Concealed information detection using EEG for lie recognition by ERP P300 in response to visual stimuli: A review

MARTINA ZABCIKOVA, ZUZANA KOUDELKOVA, ROMAN JASEK
Department of Informatics and Artificial Intelligence
Tomas Bata University in Zlin, Faculty of Applied Informatics
Nad Stranemi 4511, 760 05 Zlin
CZECH REPUBLIC

Abstract: - Nowadays, lie detection based on electroencephalography (EEG) is a popular area of research. Current lie detectors can be controlled voluntarily and have several disadvantages. EEG-based lie detectors have become popular over polygraphs because human intentions cannot control them, are not based on subjective interpretation, and can therefore detect lies better. This paper's main objective was to give an overview of the scientific works on the recognition of concealed information using EEG for lie detection in response to visual stimuli of faces, as there is no existing review in this area. These were selected publications from the Web of Science (WoS) database published over the last five years. It was found that the Event-Related Potential (ERP) P300 is the most often used method for this purpose. The article contains a detailed overview of the methods used in scientific research in EEG-based lie detection using the ERP P300 component in response to known and unknown faces.

Key-Words: - electroencephalography, EEG, lie detection, concealed information detection, EEG-based lie detection, ERP P300, visual stimuli, known and unknown faces

Received: April 19, 2021. Revised: July 11, 2022. Accepted: August 9, 2022. Published: September 9, 2022.

1 Introduction

Recently, there has been much interest from the scientific community in recognizing lies using various methods. An existing device for lie detection is a polygraph measuring the autonomic nervous system's response. However, its accuracy and reliability vary widely across different investigative problems. Subjects can control their physiological responses, and it is impossible to determine precisely whether the subject is lying or not under stress. To overcome this problem, brain signals are used to recognize concealed information in the brain to detect the lie. [1] [2]

Among the frequently used techniques showing their advantages in lie detection are Electroencephalography (EEG), functional Magnetic Resonance Imaging (fMRI), and functional Near-Infrared Spectroscopy (fNIRS). [1] The most commonly used method is EEG. [1] The EEG method is mainly used in medicine for monitoring and diagnosing epilepsy, stroke, seizures, or sleep disorders. However, the EEG method has a more extensive application, for example, in communication and control, entertainment, or security.

The use of the EEG signal for lie detection has been investigated since the end of the 20th century when this area was first focused on by Farwell et al. [2]. Over the last few years, the issue of lie recognition using EEG has developed. Researchers are devising various methods to improve classification and high-quality lie recognition using EEG. EEG signals can reveal many important features of our thinking, making it a better tool for detecting a lie. Recent studies demonstrate the potential applicability of this technology for lie detection. Although this idea originated a few years ago, there are still many opportunities for improvement, such as more powerful classification algorithms, better availability, or lower cost. [2]

Recent improvements in medical imaging methods have improved our knowledge of brain function. These techniques have enabled researchers to create applications based on a better understanding of brain activity. Like DNA or fingerprints, which successfully identify the offender, another suitable option may be to examine the offender's brain. Recent studies have demonstrated that the brain's electrical activity can be a reliable indicator of how information is being processed in the brain and thus identify the perpetrators of a crime. This method could be beneficial and save much time in questioning witnesses and suspects and therefore has great potential in the criminal sciences as a new investigative tool for linking crime evidence with information stored in the offender's brain. Polygraphs and electroencephalographs have a significant advantage over conventional examination methods because they can be used in any case. [2]

It was found that the most frequently used method in this area is Event-Related Potential (ERP) P300. Therefore, the article's primary focus will be an investigation using ERP P300 for EEG-based lie detection. This research was created to provide an overview of recent works dealing with the recognition of concealed information for EEG-based lie detection in the context of ERP P300 in response to known and unknown faces, as there is no overview or summary of current research in this area. This review will serve for further research and identify the most successful and frequently used methods to create an effective fraud identification system.

2 EEG-based lie detection

2.1 Methodology

The main goal of this survey was to summarize the most frequently used methods in studies created for EEG-based lie detection published from January 2017 to January 2022. As far as we know, there has been no available literature containing reviews in the field of EEG-based lie detection focusing on visual stimuli in the last five years. An overview of the most relevant existing information sources in this area was compiled to achieve the survey's main objectives. These were specially selected publications from the Web of Science (WoS) database according to the categories created for this purpose. The following search query was used for search results: (EEG OR electroencephalogra*) AND ((lie OR decept* OR conceal*) AND (detect* OR inform* OR decept*)). Finally, the most relevant articles were selected to analyze the ERP P300 component responding to known and unknown faces for EEG-based lie detection in the last five years.

