International Journal of Engineering & Technology, 7 (4.17) (2018) 14-21

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Survey on Computer based Deception Detection Techniques

Sabu George*, Manohara Pai M.M and Radhika M Pai

Department of Information and Communication Technology,
Manipal Institute of Technology,
Manipal Academy of Higher Education, Manipal, Karnataka, India.
**Corresponding author E-mail: sabugeorge24@gmail.com*

Abstract

Deception detection plays a great role in the criminology field and it is a challenge for investigators and researchers for identifying real liar from normal behavior. There is different methods available based on brain, face, voice, etc. each has its own advantages and disadvantages. Most of the lie detection methods are based on the variation of skin resistance, respiratory rate (breath rate), heart beat rate, etc. by the physical contact of some sensors or equipment fixed on the body of the subject. These types of deception detection methods are obtrusive. In case of non-contact deception detection methods there are no sensor used on the body of the subject and the testing is done without the knowledge of the subject being tested. This paper gives a review on all these deception detection techniques.

Keywords: *Deception detection; CIT; GKT; EEG; brain fingerprint; micro-expression; emotional stress.*

1. Introduction

Deception has become a part of life and a kind of character of most of the human beings in various areas of life [1]. So there is a need for automated deception detection in reliable and efficient manner which will benefit in the applications such as interviews, security screening in airport, crime investigation, etc. The focus of the current article is to review various deception detection techniques. There are lot of factors which are closely dependent on lying behaviour of human beings. The analysis of such internal and external factors will help to identify lying behaviour of a person [2], but it is difficult to analyse an experienced lying person. Some of the responses such as fear, stuttering speech, tension, sweating, blood pressure, eye contact, facial micro-expressions and sensory activities of brain may help to analyse a lying person. It is a challenge for crime department and researchers to identify the behaviour of learned and experienced intelligent criminals, since they have lot of tactics to deceive investigators [3]. Therefore, there is a need for developing an effective lie detection system to discriminate the responses of a human from normal to lying behaviour of intelligent liars.

Most of the lie detection methods are based on the analysis of the variation of skin resistance, respiratory rate (breath rate), heart beat rate, etc. by the physical contact of some sensors or equipment fixed on the body of the subject. These types of deception detection methods are obtrusive and due to the effect on the autonomic nervous system (ANS), there is a chance for changing the physiological conditions such as breath rate, heart beat rate, etc. The subject who is being tested may be innocent but feels nervous for being under test. This leads to an inaccurate decision about the liar/innocent subject. There are some other deception detection methods used in which there are no sensors used on the body of the subject and the testing is done without the knowledge of the subject being tested. Such types of deception detection techniques are non-contact type.

Polygraph test is one of the popular method used for lie detection. Guilty Knowledge Test (GKT) and Comparison Question Test (also called Control Question Test (CQT)) are the two standardized protocols used for crime investigation. There are brain based deception detection methods such as functional Magnetic Resonance Imaging (fMRI), EEG modality and brain fingerprinting. Apart from these methods face based lie detection methods such as micro-expression based and thermal facial imaging based methods are also available since face projects internal activities of the human beings. A review of all these methods are done in this paper.

The paper is organized as follows. Signs of deception is presented in Section 2. Deception detection techniques such as polygraph testing, lie detection tests, face based deception detection, brain based deception detection and voice based deception detection are discussed in Section 3. Section 4 includes discussion which compares various methods. Finally, conclusion is given in Section 5.

2. Signs of Deception

In normal case liars do not show physiological signals or universal behaviour in most of the situations [4]. According to the theories of deception, deceivers planned to show both nonstrategic and strategic behaviour. In general, there are some cues to deceit. Following are some other signs of deception [5], in which some of the factors are observed as increased whereas some other factors are observed as decreased. The factors which are observed as increased in liars are: The time lag between answer and question, the speech hesitations such as “aahs”, “ums” or “uhs” between words and liars speak in a higher pitch compared to truth-tellers. The factors which are observed as decreased in liars are: the description of location and time, the reproduction of conversation, the inclusion of auditory and visual details and the specificity of details and quantity. These are general indicators of deception and there is no set of universal signs of deception [6]. A situational contingency is introduced for each deception interaction which

can dramatically alter the interpretation of observed behaviours. For observing signs of deception entire body analysis is required, which includes the analysis of gesture, posture, face, eyes, brain, pulse rate, blood pressure respiration rate and voice as discussed below.

On the observation of gesture and body posture Mircea Zloteanu [7] mentioned that frequent hand to hand touching, frequent face touching, infrequent rigid motion and gesturing, neither over controlled nor distressed relaxed behaviour are the signs of deception [8, 9].

According to the research of facial cues, if liars tried to hide their normal emotions while lying, during that time the micro-expressions may be present on their face [7, 10]. Leaked real emotion or fake smiles also contradict a truthful person's expected emotion [11].

Eye blinks and eye behaviour are very useful cues in deception detection [12, 13, 14]. The dynamics of eye blink, such as blink frequency or rate and blink duration are used as visual cues for spotting deceit [15]. Pupil characteristics are cues of stress or arousal. Pupil dilation is one of them. Deception influences pupillary response which leads to pupil dilation.

