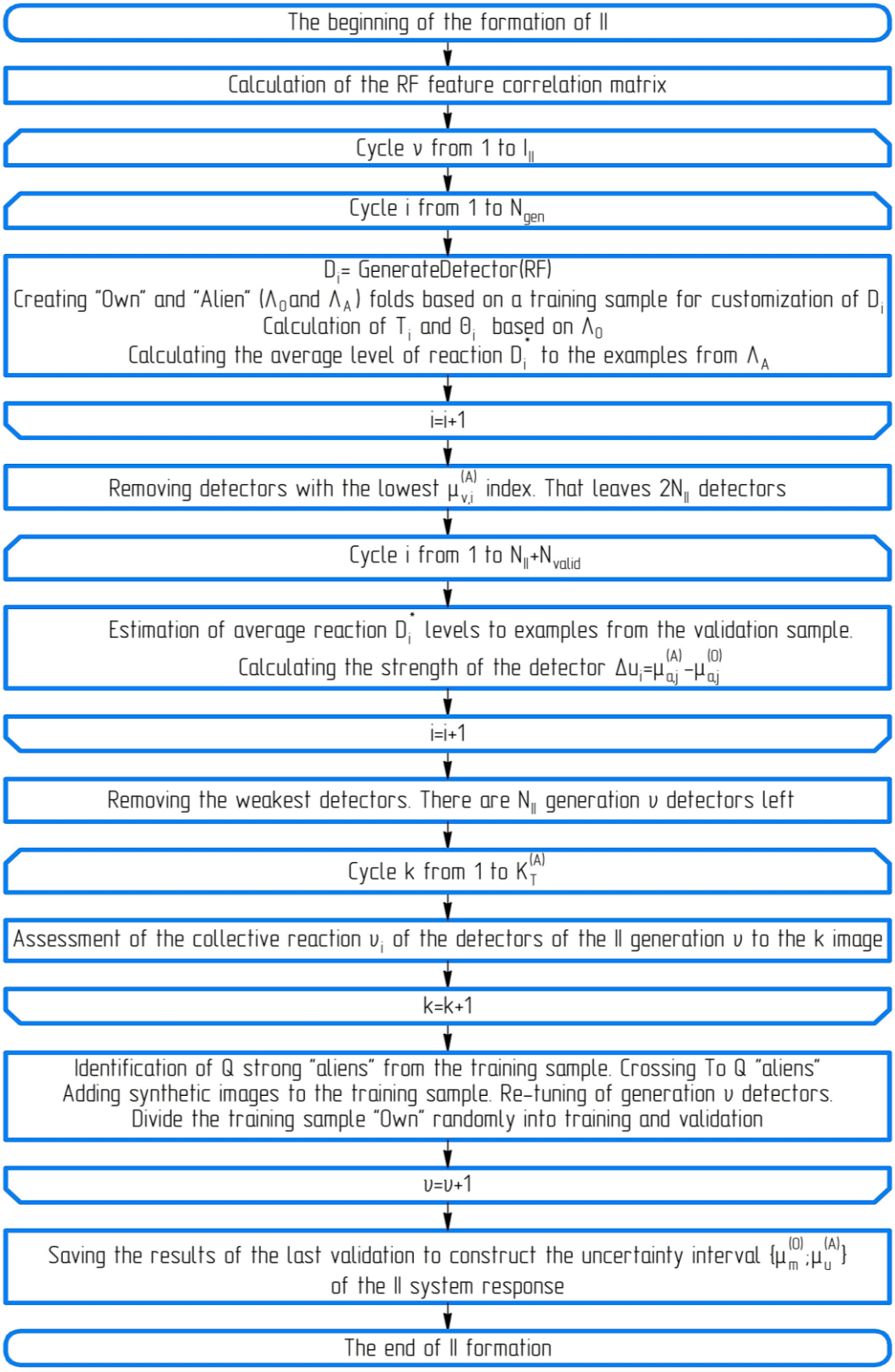

Figure 4. Schematic representation of the methodology creating innate immunity

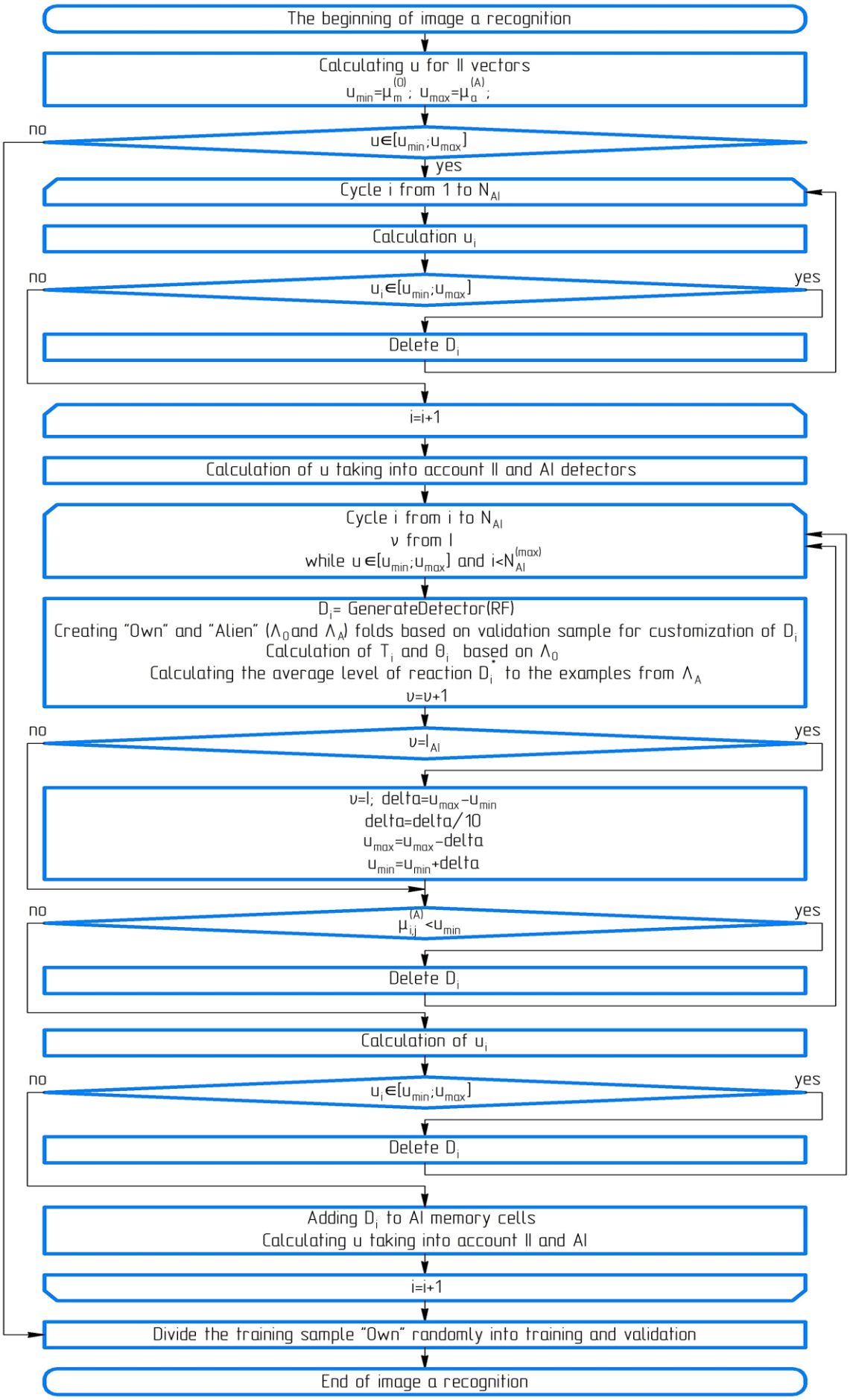

Figure 5. Schematic representation of the functioning of the methodology responsible for acquired immunity

4- Results and Discussion

The results of experimental testing of the adequacy of the proposed training methodology were obtained when classifying examples of keyboard handwriting. Many specific problems still complicate the solution to this problem, particularly considering the need to ensure information security.