2.2 Electroencephalography (EEG)

EEG is a noninvasive method for sensing the electrical activity of the brain. Electrodes are placed on the surface of the scalp. This method is most common in medicine but can also be used in other areas such as security, entertainment, emotion recognition, lie detection, communication, or control. Recently, this method has been one of the most used in the field of lie detection.

2.3 ERP P300

Based on the type of stimuli, different types of brain potentials are generated. One of them is ERP. It is a subconscious psychological reaction from a reflex generated in the human brain, measured as a result of a motor, sensory or cognitive event in the brain while processing information from EEG data. [3] [4] [5] Using ERP, brain activation associated with fraud information has been identified and is, therefore, the primary and most widely used method for detecting concealed information. [3] The P300 wave is an intensively studied ERP and is its positive component. The P300 response can be identified as a positive deviation in the EEG signal with a typical latency of approximately 300-1000 ms after stimulus presentation. [7] This response is elicited in the brain only in response to rare and meaningful stimuli in several irrelevant stimuli generating a different response in the subject's brain and is associated with many processes such as attention, recognition, and working memory. [1] [6] [7] Examining the amplitude of the P300 wave then determines if the individual is hiding any information. [3] [4] [5]

ERP P300 is recognized as a potent deception detection tool because they occupy a special place due to its most prominent peak for rare events and offers the possibility of reliable lie detection, which is resistant to countermeasures. [3] [8]

2.4 EEG data analysis

EEG data analysis is a complex process where each part is essential for successful data processing and must be solved consecutively. Fig. 1 shows a schematic overview of EEG data analysis.

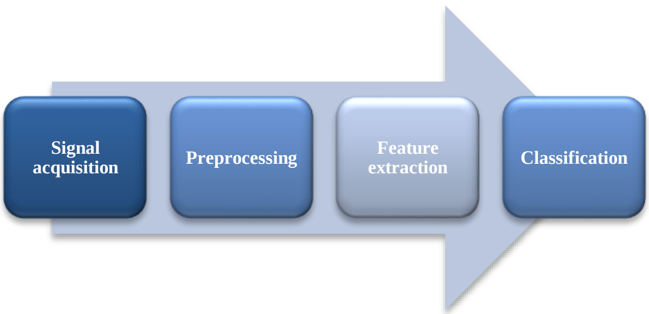

Fig. 1. EEG data analysis process.

- **Signal acquisition**: The first stage is signal acquisition. EEG signals are usually recorded using various acquisition devices such as Biosemi, EasyCap, NeuroSky, OpenBCI, or Emotiv.
- **Preprocessing**: Before proceeding to data analysis, the EEG signal must be preprocessed to remove artifacts and noise mixed with the signal, complicating the analysis of the stimulus-generated ERP P300 response and reducing system performance. [4] A bandpass filter (BPF) [4] [6] [7] [9-14] is the most often used method to remove noise and artifacts.
- **Feature extraction**: It is used to identify complex brain wave patterns, where a useful signal is

selected using a set of parameters, which are then used for classification. In previous EEG-based lie detection studies using ERPs P300, various features in the time, frequency, and wavelet domains have been used to extract information, or a combination thereof, to increase the accuracy and performance of the system. [1] [4] [5] [7] Among the most frequently used are Wavelet Transform (WT) [4] [6] [10] [12], Short-Time Fourier Transform (STFT) [14], Common Spatial Pattern (CSP) [11], Wavelet Packet Transform (WPT) [13] and Hjorth parameters [4] [9].

- **Classification**: The next step is data classification, which is used to determine whether or not the given information is present in the subject. The most frequently used method in this type of research is classification algorithms, where the resulting data are sorted into classification classes, and the effectiveness of the classifiers is tested. [3] [19] The most commonly used classification algorithms include Linear Discriminant Analysis (LDA) [4] [7] [11] [13], Support Vector Machine (SVM) [4] [6] [11], Multi-Layer Feed Forward Neural Network (MLFFNN) [4] [10] [11], Naive Bayes (NB) [11], Deep Belief Network (DBN) [12], Extreme Learning Machine (ELM) [14] and k-Nearest Neighbor (kNN) [9] [11].

2.5 Protocols

Nowadays, scientists use various lie identification techniques to distinguish between guilty and innocent, such as the Concealed Information Test (CIT) [1] [4] [5] [6] [8 - 12] [14] [15] [18] [19], Guilty Knowledge Test (GKT) [3] [7] and Deceit Identification Test (DIT) [13]. These polygraphic techniques detect psychophysiological activities, where the crime details are known only to the guilty subject. [13] They involve a series of questions to identify the subject's behavior. Various studies have performed CIT, GKT, or DIT by creating a mock criminal scenario to identify brain potential changes in EEG's cognitive components. [4] Compared to a polygraph, it is not so easy to deceive, control, or suppress.