In case of deceptive speech, the sound during the speech helps to measure cognition and arousal changes. Vocal Stress Analysis (VSA) is used for the law enforcement for deception detection [16].

Cardiorespiratory pulse rate, respiration rate and blood pressure are reliable indicators of emotional stress. During deceptive communication pulse rate was observed as increased in cardiovascular measures [17]. Related research studies shown that during deceptive situations subjects have the tendency for inhibiting breathing when facing some kind of stress.

The imaging techniques of neuroscience give more insight to brain activities related to cognition, behaviour, etc [18, 19]. Whenever a person sees an object which is familiar for him the P300 brain signal will be triggered [20, 21]. Therefore, to identify concealed knowledge, the event related potential P300 can be used.

3. Deception Detection Techniques

Deception is a complex act and in most of the situations the identifiers of behaviour are contingent. So when attempting to detect deception person dependent factors are to be considered. The strategies of lying may vary according to the situations where lie happens [22]. Also it may vary according to the interview style and power dynamics among the interviewers and subjects. These factors are related to physiological and behavioural responses and the challenge of researcher is to identify these factors and to automate the process of deception detection using computers.

There are different types of deception detection techniques which can be used according to the areas of applications such as interviews, security screening in airport, crime investigation, etc. There are some responses which help to identify deceptive behaviour. Physiological indicators (such as skin conductance, blood pressure, respiration, heart rate), tension, facial behaviours (facial micro-expressions and subtle expressions, eye blink, eye contact, gaze direction, pupil dilation), body movements, gestures, voice and speech characteristics (stuttering speech), verbal statements and style, heat emanation from faces and heads or sensory activities of brain may help to analyse a lying person. By law enforcement many forms of deception detection techniques are used around the world which are based on body contact type and non-contact type deception detection techniques.

In case of body contact type deception detection system sensors are fixed on body of the subject for testing. The sensors give accurate responses, but during the experimentation period the subject is aware that they are being tested for deception detection [23]. This may change the behavior of the subject and countermeasures can be planned. There is a chance for false positive results. Whereas in case of non-contact type deception detection system no sensors are fixed on the body of the subject being tested and the responses of the lying person is detected without his/her knowledge using thermal/visual cameras or remote sensors. Due to this reason non-contact type deception detection systems are more effective. But the sensors which are fixed on the body can detect responses more accurately than the sensors at a remote distance.

3.1 Polygraph Testing

Emotion-based physiological indicators such as blood pressure, heart rate, skin conductivity and sweating are measured in polygraph testing [24]. To test these physiological signals many sensors are fixed to the various regions of the body of the subject being tested. In the test, the graph of the poly (multiple) signals such as pulse, breathing rate, blood pressure and perspiration which are coming from various sensors attached to the body are recorded and analysed. Pneumographs wrapped around the chest of the subject is used to measure depth of respiration and rate. A blood pressure cuff is used to assess cardiovascular activity. Some electrodes are attached to the fingertips of the subjects for measuring the electro dermal response or skin conductivity as shown in the Fig.1.

Fig1: A subject undergoing polygraph test [25]

Initially in the test, the questioner asks some simple 3 or 4 questions to establish the person's signals and polygraph testing is done with real questions. The examiner of polygraph looks at the graph during and after the test and checks for significant changes of vital signs. Increased perspiration, higher blood pressure and faster heartrate indicate that the person is lying. Different people react differently to lying. Here the interpretation of the examiner is subjective. Among the existing deception detection techniques polygraph is widely used, but it is not reliable since it is based on the detection of autonomic reactions. Only well trained examiner can detect lying accurately. Also during the polygraph testing the anxiety levels of the subjects will be high that may lead to false-positive conclusions.

3.2 Lie Detection Tests

Comparison Question Test (also called Control Question Test (CQT)), Concealed Information test (CIT) (also called Guilty Knowledge Test (GKT)) and Reaction Time-based Concealed

Information Test (RT-based CIT) are the protocols used for crime investigation.

3.2.1 Comparison Question Test (CQT)

The Comparison Question Test (CQT) [26] consists of different stages. It is also called control question test. In the first stage the examiner reads the report and speaks to the police investigator to become familiar with the case. At this stage of the test the examiner checks all background information including the suspect's past criminal records. Next stage is pre-test interview. At this stage the examinee will be given a chance to talk about the case and based on the interaction between the examinee and the examiner the actual questions that are to be asked for the test period of the polygraph are framed. Then the testing procedure will be explained by the examiner and the examinee is informed to answer only "yes" or "no" for each question. Next stage is examination stage and at this stage the examinee is attached to the polygraph. In the initial part of this stage a triggered card test is used to convince the examinee that the polygraph is highly accurate. Then a series of questions are asked one by one and the examinee's physiological reactions are measured continuously. Three general types of questions are asked. They are: (1) Relevant questions – "Did you do it?" types of crime related questions, (2) Control questions - "Have you ever taken something that did not belong to you?" types of non-specific questions, and (3) Irrelevant questions – Are you sitting on a chair? [26] types of questions of neutral issues. After asking the questions the questions are repeated for number of times.

The physiological indices used in this test are: relative blood pressure changes, respiration changes and changes in electro dermal activity. Around the upper arm a partially placed cuff is used for analysing the change in blood pressure. Around the abdomen and thorax, a tube is attached which is used for analysing the changes in respiration. On the palmer surface of two fingers two electrodes are placed which are used for analysing changes in electro dermal activity.