It is necessary to minimize the possibility of false "Foe" acceptances and increase false "Friend" rejections to 9-25% of erroneous decisions. These characteristics are interdependent, and their correlation forms a threshold that maintains a certain balance. In the context of comparative analysis of identification techniques, the criterion of mean accuracy (MAC) is frequently employed, with formula 1–(FRR+FAR)/2, which calculates this measure. In addition, the equal error rate (EER), which describes the equal probability of erroneous decisions, is also applicable when the EER is approximately equal to the false acceptance rate (FAR), false rejection rate (FRR), and one-MAC. To achieve this, it is necessary to utilize a number of receiver operating characteristic (ROC) curves that illustrate the extent to which the false acceptance rate (FAR), false rejection rate (FRR), and thresholds are correlated during the course of the tests. When the mean accuracy (MAC) value is relatively low, for instance, at less than 0.85 (or EER greater than 0.1), then adjusting the FAR to 0.0001 will result in the following expression: 1≥FRR>0.5. Therefore, the specificity of the ROC curves can be significantly determined.

Many studies related to biometric personal identification and machine-learning-based classification have used EER indicators. Table 1 presents the results of the algorithms evaluated using this indicator.

Table 1. Results of different algorithms based on EER indicator.

Method	EER value	Year of study	Source
Fuzzy-Rough Nearest Neighbour	0.3601	2019	Liew et al. (2019) [10]
Sequence alignment algorithms	0.4	2007	Revett et al. (2007) [35]
Feed-Forward Neural Network	0.09	2019	Hammad et al. (2018) [36]
Low-cost sensor dataset	0.16	2018	Blasco et al. (2018) [37]
Random forest	0.169	2021	Marteau et al. (2021) [38]
Support vector machine	0.81	2004	Yu et al. (2004) [39]
Proposed model	**0.08**	**2024**	

The high performance confirms that it is not easy to obtain such results, even when considering the capabilities of the neural network basis. It is necessary to have large training sets to use the high potential of the techniques responsible for deep learning, which is not realistic (over 300 samples for each user).

Several information arrays with keyboard handwriting were used to test the productivity of the methodology [40-42]. To illustrate, an array of data has been collated on 32 users who have entered one phrase on multiple occasions." (n=62, using error-free entry).

The experiment was conducted using a variety of training set sizes with samples of the "Friend" type, beginning with K_G= 20 and culminating in K_G= 40. The training and validation subsets of the "Friend" samples, conducted prior to the commencement of training, were performed on the basis of the expression $K_G^{(T)} = 2 \cdot K_G^{(V)}$. The remaining samples were then included in the test set. The tests involved cross-comparison (computing FAR to compare all samples of participants to the "ideal" of other users). Consequently, for each participant, the dimensionality of the "Foe" test sets was as follows: the first base, 19900, and the second base, 1968. Figure 6 shows the test results. In this instance, the FAR parameter was 0.0001, while the FRR parameter was 0.193. During testing, the EER value corresponded to 0.02745 [40, 42].

The manner in which training sets are formed has a significant impact on the reliability of decisions made. The outcome of the preliminary testing, which was conducted in accordance with the specified time parameters, substantiates this assertion. To select training samples in a uniform manner, the training sets were aligned with the objectives of the study. However, when the training and subsequent testing of samples occur at varying times, the representativeness of the set is reduced. In instances where the sensors responsible for innate immunity are operational, a discernible discrepancy in the proportion of correct determinations can be observed in the innate immunity mode, in other words $N_{AI}^{(max)} = 0$) and acquired immunity + innate immunity (this case involves both categories when $N_{AI}^{(max)} > 0$).

By employing the provided specifications, it is possible to construct secure neural network biometric containers, which are defined as neural network biometric containers that incorporate elements that are not directly examinable owing to reversible or irreversible transformations. The conventional neural-network biometric container is a structured data block. Neurons are linked together via cross-links. Following the training phase, the tables of each neuron are encrypted by superimposing a gamma, which represents the checksum of the outputs of all preceding neurons in the chain. The neuro-immune container has the potential to compromise the knowledge of the AI model, as the majority of detectors do not conceal the parameters of the feature distribution, in contrast to the correlation neurons. This approach is employed to enhance the entropy of responses, thereby safeguarding against knowledge extraction.