The protocols are based on recognizing a particular stimulus, such as a murder weapon, the victim's name, or a victim's photo. [18] The classic paradigm for these protocols includes three categories of stimuli presented to participants called probes, targets, and irrelevant:

- **Probes**: An infrequently occurring rare and meaningful stimulus related to a crime identified only by guilty participants. Probe images act as a stimulus for the subject generating a P300 wave and are images of an object or a familiar face involved in a mock crime leading to strong memory traces. [18]
- **Targets**: A non-criminal stimulus used to gain attention and control whether the subject is cooperating. These irrelevant items are known to all guilty and innocent participants and generate a P300 response. [18]
- **Irrelevant**: A series of irrelevant items shown to all subjects but do not identify them as guilty or innocent because they are unrelated to the crime under investigation and do not generate any P300 response. [18]

It was found that the most commonly used method for analyzing an individual's lying behavior is the CIT method based on the ERP P300 paradigm, where the responses to individual stimuli are examined. If P300 appears, it can be determined that the subject is lying. This method was used, for example, by Bablani et al. [4] [6] [9 - 12] and Dodia et al. [14] to identify fraud.

2.6 Visual ERP P300

Previous studies have further shown that faces can be effectively used as stimuli in the context of ERP P300 to implement an efficacious lie detection system, as the P300 component is sensitive to covert facial recognition. Visual stimuli of known and unknown faces based on P300 elicit different brain reactions and thus help to identify the guilty person, e.g., whether the subject knows the face of a particular person (victim, accomplice, member of a terrorist group). [1] [7] [8] [20]

2.7 The current state of EEG-based lie detection in the context of visual ERP P300

There are a lot of research articles and scientific papers dealing with EEG-based lie detection these days. Many scientists have conducted different tests and applied different approaches to the binary classification of EEG data into guilty and innocent. [9] The following paragraphs will summarize previous studies on detecting concealed information for EEG-based lie detection in the context of ERP P300 in response to known and unknown faces.

Mehrnam et al. designed a new pattern recognition system in response to the ERP P300 wave, which classifies guilty and innocent subjects using the GKT technique. The purpose was to extend the set of properties with nonlinear elements to improve the classification. Signals were recorded from 49 subjects. They used BPF for preprocessing and several morphological characteristics, frequency bands, and wavelet coefficients for feature extraction. A genetic algorithm (GA) was used to select the best set of functions. They performed data analysis only on the Pz channel. The results show that the method correctly classified 91.83% of subjects due to combining basic and nonlinear properties using the LDA classifier and the new adaptive threshold approach. [7]

Bablani et al. proposed an approach to identifying deception by CIT using EEG signals in ERP P300 in response to known and unknown faces. Data collection of 10 subjects was performed using a 16-channel EasyCap device. Signal preprocessing was performed by passing raw EEG signals through a BPF. This work used Hjorth parameters (activity, mobility, and complexity) for feature extraction and kNN as a classifier. After performing the analysis on individual subjects, they achieved an average accuracy of 81.9%. [9]

Bablani et al. also used a deep learning technique using a limited Boltzmann machine with a wavelet to obtain information in the time and frequency domains. They experimented on EEG data recorded by performing CIT using a 16-channel EasyCap device by examining the ERP P300 wave, where subjects were presented with images of known and unknown personalities. EEG signals were preprocessed with BPF and analyzed by WT. To classify EEG data into guilty and innocent people, they developed a DBN, with an average classification accuracy of 81.03% for 10 subjects. [12]

In another study, Bablani et al. analyzed the individual's lying behavior using the ERP P300 and developed a new scenario for CIT. This work included a simulated criminal scenario using a 16-channel EasyCap device to obtain EEG from 10 subjects recognizing the faces of known and unknown personalities. BPF was used to remove signal-mixed noise. They used different extraction techniques of functions in different domains (amplitude, complexity, mobility, frequency, power, wavelet) for a more accurate EEG data analysis. The set framework was developed by aggregating the results of the three best classifiers (LDA, SVM, MLFFNN) from the five classifiers using the classification assessment and the weighted voting (WV) approach. The accuracy of data classification for guilty and innocent of 84.7% was achieved using the proposed framework (3-WV). [4]

Furthermore, Bablani et al. proposed a fraud identification system where EEG data of 10 subjects were obtained when performing CIT for experimental analysis of ERP P300 in recognition of known and unknown personalities. They used BPF for preprocessing data of 16 channels and extracting signals using various extraction methods. Among the various approaches to feature extraction, WT has proven to be the best in combination with SVM. They proposed a new cost function where the BAT algorithm was used to optimize SVM parameters to increase the accuracy of the SVM classification. The BAT binary algorithm was used to select EEG channels. After removing non-functional canals located in the brain's occipital lobe, the system's performance increased to an average accuracy of up to 96.8%. [6]