The deception versus truth analysed is based on the comparison of control and relevant question responses. Truthful subjects are expected to exhibit more pronounced responses to the control questions whereas deceptive subjects are expected to exhibit more pronounced responses to relevant questions. If a consistent pattern is observed such as longer responses to the control questions means that no deception is indicated and the examinee has answered truthfully, whereas longer responses to the relevant than the control question means the examinee was lying and deception is indicated. Inconclusive decision occurs if there is no difference in the responses to the two types of questions or an inconsistent pattern of response.

3.2.2 Concealed Information Test

The concealed information test (CIT) is also called guilty knowledge test (GKT) which presents a question set which includes one crime related item or critical item and several noncritical items i.e. control items to an examiner. The research shows that the concealed knowledge will inspire responses mainly for the guilty suspects [27]. To understand the crime-related information of the suspects, there are some sufficient techniques which allow for memory assessment of suspects. Guilty subjects possess knowledge about the violation and they can recognize scenes about the violation. So they are unique in comparison to innocent suspects. For instance, a murder can be identified by asking some probe questions such as the murder weapon – the weapon used in the murder. It can be asked among some irrelevant items such as an axe, a rope, a gun, etc. Here only the guilty suspect can distinguish the probe among other items. This approach helps to identify concealed knowledge, which was traditionally known as Guilty Knowledge Test (GKT). In the approach of Verschuere et al. the GKT is also referred as the Concealed Information Test (CIT) [28].

3.2.3 Reaction Time-based Concealed Information Test (RT-based CIT)

In Reaction Time-based Concealed Information Test (RT-CIT) concealed knowledge is detected using the reaction time variations between probes (critical) and irrelevant (encountered) information. In 2012, Visu-Petra et al. conducted a study using reaction time based CIT [29]. In the study they collected and examined the anxiety measures and the individual analysis of functions like working memory, shifting and inhibition in relation to the information of concealing. The analysis has shown that the effect of detection was based on function measures except verbal working memory. Again in 2013, Visu-Petra et al. conducted a study using interface design and they identified the chance to optimise the efficiency of detection of RT-CIT by keep on increasing executive load [30]. They introduced various concurrent tasks experimentally and identified which is essential to conceal information when interrupted and they have shown that there is a system which serves both deceptive responses and executive functioning. The way how an individual conceals is directly related to the efficiency of executive functions.

3.3 Face based Deception Detection Techniques

When a subject starts lying his/her brain activity increases. Due to this, the facial muscle movements also increase and as a result corresponding facial expressions are obtained. The advantage of facial expression based deception detection system is that it is non-contact type, in that no sensors are needed in the body of the subject being analyzed. Face based deception detection system [31] is non-contact type system which helps to capture and analyze deceptive faces without the subject being aware of getting analyzed and is effective and convenient than other deception detection system. Emotional clues and cognitive clues can be considered as behavioral signs of deception [32]. Studies show that genuine expression can be identified from the muscle variations. For example, it is possible to measure the difference between Duchenne Smile or genuine smile and Non-Duchenne Smile or a fake smile. Both the orbicularis oculi muscle (AU6) and the zygomatic major muscle (AU12) stimulation happens for Duchenne smiles, while only stimulation of the zygomatic muscle happens for Non-Duchenne smiles [33]. The eye skin control is performed by the orbicularis oculi muscles and is difficult to position them to the normal smile movement voluntarily. These muscles can move in proper happiness position only for natural feelings. Only an emotion of enjoyment or happiness can move these facial muscles into actual position of happiness. Due to these reasons psychologists have been cataloging facial variations as clues to deception. The advantage of facial expression based deception detection system is that it is non-contact type.

3.3.1 Facial Visual Cues based Approach

A large number of psychological studies have been focused on the facial expression based emotion recognition over the past several decades. Contractions of facial muscles result in appropriate facial expressions of emotions including macro, micro and subtle expression. The expressions are powerful tools for the investigators for analyzing human behavior since they are automatic, immediate and unconscious. The studies show that the emotions such as fear, distress, distrust, disgust or contempt may appear during deception. Ekman identified 46 facial muscles and corresponding Action Units (AUs) are defined and he developed Facial Action Coding System, or FACS [34]. Ekman observed that while lying some of the subjects tried to hide their emotions and during that time micro-expressions are present in their face and he studied their emotional state and concluded that micro-expressions are

behavior cues for deception detection.

3.3.2 Micro-Expression based Approach

Micro-expression is a subtle and brief facial movement that exists around 1/25 to 1/5 of a second when a person conceals an emotion [35]. Ekman studied the emotional state of human being through micro-expressions and he observed that a micro-expression reflects a human's real intent. Therefore, micro expression is a behavioral clue for lie detection [36]. In general, micro-expressions are of low intensity, short duration, and usually local movements. To recognize micro-expression, there are technical challenges. First challenge is to analyze the brief expression, because the micro-expression lasts from 1/25 to 1/5 seconds. A high speed camera helps to capture such a brief expression. Use of 200fps camera assures faster facial motion in more than 10 frames and this time resolution is sufficient for detecting and recognizing the micro-expression. Second challenge is the difficulty in recognizing the subtle variations in facial skin areas using computer vision approaches. For micro-expression analysis databases are available. One of the popular database available for micro-expression is Chinese Academy of Sciences Micro-expression (CASME) Database. The micro-expression database CASME [37] was created by State Key Lab of Brain and Cognitive Science, Institute of Psychology at Chinese Academy of Science in China. Figure 2 shows the frame sequence in the CASME Database.