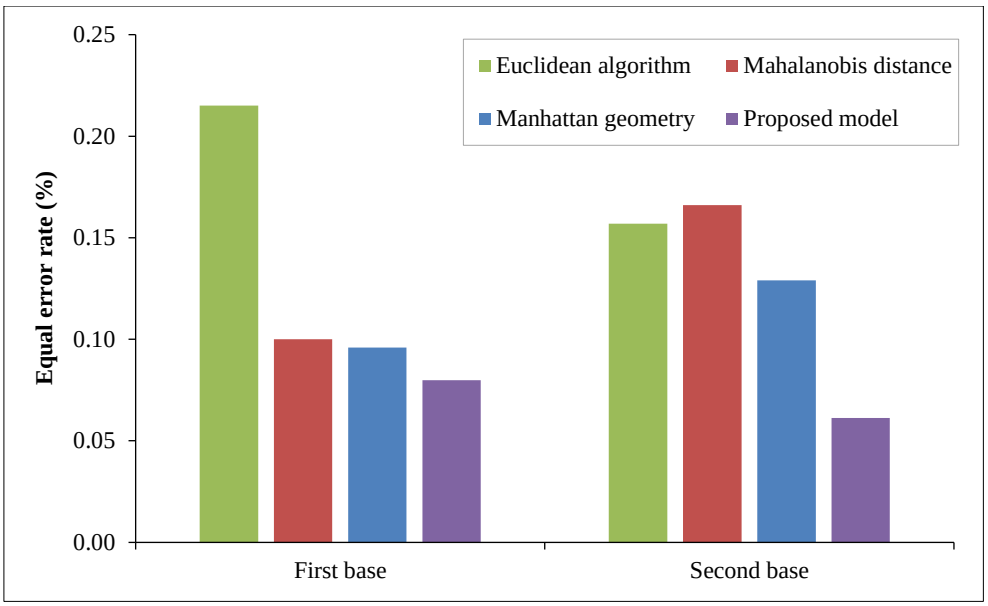

Figure 6. Performance of the proposed methodology considering the EER criterion.

Long-term training of the model will ensure a higher degree of reliability in decision-making processes and provide a sufficient level of trusted AI. It should be noted that the training of the neuroimmune model requires a significant investment in time but will result in a higher degree of reliability for each decision. It is important to highlight that the training process is relatively stable; however, if I_{II} values are high, subsequent retraining is necessary. When increasing N_{II}, the current EER will decrease and then stop altogether if the decision of the innate immunity sensors becomes too dependent.

This model and its training followed the laws of trusted AI and artificial neural networks:

1. The proposed model offers the potential to increase the percentage of correct solutions, thereby differentiating itself from traditional detectors. Furthermore, its identification accuracy exceeds that of the conventional detectors;
2. Sustained learning (The probability of subsequent retraining throughout the development of innate immunity is comparatively low);
3. High adaptability (due to changes in the characteristics and the composition of sensors);
4. Communication (the presence of innate immunity forms a set of characteristics that strengthen the acquired immunity of all sensors);
5. Increased reliability of all the decisions made by the model;
6. Acquired immunity creates memory;
7. Resistance to destructive influences from external threats.

Groups of protected neural network biometric containers can also form, that is, structured information blocks, storing the base characteristics of the trained neural network transducers. This protection operates in the following manner. An entire set of neurons forms an integral chain owing to cross-links. Once neurons have undergone training, encoding of the checksum of the output channels associated with each neuron is initiated. This process occurs in the following order.

$$tables_l^{'} = XOR(tables_l, hash(pass, b_1, \ldots, b_{l-1}))$$

In this context, l represents the index of the sequence neurons, *hash*() denotes the cryptographic hash function, and pass refers to the password for enhanced security.

Typically, the initial neurons lack any form of protection, whereas the remaining neurons are equipped with built-in protection in the form of weight. Consequently, it is exceedingly challenging to reconstruct information from the training subsets using a direct numerical technique. For this reason, the current characteristics b_l are unknown to the attackers. This method substantially enhances the unpredictability of the response from the "Foe" examples, providing a robust safeguard against data breaches.

Concurrently, it is imperative to situate groups of classical or interconnected neurons at the sequence's commencement, and groups of detectors at its culmination. This is because of the high probability of compromising the ideal and the users' keys, which could otherwise be achieved.