In another work, Dodia et al. proposed an approach for lie detection using EEG by performing a DIT based on ERP P300 in response to known and unknown faces. The experiment was performed using an EEG acquisition device to collect data from 20 subjects. The signals from the 16-channel EasyCap device were preprocessed using BPF and discretized into waves using WPT. The properties were extracted from detailed coefficients obtained from the WPT and then entered as input to the LDA classifier. The proposed approach for identifying deception using WPT and LDA resulted in a high classification accuracy of 91.67%. [13]

Further, Dodia et al. designed a CIT examining the ERP P300, where signals obtained from 20 subjects detected by a 16-channel EasyCap device were preprocessed using BPF. The experiment included reactions to pictures of celebrities and friends. Then, a STFT method extracted features from EEG signals. Binary BAT was used to select the optimal subset of functions. The acquired set of features was then given as input to the ELM classifier for training the guilty and innocent. The resulting accuracy obtained from the proposed lie detection system was 88.3%. [14]

In another paper, Bablani et al. proposed a hybrid three-stage CIT classification approach that combines the benefits of WT, k-means clustering, and MLFFNN. The test was developed by analyzing the ERP P300 component of EEG data during a fake crime to recognize known faces. EEG data from 10 participants were recorded using a 16-channel EasyCap device for CIT to implement the proposed frame and preprocessed using BPF. The performance of the proposed system provided an accuracy of 83.1%. [10]

In another work, Bablani et al. developed CIT using the ERP P300 component, where subjects observed images of known and unknown faces during the experiment. EEG data of 7 subjects from 10 subjects were used for training and 3 for testing. BPF was used to preprocess the EEG data obtained by the 16-channel EEG cap, and the CSP was used to feature extraction. The fuzzy integrator system was developed using performance indicators of classifiers as predecessors (LDA, MLFFNN, SVM, kNN, NB). Experimental results demonstrated an average classification accuracy of 86.7% for three subjects using the weighted voting approach. [11]

All these studies achieved a high classification accuracy of about 81-97%. An overview and comparison of particular methods for recognizing hidden information for lie detection using EEG in the context of ERP P300 in response to known and unknown faces can be seen in Table 1.

Authors	Protocol	Dataset	Number of subjects	EEG device	Number of channels	Preprocessing	Feature extraction	Classification	Accuracy
Mehrnam et al. (2017) [7]	GKT	Current study dataset	49	Ag/AgCl electrodes	1	BPF	Combination	LDA	91.83 %
Bablani et al. (2018) [9]	CIT	Current study dataset	10	EasyCap	16	BPF	Hjorth parameters	kNN	81.9 %
Bablani et al. (2018) [12]	CIT	Current study dataset	10	EasyCap	16	BPF	WT	DBN	81.03 %
Bablani et al. (2019) [4]	CIT	Current study dataset	10	EasyCap	16	BPF	Combination	3-WV (LDA, SVM, MLFFNN)	84.7%
Bablani et al. (2019) [6]	CIT	Current study dataset	10	EasyCap	13	BPF	WT	SVM	96.8 %
Dodia et al. (2019) [13]	DIT	Current study dataset	20	EasyCap	16	BPF	WPT	LDA	91.67 %
Dodia et al. (2019) [14]	CIT	Current study dataset	20	EasyCap	16	BPF	STFT + BBAT	ELM	88.3 %
Bablani et al. (2020) [10]	CIT	Current study dataset	10	EasyCap	16	BPF	WT	MLFFNN	83.1 %
Bablani et al. (2021) [11]	CIT	Current study dataset	10	EasyCap	16	BPF	CSP	Fuzzy (LDA, MLFFNN, SVM, kNN, NB)	86.7 %

Table 1 Comparison of existing approaches.

3 Results

For EEG-based lie detection using the ERP P300 paradigm in response to visual stimuli of known and unknown faces, researchers in the works mentioned above used different approaches to analyze an individual's lying behavior. They either applied these approaches to multiple canals [4] [6] [9] [10] [11] [12] [13] [14] or only to the Pz canal [7].

Based on the research, it can be stated that the most used method for analyzing the behavior of an individual while lying is the CIT method, see Fig. 2. Furthermore, all selected studies used their own dataset created directly in the given articles. In Fig. 3., we can see that the number of subjects for the experiment was mostly around 10. One of the most frequently used devices for signal acquisition in selected works is EasyCap; see Fig. 4. Fig. 5 illustrates that most selected works focused on 16-channel data. Furthermore, they used the BPF method for preprocessing in all works, allowing only a specific range of frequencies and attenuating frequency values outside this range without reducing the signal quality. Fig. 6 shows that the most widely used method for feature extraction in recognition of concealed information for EEG-based lie detection was the WT method. The most used methods for classification were LDA, SVM, and MLFFNN, see Fig. 7.