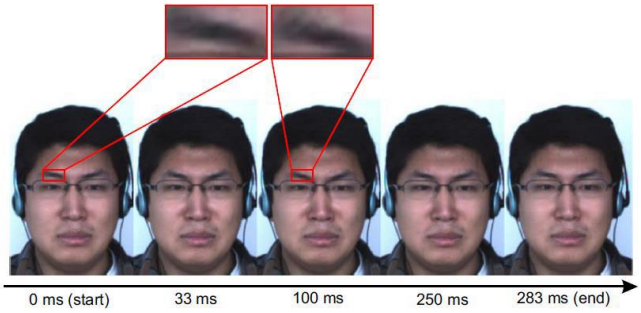

Fig.2: Frame sequence in the CASME database [37]

3.3.3 Eye Blinks as Cue to Deception

Studies show that eye blink has an important role for deception detection. There is a debate over the question of the changes of blink rate during deception. Some of the research have shown that blink rate decreases while lying and whereas some other research show that blink rate increases at the time of deception. Earlier studies of [38], [39] and [40] show that while lying blink rate increases whereas the studies of [41], [42] and [43] show that blink rate decreases during deception. 2013, Marchak [44] observed in mock crime experiments that eye blinks help to detect deception regarding past acts. In 2014, Perelman [45] collected eye blink frequency data via electromyography during the interview. He observed that liars displayed eye blink frequency suppression while lying, while truth tellers exhibited an increase in eye blink frequency during the mission relevant questioning period. Recent study conducted by S. George et al. [15] observed that blink count and blink duration are more while lying.

3.3.4 Facial Thermal Pattern based Approach

Facial thermal image captured using thermal camera is used for the analysis of the facial thermal patterns [46]. Facial thermal image helps to identify and track individual blood vessels and blood flow patterns. In thermal image analysis face is analyzed based on the radiated heat from the face. Blood flow pattern around the eyes are used for deception analysis. In case of thermal facial analysis covered face can also be used. But subjects with eye glasses give wrong results. Some facial makeup power can also reduce thermal emissions.

In 2014 Bashar A. Rajoub et al. [47] used thermal imaging to observe the thermal variations of periorbital region and analyzed a discriminative signature for detecting deception. They proposed a novel methodology by presenting automated deception detection which was validated experimentally on 492 (243 truths and 249 lies) thermal responses extracted from 25 participants. To classify the thermal responses a k-nearest neighbor classifier was used using various strategies for data representation. They tracked the right and left eye corners for a period of 1.7 sec. They reported an 87% ability to predict the truth/lie responses based on fivefold cross validation. Fig. 3 shows a thermal facial image of a subject during questioning.

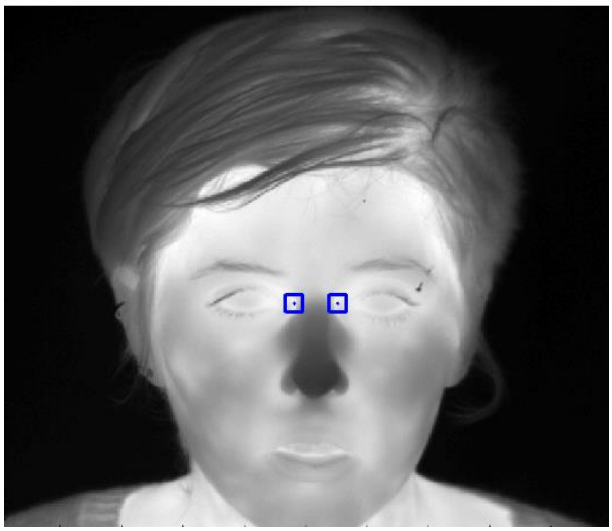

Fig3: A thermal facial image of a subject during questioning [47]

In 2016, Mohamed Abouelenien et al. [48] conducted an experiment for analyzing the region of face where more thermal facial features are available for deceit indication. In their approach they manually located whole face, periorbital regions and forehead of each subject from the 1st frame based on the pixel locations of their boxes for 30 subjects. After locating the three regions the Shi-Tomasi corner detection algorithm is used for detecting points of interest. The varying temperature points are identified and tracked using Kanade Lucas Tomasi (KLT) tracking method. To eliminate the uncertain points and outliers the forward-backward error is also calculated by tracking back and forth points. Geometric transformation was applied for specifying the correct points matching between successive frames in each of the three region's bounding box.

3.4 Brain based Deception Detection Techniques

EEG modality, Brian fingerprint, functional Magnetic Resonance Imaging based lie detection methods are the popular brain based lie detection methods.

3.4.1 EEG based Deception Detection

For brain signals, Electroencephalography (EEG) helps to analyse internal responses of brain as shown in Fig. 4. The electrical potential from each neuron of the brain is recorded by using Electroencephalogram. There are five lobes in human brain namely Parietal (P), Frontal (F), Occipital (O), Temporal (T) and Central (C). These lobes have got important role for internal and external behaviour of human being. When a person is lying the thinking portion of the brain is more active and the analysis of the part of brain which helps for thinking will help to understand deceptive behaviour of human being.