5- Conclusion

This study reviewed the features of the neuroimmune model, identified its advantages, described different training formats, and provided a list of arguments and experimental results, which confirmed its high performance. Identification by keyboard handwriting revealed the higher potential of the proposed model against multilayer artificial neural networks. At the same time, training the proposed model is quite simple, for which the characteristics N_{II} and N_{AI} are used, affecting the reliability of each decision, and characteristics I_{II} and I_{AI}, which establish the timeframe for training and the degree of dependability for all proposed choices.

It is important to note that the objective of this study was not to provide a rationale for the superiority of the proposed system over existing alternatives. The subject under discussion concerns tools that are fundamentally different in design and that are intended to achieve various goals. Furthermore, these tools can be used in a unified system. To illustrate, a deep convolutional neural network may be employed for feature extraction, whereas a flexible neuroimmune model can facilitate identification.

The effectiveness of the proposed system is contingent on a variety of interactions, which are essentially the basis of a classical detector, that is, an analog of neurons. The ideas presented in this paper on reducing the impact of personal data drift owing to changes in the psychophysical states of users may be useful in further research in the field of using trusted artificial intelligence systems in biometric authentication systems.

6- Declarations

6-1- Author Contributions

Conceptualization, E.Yu.L.; methodology, V.Zh.K. and A.N.M.; software, N.Z.I.; validation, E.Yu.L.; formal analysis, I.A.A. and V.Zh.K.; investigation, V.Zh.K. and A.N.M.; resources, I.A.A. and A.N.M.; data curation, E.Yu.L.; writing—original draft preparation, N.Z.I., E.Yu.L., and V.Zh.K.; writing—review and editing, A.N.M. and I.A.A.; visualization, N.Z.I.; supervision, V.Zh.K.; project administration, A.N.M.; funding acquisition, V.Zh.K. All authors have read and agreed to the published version of the manuscript.

6-2- Data Availability Statement

The data presented in this study are available in the article.

6-3- Funding

This work was supported by a grant for research centers in the field of artificial intelligence, provided by the Analytical Center for the Government of the Russian Federation in accordance with the subsidy agreement (agreement identifier 000000D730321P5Q0002) and the agreement with the Ivannikov Institute for System Programming of the Russian Academy of Sciences dated November 2, 2021, No. 70-2021-00142.

6-4- Institutional Review Board Statement

Not applicable.

6-5- Informed Consent Statement

Not applicable.

6-6- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

7- References

[1] Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. IEEE Access, 9, 34541–34557. doi:10.1109/ACCESS.2021.3061589.

[2] Ryu, R., Yeom, S., Herbert, D., & Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. ICT Express, 9(6), 1183–1197. doi:10.1016/j.icte.2023.04.003.

[3] Kurowski, M., Sroczyński, A., Bogdanis, G., & Czyżewski, A. (2021). An automated method for biometric handwritten signature authentication employing neural networks. Electronics (Switzerland), 10(4), 1–19. doi:10.3390/electronics10040456.

[4] Zenisek, J., Holzinger, F., & Affenzeller, M. (2019). Machine learning based concept drift detection for predictive maintenance. Computers and Industrial Engineering, 137, 106031. doi:10.1016/j.cie.2019.106031.

[5] Chen, K., Koh, Y. S., & Riddle, P. (2015). Tracking drift severity in data streams. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 9457, pp. 96–108). Springer. doi:10.1007/978-3-319-26350-2_9.

[6] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4–20. doi:10.1109/TCSVT.2003.818349.

[7] Bharadwaj, S., Amin, P., Ramya, D. J., & Parikh, S. (2024). Reliable human authentication using AI-based multibiometric image sensor fusion: Assessment of performance in information security. Measurement: Sensors, 33, 101140. doi:10.1016/j.measen.2024.101140.

[8] Alshazly, H., Elmannai, H., Alkanhel, R. I., & Abdelnazeer, A. (2024). Advancing Biometric Identity Recognition with Optimized Deep Convolutional Neural Networks. Traitement Du Signal, 41(3), 1405–1418. doi:10.18280/ts.410329.