All of the above work used machine learning methods and statistical approaches to data in the brain's response to three types of stimuli: probes, targets, and irrelevant to the detection of concealed information stored in the brain. The purpose of the experiments was to find out with what success rate the method helps detect lies. The best results in the binary classification of guilty and innocent classes in the context of ERP P300 in response to known and unknown faces using EEG were achieved by Bablani et al. with an average data classification accuracy of 96.8% using WT for extraction and SVM for classification. [6]

Another notable result is that researchers in this area have recently focused on combining several different methods, technologies, approaches, and algorithms to achieve higher accuracy of EEG data classification for lie detection. The combination of different methods can achieve a better classification than individual techniques. [1] [2] [4]

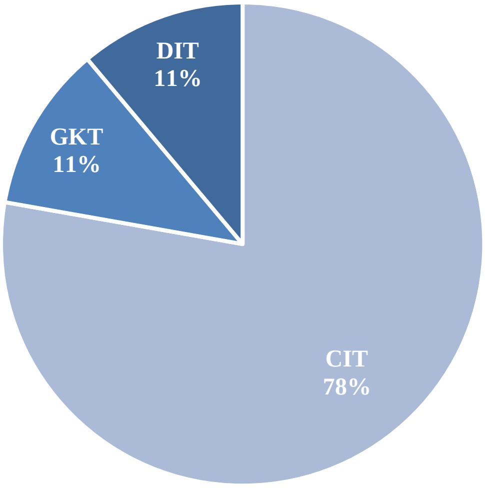

Fig. 2. The most used protocols ranged from 2017 to 2022.

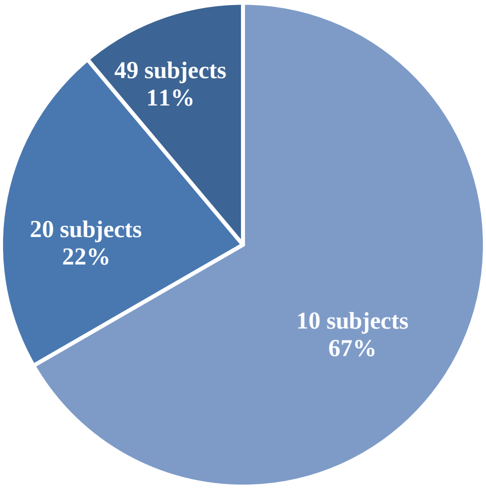

Fig. 3. The most used number of subjects in given experiments.

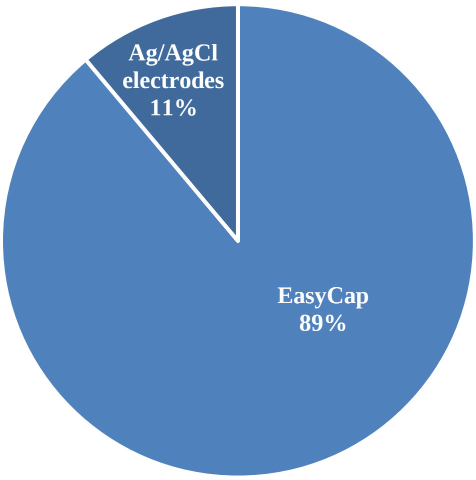

Fig. 4. The most frequently used techniques for signal acquisition.

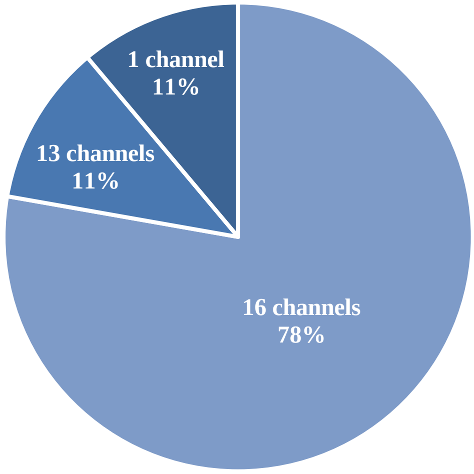

Fig. 5. The most frequently used number of channels.

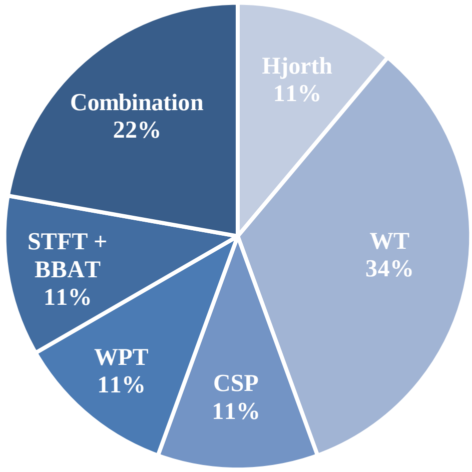

Fig. 6. The most used methods for feature extraction from 2017 to 2022.