Electroencephalography is the superposition of many signals [50] from the brain and by change of time these signals are detected after the events such as seeing a picture, listening to a sound, etc.

The researchers found that it helps to analyse the background activity of the brain and they proposed the use of event-related variations in EEG and is known as Event Related Potential (ERP) [51]. ERP is useful for analyzing background activity of brain which helps for concealed information detection. The ERP has several components. N1, N2, P1, P2, N300 and P400 are the signals in the ERP. The signals which arise after 250ms refer higher level cognitive process. Whenever a subject sees a familiar object the P300 brain signal will be triggered. The ERP P300 can be used to determine concealed knowledge.

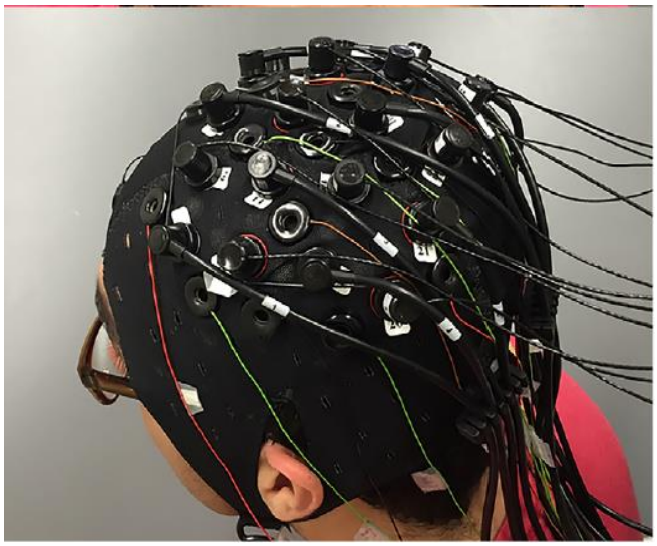

Fig4: A subject undergoing EEG [49]

The imaging techniques of neuroscience give more insight to brain activities related to cognition, behavior, etc. Compared to fMRI method EEG method is more portable and less technical expertise required [52].

3.4.2 EEG-Based Concealed Information Test

Deng Wang et al. [53] proposed EEG based deception detection method. In the method they used concealed information test technique for analysing brain waves just by evoking control and relevant stimuli. The hierarchical knowledge construction algorithm is used for EEG based CIT. In the algorithm, they used supervised learning for high accuracy. There are 11 subjects in the experiment. Each subject was asked to tell 5 numbers that are having 4 digits. Among one number is their year of birth and it was not said which number corresponds to the year of birth till to the end of the experiment. Each number including year of birth is displayed number of times and corresponding EEG signals are recorded and analysed. The algorithm gives low computation time and high classification accuracy which can be used for real time applications.

3.4.3 P300 based Lie Detection Methods

P300 is the most important signal among other types of signals which constitute ERP signal used for lie detection. In 2006, Anna Caterina [54] conducted a study for differentiating the cognitive elements of deception and truth. It focused to evoke high motivation for detection and it was designed to minimize anxiety about being deceptive of subjects. The task was designed as poker-like card game and also according to modified Guilty Knowledge Test. There are 5 subjects in the study and they are given 5 cards. One from each suit of the 4 of the cards are displayed on the computer screen. The identities of these 4 cards are informed in a form of poker, which are known by the researchers. The subjects are given 3 sealed envelopes each having playing cards kept in their hand. Then they are asked to choose the 5^{th} card from the given envelopes. They are informed that if they are successful in concealing the identity of the card they are given $50. The experimenter examined the brain responses of the participants by keep on presenting the cards and asking “Do you have this card?” question. EEG is a nonstationary signal. To analyse deceptive and truthful responses, wavelet transform method is used for the feature extraction of EEG. More reliable results for deception detection is achieved using joint time-frequency features. F3, F4, F7 and F8 are the 4 electrode sites considered for recording the responses of the 5 subjects of the modified version of the GKT. The results show that the differences of truthful deceptive responses identified in the range of frequency corresponds to EEG beta rhythm and within a time window which coincides with the P300 component. The wavelet coefficients corresponding to the beta rhythm are able to distinguish truth and lie in time windows from 0.3 to 1sec post stimulus shows it gives promising result for deception detection.

In 2009, Vahid Abootalebi et al. [55] conducted P300 based Guilty Knowledge Test (GKT). In P300 based GKT, the assumption is that there is a chance to elicit P300 component if the participant has guilty knowledge of the stimuli and ERP with no or small P300 component if the subject has no knowledge about the probe items. Vahid Abootalebi et al. selected 62 subjects and conducted a mock crime experiment. In the scenario without presence of the examiner the subject was given freedom to access the Jewellery box. The guilty participant opened the jewellery box and innocent participant never opened the jewellery box. After that the examiner came back to the room and conducted P300 based Guilty Knowledge Test by displaying 5 different jewellery pictures one by one randomly which contains one target, three irrelevants and one probe. The target was presented to the subject at the time of training. The object in the box was the probe. The subject was asked to press ‘No’ for unknown items and ‘Yes’ for familiar items. The innocent subjects replied honestly and guilty subjects answered falsely. The analysis showed that the amplitude of the P300 to the probe stimuli in guilty subjects are larger than that of the innocent subjects. In 2015, Artha Ivonita Simbolon et al. [56], used ERP method by utilizing P300 signal for analyzing a person is lying or not. In the experiment 11 male subjects are participated. The extracted features of the data sets are trained using SVM and the responses are predicted using test data with the help of a mat lab program.