[9] Gaber, T., Nicho, M., Ahmed, E., & Hamed, A. (2024). Robust thermal face recognition for law enforcement using optimized deep features with new rough sets-based optimizer. Journal of Information Security and Applications, 85, 103838. doi:10.1016/j.jisa.2024.103838.

[10] Bleha, S., Slivinsky, C., & Hussien, B. (1990). Computer-Access Security Systems Using Keystroke Dynamics. IEEE Transactions on Pattern Analysis and Machine Intelligence, 12(12), 1217–1222. doi:10.1109/34.62613.

[11] Gunetti, D., Picardi, C., & Ruffo, G. (2005). Keystroke analysis of different languages: A case study. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 3646 LNCS, 133–144. Springer. doi:10.1007/11552253_13.

[12] Crawford, H. (2010). Keystroke dynamics: Characteristics and opportunities. PST 2010: 2010 8th International Conference on Privacy, Security and Trust, 205–212. doi:10.1109/PST.2010.5593258.

[13] Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. IEEE Access, 12, 64300–64334. doi:10.1109/ACCESS.2024.3395417.

[14] Budžys, A., Kurasova, O., & Medvedev, V. (2024). Deep learning-based authentication for insider threat detection in critical infrastructure. Artificial Intelligence Review, 57(10), 272. doi:10.1007/s10462-024-10893-1.

[15] Alexandrov, I. A., Kirichek, A. V., Kuklin, V. Z., & Chervyakov, L. M. (2023). Development of an Algorithm for Multicriteria Optimization of Deep Learning Neural Networks. HighTech and Innovation Journal, 4(1), 157–173. doi:10.28991/HIJ-2023-04-01-011.

[16] Ding, S., Li, H., Su, C., Yu, J., & Jin, F. (2013). Evolutionary artificial neural networks: A review. Artificial Intelligence Review, 39(3), 251–260. doi:10.1007/s10462-011-9270-6.

[17] Hajinazar, S., Thorn, A., Sandoval, E. D., Kharabadze, S., & Kolmogorov, A. N. (2021). MAISE: Construction of neural network interatomic models and evolutionary structure optimization. Computer Physics Communications, 259, 107679. doi:10.1016/j.cpc.2020.107679.

[18] Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering, 119, 109485. doi:10.1016/j.compeleceng.2024.109485.

[19] Wang, X., Wang, S., Liang, X., Zhao, D., Huang, J., Xu, X., Dai, B., & Miao, Q. (2024). Deep Reinforcement Learning: A Survey. IEEE Transactions on Neural Networks and Learning Systems, 35(4), 5064–5078. doi:10.1109/TNNLS.2022.3207346.

[20] Loufakis, M., Manis, O., Kioroglou, C., Kolokas, N., Ioannidis, D., Tzovaras, D., & Stankovski, M. (2024). Intelligent Model Management: Using Reinforcement Learning to Detect Data Drift and Retrain Industrial Machine Learning Systems. 26th International Conference on Digital Signal Processing and Its Applications, DSPA 2024, Moscow, Russian Federation. doi:10.1109/DSPA60853.2024.10510082.

[21] Liew, S. H., Choo, Y. H., & Low, Y. F. (2019). Fuzzy-rough classification for brainprint authentication. Jordanian Journal of Computers and Information Technology, 5(2), 109–121. doi:10.5455/jjcit.71-1556703387.

[22] Hosseinzadeh, D., & Krishnan, S. (2008). Gaussian mixture modeling of keystroke patterns for biometric applications. IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews, 38(6), 816–826. doi:10.1109/TSMCC.2008.2001696.

[23] Jeanjaitrong, N., & Bhattarakosol, P. (2013). Feasibility study on authentication based keystroke dynamic over touch-screen devices. 13th International Symposium on Communications and Information Technologies: Communication and Information Technology for New Life Style beyond the Cloud, ISCIT 2013, 238–242. doi:10.1109/ISCIT.2013.6645856.

[24] Borodin, A. A., Kabulova, E. G., & Polozhentsev, K. A. (2016). Video detection of problems in the melting of consumable electrodes in a vacuum arc furnace. Steel in Translation, 46(5), 322–324. doi:10.3103/S0967091216050041.

[25] Berto, R. (2014). The role of nature in coping with psycho-physiological stress: A literature review on restorativeness. Behavioral Sciences, 4(4), 394–409. doi:10.3390/bs4040394.