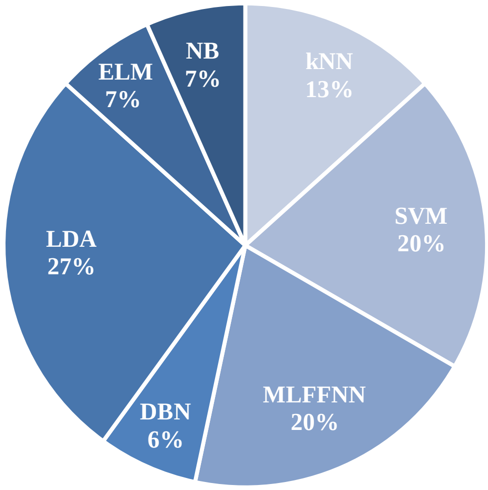

Fig. 7. The most used methods for classification ranged from 2017 to 2022.

4 Discussion

EEG signals can reveal many important features of our thinking, which makes it a better tool for detecting deception. Nowadays, scientists use the ERP P300 method to detect lies, where they examine reactions to individual stimuli. If the P300 occurs, it can be determined that the subject is lying. It is not as easy to deceive, control, or suppress as the polygraph. Most of the work has focused on examining visual stimuli by facial recognition [4] [6-14]. There are many different ways to visually present brain response data. One method often effective in providing a visual representation of differences in brain responses involves plotting the average responses to probe, target, and irrelevant stimuli as voltage over time at a specific scalp location. [2] The probe stimuli are visual stimuli such as pictures of faces, weapons, objects, or names. However, some works have dealt with interviews [26], audiovisual stimuli [17], name recognition [1] [18] [22] [27], autobiographical information [18] [21] [25], or identification of the objects of the crime. [5] [15] [19] Different experiments were created with mock crime scenarios (theft [19] [23] [24]), including the victim's face [4], a murder weapon, the accomplice's name, or a stolen object (coin [15] [19], money, jewelry [5] [16], mobile phone [15] [19], watch [23]). It is ascertained here whether or not the subject participated in the given event or is aware of the crime scene or the given object. [2] [20]

Thanks to the development of wearable devices containing EEG sensors, this technology is more accessible and user-friendly. There are currently several devices with different numbers of channels for obtaining EEG signals, which have been used by scientists in recent years in this field, such as EasyCap [4] [9] [10] [12] [13] [14], Biosemi [1] [8], and Emotiv [3]. Some researchers used only Ag/AgCl electrodes without a headset [7].

The P300 component is often measured at the Pz, Fz, and Cz electrodes in the skull's midline. [8] [15] In previous studies focusing on the analysis of EEG signals, it was found that the maximum amplitude of this component is in the parietal lobe (Pz), the minimum in the frontal lobe (Fz), and takes the mean values in the central lobe (Cz). However, many scientists have focused mainly on analyzing only one Pz channel in the parietal area, where the amplitude of ERP P300 is the highest. [1] [5] [7] [14] [15] [18] [19]

Most researchers have focused on lie detection using various classification methods. However, some have also focused on using statistical methods for detecting lies, such as ANOVA (analysis of variance) [28] or t-test [29]. One of the most frequently used algorithms for classifying binary classes into guilty and innocent (information present or absent) is LDA. [4] [7] [11] [13]

Many authors have also worked on removing artifacts. In order to obtain and then remove the artifacts of blinking and eye movements in the studies, they most often used another measurement method such as EOG (Electrooculogram) [1] [5] [7] [8] [9] [12] [18], which can be divided into vertical EOG (VEOG) and horizontal EOG (HEOG). Eye artifacts obtained by the EOG method were removed using algorithms or visual inspection.

Another important finding is that researchers in this field have recently focused on combining multiple methods, technology approaches, and algorithms in signal analysis for lie detection to achieve a higher classification accuracy of concealed information recognition. Some researchers have focused, for example, on the combination of different methods such as EEG/fNIRS [1], EEG/PPG (Photoplethysmography) [26], and EEG/rTMS (repetitive Transcranial Magnetic Stimulation) [24]. Some have also focused on a combination of algorithms such as SVM, LDA, MLFFNN, NB, and kNN [4] [11] for more accurate fraud detection. By combining different methods, better classification can be achieved than individual approaches. [1] [2]

The evidence presented here and several other studies suggest that recent developments in neuroscience enable researchers to detect information stored in the brain that could noninvasively, objectively, and accurately link criminals to a specific crime. Therefore, this method's potential is to resolve cases faster, more accurately, and more efficiently and provide innocent suspects with noninvasive, stress-free, and reliable means of exemption. [2]

However, even with today's modern methods and algorithms, 100% accuracy of lie detection has not yet been achieved. Despite the high level of classification accuracy that some research has achieved, there are still several opportunities for improvement, such as maximum classification accuracy, lower cost, better availability, reduced time consumption, and real-time use. Using methods for extraction, classification, and selection of elements may be crucial, as a different method is suitable for each type of data processing. Emphasis is placed on the size of datasets, the type of stimulus, or the experiment protocol when selecting methods for extraction and classification. Because each algorithm has a varied computing complexity and data processing time, selecting a classifier can be challenging. The highest success of the binary classification of guilty and innocent data in the context of CIT based on the examination of ERP P300 in response to the recognition of known and unknown faces was achieved by Bablani et al. with an accuracy of 96.8%.