In 2017 Syed Kamran Haider et al. [57] proposed a P300 based lie detection algorithm. In the experiment they selected 20 subjects and cash, jewellery and smart phone were placed in front of them. Some participants had stolen the item and the university authorities filed case for the stolen item. It was mainly to put the participant under pressure for truth and lie responses. It was informed to the subjects to count the questions asked by the investigator to check whether the subject is mentally attentive and there is no fluctuation in thoughts while acquiring data. That way authenticity of data was achieved. 16 channels Emotiv epoc headset was used for recording EEG data. Field Programmable Gate Array (FPGA) architecture is used for the algorithm implementation which ensures low power consumption and high performance. Linear Discriminant Analysis (LDA) classification is used for P300 component analysis corresponds to each channel of electrode.

3.4.4 Brain Fingerprinting

In case of polygraph test measurement of autonomic arousal such as sweating, heart rate and blood pressure are analysed for guilty knowledge whereas in case of brain fingerprinting electrical brain activity is measured via special sensors contained in a fitted headband. Brain fingerprinting is based on determining whether a person recognizes specific information which is related to an activity or event by measuring responses of electrical brain wave to the pictures or words displayed on a monitor [58]. It was patented by Lawrence Farwell. There is a theory that the reaction of suspect to an activity details or an event will reflect if the subject had earlier knowledge about the activity or event. In this method "Memory and Encoding Related Multifaceted Electroencephalographic Re-

sponse" (MERMER) is used to identify familiarity reaction. Lie detection is one of the applications. Fig. 5 shows a subject undergoing brain fingerprinting. The brain fingerprinting system detects the response called ‘‘Aha!’’ response [58] and its corresponding EEG pattern when a participant identifies a specific crime feature scene, like the weapon used for the crime. It is clear from this idea that the subject is known to the relevant information. The tell-tale response of brain is absent if the participant is not possessing the relevant knowledge.

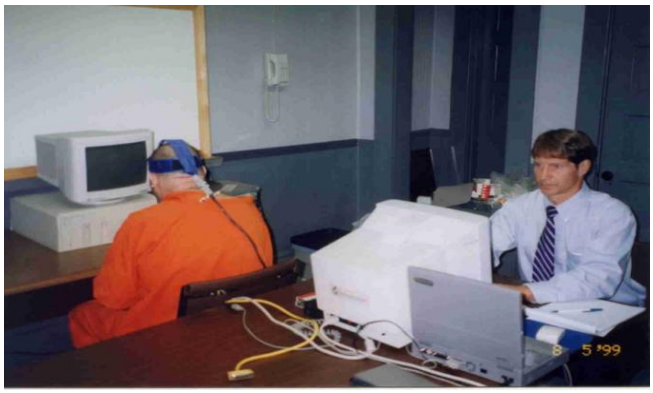

Fig5: A subject undergoing brain fingerprinting [58]

3.4.5 Functional MRI-based Deception Detection

Functional magnetic resonance imaging (fMRI) detects blood flow changes and measures the brain activity [59]. During feigned memory impairment, it helps to analyse the nature of cerebral activation. The deception detection technique used in fMRI is blood-oxygen-level dependent (BOLD). In 2010, Tatia et al. [60] conducted an experiment for analysing neural correlation of lie according to affective information study using fMRI. In the experiment 13 right-handed healthy male Chinese volunteers underwent fMRI while they were lying. They found that neural activity associated with deception is valence-related. Also during deception signal pattern of BOLD was observed about the valence of negative and positive pictures.

3.5 Voice based Deception Detection Techniques

The research shows that emotional stress in voice is an indication of deception. In 2015 Rodellar et al. [61] introduced a method to analyse stress due to alterations in speech. This analysis helps to identify deceptive speech. Deceptive speech and neutral or truthful speech were evoked by forcing to reply politics and society related "hot questions". Fisher's linear discriminant and Log-likelihood ratios analysis were used for processing the data. Independent results for female and male are presented. Results obtained after the classification for neutral speech is around 100%, while for stressed speech classification rate is around 67%.

4. Discussion

There are lot of factors which are closely dependent on lying behaviour of human being. The analysis of such internal and external factors will help to identify lying behaviour of a person. Some of the responses such as fear, stuttering speech, tension, sweating, blood pressure, eye contact, facial micro-expressions and sensory activities of brain may help to analyse a lying person. It is not so easy to identify the responses of the lying behaviour in all cases because d*uring deception an experienced liar* gives ambiguous signals, which confuses the researchers to analyse. So it is difficult to analyse an experienced lying person since they have lot of tactics to deceive investigators [3].