[26] Quigley, K. S., Gianaros, P. J., Norman, G. J., Jennings, J. R., Berntson, G. G., & de Geus, E. J. C. (2024). Publication guidelines for human heart rate and heart rate variability studies in psychophysiology—Part 1: Physiological underpinnings and foundations of measurement. Psychophysiology, 61(9), 1–63. doi:10.1111/psyp.14604.

[27] Bach, D. R., Castegnetti, G., Korn, C. W., Gerster, S., Melinscak, F., & Moser, T. (2018). Psychophysiological modeling: Current state and future directions. Psychophysiology, 55(11), 13214. doi:10.1111/psyp.13209.

[28] Borgianni, Y., & MacCioni, L. (2020). Review of the use of neurophysiological and biometric measures in experimental design research. Artificial Intelligence for Engineering Design, Analysis and Manufacturing: AIEDAM, 34(2), 248–285. doi:10.1017/S0890060420000062.

[29] Ge, Y., Xu, X., Li, J., Lu, X., & Zhang, K. (2007). The effect of secondary task on driving performance, physiological indices and mental workload: A study based on simulated driving. International Conference on Transportation Engineering 2007, ICTE 2007, 38, 491–496. doi:10.1061/40932(246)81.

[30] Rosen, O., & Thompson, W. K. (2009). A Bayesian regression model for multivariate functional data. Computational Statistics and Data Analysis, 53(11), 3773–3786. doi:10.1016/j.csda.2009.03.026.

[31] Bookstein, F. L. (2019). Reflections on a Biometrics of Organismal Form. Biological Theory, 14(3), 177–211. doi:10.1007/s13752-019-00320-y.

[32] Holsapple, C. W., Lee, A., & Otto, J. (1997). A machine learning method for multi-expert decision support. Annals of Operations Research, 75, 171–188. doi:10.1023/a:1018955328719.

[33] Dasgupta, D. (2007). Advances in artificial immune systems. IEEE Computational Intelligence Magazine, 1(4), 40–49. doi:10.1109/mci.2006.329705.

[34] Gehrlein, W. V. (1983). Condorcet's paradox. Theory and Decision, 15(2), 161–197. doi:10.1007/BF00143070.

[35] Revett, K., Tenreiro De Magalhães, S., & Santos, H. M. D. (2007). On the use of rough sets for user authentication via keystroke dynamics. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 4874 LNAI, 145–159. Springer. doi:10.1007/978-3-540-77002-2_13.

[36] Hammad, M., Luo, G., & Wang, K. (2019). Cancelable biometric authentication system based on ECG. Multimedia Tools and Applications, 78(2), 1857–1887. doi:10.1007/s11042-018-6300-2.

[37] Blasco, J., & Peris-Lopez, P. (2018). On the feasibility of low-cost wearable sensors for multi-modal biometric verification. Sensors (Switzerland), 18(9), 2782. doi:10.3390/s18092782.

[38] Marteau, P. F. (2021). Random Partitioning Forest for Point-Wise and Collective Anomaly Detection - Application to Network Intrusion Detection. IEEE Transactions on Information Forensics and Security, 16, 2157–2172. doi:10.1109/TIFS.2021.3050605.

[39] Yu, E., & Cho, S. (2004). Keystroke dynamics identity verification - Its problems and practical solutions. Computers and Security, 23(5), 428–440. doi:10.1016/j.cose.2004.02.004.

[40] Killourhy, K. S., & Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. Proceedings of the International Conference on Dependable Systems and Networks, 125–134. doi:10.1109/DSN.2009.5270346.

[41] Tyapkin, V. N., Ishchuk, I. N., Kabulova, E. G., Semenov, M. E., & Meleshenko, P. A. (2016). Singular Spectral Analysis in Filtration of Noise-contaminated Signals of Pseudolite Navigation. Indian Journal of Science and Technology, 9(46), 107567. doi:10.17485/ijst/2016/v9i46/107567.

[42] Muliono, Y., Ham, H., & Darmawan, D. (2018). Keystroke Dynamic Classification using Machine Learning for Password Authorization. Procedia Computer Science, 135, 564–569. doi:10.1016/j.procs.2018.08.209.