5 Conclusion

The central part of the article was an overview of recent scientific research for EEG-based lie detection using the ERP P300 paradigm in response to known and unknown faces. The CIT method was the most commonly used method for analyzing an individual's lying behavior. It is evident from the survey that all scientists used their own dataset in the selected papers, and all used the BPF method for preprocessing. The experiment's most common number of subjects was around 10, and one of the most frequently used devices for signal acquisition in selected articles is the EasyCap. Furthermore, it turned out that most of the selected works focused on 16-channel data. The scientists used the WT method the most for feature extraction in this context. The LDA, SVM, and MLFFNN algorithms were most often used as classifiers. Another important finding is that researchers in this area have recently focused on combining several methods for EEG-based lie detection to achieve higher classification accuracy. Recent advances in EEG mobile devices have opened the door to many innovations in various applications. The contribution of this study is an overview of the most recently used methods in this area for creating an efficient fraud detection system utilizing visual stimuli of faces. Based on the survey, it can be concluded that this technology has great potential for more effective lie detection.

References:

[1] X. Lin, L. Sai, and Z. Yuan, Detecting Concealed Information with Fused Electroencephalography and Functional Near-infrared Spectroscopy, *Neuroscience*, Vol. 386, 2018, pp. 284–294.

[2] L. A. Farwell, and S. S. Smith, Using brain MERMER Testing to Detect Knowledge Despite Efforts to Conceal, *Journal of Forensic Sciences*, Vol. 46, 2001, pp. 135–143.

[3] S. Anwar, T. Batool, and M. Majid, Event Related Potential (ERP) based Lie Detection using a Wearable EEG headset, *Proc. 2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST),* 2019, pp. 543–547.

[4] A. Bablani, D. R. Edla, D. Tripathi, and V. Kuppili, An efficient Concealed Information Test: EEG feature extraction and ensemble classification for lie identification, *Machine Vision and Applications*, Vol. 30, 2019, pp. 813–832.

[5] N. Saini, S. Bhardwaj, and R. Agarwal, Classification of EEG signals using hybrid combination of features for lie detection, *Neural Computing and Applications*, Vol. 32, 2020, pp. 3777–3787.

[6] A. Bablani, D. R. Edla, D. Tripathi, S. Dodia, and S. Chintala, A Synergistic Concealed Information Test With Novel Approach for EEG Channel Selection and SVM Parameter Optimization, *IEEE Transactions on Information Forensics and Security*, Vol. 14, 2019, pp. 3057–3068.

[7] A. H. Mehrnam, A. M. Nasrabadi, M. Ghodousi, A. Mohammadian, and S. Torabi, A new approach to analyze data from EEG-based concealed face recognition system, *International journal of psychophysiology*, Vol. 116, 2017, pp. 1–8.

[8] A. Alsufyani, O. Hajilou, A. Zoumpoulaki, M. Filetti, H. Alsufyani, Ch. J. Solomon, S. J. Gibson, R. Alroobaea, and H. Bowman, Breakthrough Percepts of Famous Faces, *Psychophysiology*, Vol. 56, 2019.

[9] A. Bablani, D. R. Edla, and S. Dodia, Classification of EEG Data using k-Nearest Neighbor approach for Concealed Information Test, *Procedia Computer Science*, Vol. 143, 2018, pp. 242–249.

[10] A. Bablani, D. R. Edla, V. Kuppili, and D. Ramesh, A Multi Stage EEG data classification using k-Means and Feed Forward Neural Network, *Clinical Epidemiology and Global Health*, Vol. 8, 2020, pp. 718–724.

[11] A. Bablani, D. R. Edla, V. Kuppili, and R. Dharavath, Lie Detection Using Fuzzy Ensemble Approach With Novel Defuzzification Method for Classification of EEG Signals, *IEEE Transactions on Instrumentation and Measurement*, Vol. 70, 2509413, 2021, pp. 1–13.

[12] A. Bablani, D. R. Edla, and V. Kuppili, Deceit Identification Test on EEG Data Using Deep Belief Network, *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2018, pp. 1–6.