4.1 Non-Contact vs. Body Contact Type Methods

Body contact type detection methods are based on the analysis of the variation of skin resistance, respiratory rate (breath rate), heart beat rate, etc. by the physical contact of some sensors or equipment fixed on the body of the subject. In this type of deception detection system due to the effect on the autonomic nervous system (ANS), there is a chance for changing the physiological conditions such as breath rate, heart beat rate, etc. The subject who is being tested may be innocent but feels nervous for being under test. This leads an inaccurate decision about the liar/innocent subject.

Whereas in the case of non-contact type deception detection methods there are no sensor used on the body of the subject and the testing is done without the knowledge of the subject being tested. The factors which are closely dependent on lying behaviour of human beings are analysed using visual or thermal cameras or some other remote equipment which help to capture various parameters. The non-contact methods help to analyse the subject without the knowledge of the subject being tested. So in non-contact method we get exact emotion since they are not aware that they are being tested. But the camera or other equipment cannot detect much accurately than the sensors on the body. In case of body contact type methods, the sensors give accurate responses, but during the experimentation period the subject is aware that they are being tested for deception detection [23]. This may change the behaviour of the subject and counter-measures can be planned.

4.2 Polygraph Test vs. Voice Stress Tests

People may confuse voice stress test with polygraph test due to the similarity of the questioning test. Polygraph is forensic psycho physiological examination, which collects forensic data of cardiovascular activity, sweat gland activity and respiratory activity whereas subtle changes in voice are analysed in voice stress test. Polygraph is not reliable since it is based on the detection of autonomic reactions. Only well trained examiner can detect lying accurately. Also during the polygraph testing the anxiety levels of the subjects will be high that may lead to false-positive conclusions. The accuracy of the analysis of voice stress is poor and is not reliable for most of the deception detection situations. But voice of subject can be analysed without knowledge of them.

4.3 Face vs. Brain based Approaches

Whenever a person starts lying his/her brain activity increases. Due to this, the facial muscle movements also varies and corresponding facial expressions are obtained. So in face based methods whatever brain activities happen while lying are expressed in face are analysed. Here the advantage is the muscle movements can be captured at remote area without knowledge of the subject. Whereas brain based methods require some sensors to detect brain activities. In brain based methods brain activities can be detected more accurately than face based methods since all brain activities while lying are not available at the face. In brain based methods, the subject is aware that they are being tested for deception. The subject who is being tested may be innocent but feels nervous for being under test. This leads an inaccurate decision about the liar/innocent subject.

The brain activities of a subject can be detected accurately using brain based methods. Whereas non-contact methods help to analyse the actual emotions without knowledge of the subject, but detection accuracy of non-contact methods are less compared to brain based method. Therefore, the method which can accurately read the brain status of a subject remotely without his knowledge is more efficient method for deception detection.

4.4 Visual vs. Thermal Approaches

In visual domain visual camera is used whereas in thermal domain thermal camera is used for capturing facial variations. In visual domain macro, micro and subtle facial expressions are analyzed. Visual analysis of face also includes facial Action Units (AUs), eye blink status and iris properties. An experienced liar may try to hide his expressions and in such situations micro-expression has significant role. Whenever people tried to hide their emotions and during that time micro-expressions are present in their face. So micro expression is a behavioral clue for lie detection since it reflects a human's real intent. Whereas in thermal domain facial thermal image helps to identify and track individual blood vessels and blood flow patterns. In thermal image analysis face is analyzed based on the radiated heat from the face. Blood flow pattern around the eyes are used for deception analysis. In case of thermal facial analysis covered face can also be used. But subjects with eye glasses give wrong results. Some facial makeup can also reduce thermal emissions. In visual domain for analyzing micro-expression high speed visual camera is needed which is expensive, where as in thermal domain special type thermal camera is required which is very expensive than high speed camera.
An interview type psychological experiment was conducted by us in visual domain using a high speed camera with the participation of 62 subjects and the micro-muscle movements were analyzed while lying. The analysis shows that the Action Units such as AU01, AU06, AU09, AU10, AU20, AU23 and AU45 are having significant role while lying. This experiment shows visual domain approach using high speed camera is one of the convenient method for deception detection without the knowledge of the subject being tested.

5. Conclusion

The objective of this survey is to provide a concise introduction to the research towards the methods and techniques of lie detection. Most of the deception detection techniques are based on the variation in the measurement of physiological conditions like skin resistance, breath rate, heart beat rate, etc. by the physical contact of some sensors or equipment fixed on the body of the subject. These types of deception detection methods are obtrusive. In case of non-contact type deception detection methods there are no sensors used on the body of the subject and the testing is done without the knowledge of the subject being tested. In this paper brain, face and voice based deception methods are reviewed. By comparing all these methods, the conclusion is that the method which can accurately read the brain status of a subject remotely without his knowledge is more efficient method for deception detection and such types of methods are not yet developed.

References

[1] Madeline Smith, Jeffrey Hancock, Lindsay Reynolds, and Jeremy Birnholtz, "Everyday deception or a few prolific liars? the prevalence of lies in text messaging" Computers in Human Behavior, vol. 41, no. 3, pp. 220–227, 2014.

[2] Xiang Yu, Shaoting Zhang, Zhennan Yan, Fei Yang, Junzhou Huang, Norah E. Dunbar, Matthew L. Jensen, Judee K. Burgoon, and Dimitris N. Metaxas, "Is Interactional Dissynchrony a Clue to Deception? Insights from Automated Analysis of Nonverbal Visual Cues", IEEE Transactions on Cybernetics, Vol. 45, No. 3, pp. 492-506, 2015.