[13] S. Dodia, D. R. Edla, A. Bablani, D. Ramesh, and V. Kuppili, An Efficient EEG based Deceit Identification Test using Wavelet Packet Transform and Linear Discriminant Analysis, *Journal of Neuroscience Methods*, Vol. 314, 2019, pp. 31–40.

[14] S. Dodia, D. R. Edla, A. Bablani, and R. Cheruku, Lie detection using extreme learning machine: A concealed information test based on short-time Fourier transform and binary bat optimization using a novel fitness function, *Computational Intelligence*, Vol. 36, 2019, pp. 637–658.

[15] A. Akhavan, and M. H. Moradi, Detection of Concealed Information Using Multichannel

Discriminative Dictionary and Spatial Filter Learning, *IEEE Transactions on Information Forensics and Security*, Vol. 13, 2018, pp. 2616–2627.

[16] J. Gao, J. Song, Y. Yang, S. Yao, J. Guan, H. Si, H. Zhou, S. Ge, and P. Lin, Deception Decreases Brain Complexity, *IEEE Journal of Biomedical and Health Informatics*, Vol. 23, No. 1, 2019, pp. 164–174.

[17] W. Chang, H. Wang, Z. Lu, and Ch. Liu, A Concealed Information Test System Based on Functional Brain Connectivity and Signal Entropy of Audio-Visual ERP, *IEEE Transactions on Cognitive and Developmental Systems*, Vol. 12, No. 2, 2020, pp. 361–370.

[18] G. Lukacs, A. Grzadziel, M. Kempkes, and U. Ansorge, Item Roles Explored in a Modified P300-Based CTP Concealed Information Test, *Applied Psychophysiology and Biofeedback*, Vol. 44, 2019, pp. 195–209.

[19] A. Akhavan, M. H. Moradi, and S. R. Vand. Subject-based discriminative sparse representation model for detection of concealed information, *Computer Methods and Programs in Biomedicine*, Vol. 143, 2017, pp. 25–33.

[20] L. A. Farwell, Brain fingerprinting: a comprehensive tutorial review of detection of concealed information with event-related brain potentials, *Cognitive Neurodynamics*, Vol. 6, 2012, pp. 115–154.

[21] M. Funicelli, L. White, S. Ungureanu, and J. R. Laurence, An Independent Validation of the EEG-Based Complex Trial Protocol with Autobiographical Data and Corroboration of its Resistance to a Cognitively Charged Countermeasure, *Applied Psychophysiology and Biofeedback*, Vol. 46, 2021, pp. 287–299.

[22] A. Alsufyani, K. Harris, A. Zoumpoulaki, M. Filetti, and H. Bowman, Breakthrough percepts of famous names, *Cortex*, Vol. 139, 2021, pp. 267–281.

[23] P. Liu, H. Shen, and S. Ji, Functional Connectivity Pattern Analysis Underlying Neural Oscillation Synchronization during Deception, *Neural Plasticity*, Vol. 2019, 2019, p. 10.

[24] I. Karton, and T. Bachmann, Disrupting dorsolateral prefrontal cortex by rTMS reduces the P300 based marker of deception. *Brain Behavior*, Vol. 7, No. 4, 2017.

[25] Q. Liu, X.G. Zhao, Z.G. Hou, and H.G. Liu, Deep Belief Networks for EEG-Based Concealed Information Test, *Advances in Neural Networks*, Vol. 10262, 2017, pp. 498–506.

[26] M. D. Kohan, A. M. Nasrabadi, M. B. Shamsollahi, and A. Sharifi, EEG/PPG effective connectivity fusion for analyzing deception in interview, *Signal Image and Video Processing*, Vol. 14, 2020, pp. 907–914.

[27] S. Thakur, R. Dharavath, and D. R. Edla, Spark and Rule-KNN based scalable machine learning framework for EEG deceit identification, *Biomedical Signal Processing and Control*, Vol. 58, 2020.

[28] Y.F. Lai, M.Y. Chen, and H.S. Chiang, Constructing the lie detection system with fuzzy reasoning approach, *Granular Computing*, Vol. 3, 2018, pp. 169–176.

[29] W. Chang, H. Wang, Ch. Hua, Qi. Wang, and Y. Yuan, Comparison of different functional connectives based on EEG during concealed information test, *Biomedical Signal Processing and Control*, Vol. 49, 2019, pp. 149–159.

Contribution of individual authors to the creation of a scientific article (ghostwriting policy)

Martina Zabcikova was responsible for the overall research progress and writing the paper.
Zuzana Koudelkova participated in the survey, concept, and verification of the results.
Roman Jasek was responsible for the supervision and conceptualization of the article.

Sources of funding for research presented in a scientific article or scientific article itself

This work was supported by IGA (Internal Grant Agency) of Tomas Bata University in Zlin under the project No. IGA/CebiaTech/2022/006.

Creative Commons Attribution License 4.0 (Attribution 4.0 International , CC BY 4.0)