[3] Mohamed Abouelenien, Veronica Perez-Rosas, Rada Mihalcea, and Mihai Burzo, "Deception detection using a multimodal approach" In Proceedings of the 16th International Conference on Multimodal Interaction, New York, NY, USA. ACM, pp. 58–65, 2014.

[4] Masip J, "Deception detection: State of the art and future prospects", Psicothema, Vol.29, No. 2, pp.149-159, 2017.

[5] Vrij, A., Leal, S., Mann, S., Vernham, Z., & Brankaert, F., "Translating theory into practice: Evaluating a cognitive lie detection training workshop", Journal of Applied Research in Memory and Cognition, Vol. 4, No. 1, pp. 110-120, 2015.

[6] Mohamed Abouelenien, Verónica Pérez-Rosas, Bohan Zhao, Rada Mihalcea and Mihai Burzo,"Gender-based Multimodal Deception Detection", Proceedings of the Symposium on Applied Computing, Marrakech, Morocco, April 03 - 07, 2017, ACM, New York, NY, USA, pp. 137-144, 2017.

[7] Mircea Zloteanu, "Emotions and Deception Detection", Ph.D. Thesis, Psychology and Language Sciences, University College London, UK, 2016.

[8] Wu, Z., Singh, B., Davis, L.S., Subrahmanian, V, "Deception detection in videos", Association for the Advancement of Artificial Intelligence, 2017.

[9] Jackie Hillman, Aldert Vrij, and Samantha Mann, "Um they were wearing : The effect of deception on specific hand gestures". Legal and Criminological Psychology, Vol. 17, No. 2, pp. 336–345, 2012.

[10] Gautam Krishna , Chavali Sai Kumar N V , Bhavaraju Tushal , Adusumilli Venu Gopal , Puripanda, "Micro-Expression Extraction For Lie Detection Using Eulerian Video (Motion and Color) Magnification", Master Thesis, Department of Applied Signal Processing Blekinge Institute of Technology; Karlskrona, Sweden, 2015.

[11] Porter, S., Brinke, L., Baker, and Wallace, B. (2011). Would I lie to you?"Leakage" in deceptive facial expressions relates to psychopathy and emotional intelligence. Personality and Individual, Vol. 2, No.51, pp. 133–137, 2011.

[12] MatthiasGamer, YoniPertzov, "Detecting Concealed Information and Deception Recent Developments", Academic Press, 169-186, 2018.

[13] Frank M. Marchak, "Detecting false intent using eye blink measures", Frontiers in Psychology, Vol.4, Article. 736, pp. 1-9, 2013.

[14] Su, L., and Levine, M. "Does lie to me lie to you? an evaluation of facial clues to high-stakes deception". Computer Vision and Image Understanding, Vol. 147, No.2, pp.52–68, 2016.

[15] Sabu George, Manohara Pai M.M., Radhika M Pai and Samir Kumar Praharaj "Eye Blink Count and Eye Blink Duration Analysis for Deception Detection", IEEE ICACCI, Sixth International Conference on Advances in Computing, Communications and Informatics, Sep. 13 - 16, 2017, Manipal, pp 224-229, 2017.

[16] Savita Sondhi, Ritu Vijay, Munna Khan and Ashok K. Salhan, "Voice Analysis for Detection of Deception", 11th International Conference on Knowledge, Information and Creativity Support Systems (KICSS), Yogyakarta, Indonesia, 10-12 Nov. 2016.

[17] Nidhi Srivastava , Sipi Dubey, "Deception detection using artificial neural network and support vector machine", Biomedical Research 2018, Vol. 29, No. 10, pp. 2044-2048, 2018.

[18] Dominik R.Bach, SamuelGerster, AthinaTzovara and GiuseppeCastegnetti, "A linear model for event-related respiration responses", Journal of Neuroscience Methods, Vol. 270, No.2, pp. 147–155, 2016.

[19] Rumeysa Cakmak and Akram M. Zeki, "Neuro Signal Based Lie Detection", 2015 IEEE International Symposium on Robotics and Intelligent Sensors (IEEE IRIS20I5), 18-20 Oct. 2015, Langkawi, Malaysia, 2015.

[20] Artha Ivonita Simbolon, Arjon Turnip, Jeperson Hutahaean, Yessica Siagian and Novica Irawati, "An Experiment of Lie Detection based EEG-P300 Classified by SVM Algorithm", 2015 International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology (ICACOMIT), Bandung, Indonesia, October 29–30, 2015.

[21] Arjon Turnip and Artha Ivonita, "Online Brain Activity Extraction from EEGP300 Signals with Nonlinear Autoregressive Model", Internet-working Indonesia Journal, vol.8, no.1, pp. 35-39, 2016.

[22] Jiwei Li, Myle Ott, Claire Cardie, and Eduard Hovy, "Towards a general rule for identifying deceptive opinion spam", In Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics, Baltimore, Maryland, 2014.

[23] Vrij, A., and Fisher, R., "Which lie detection tools are ready for use in the criminal justice system?" Journal of Research in Memory and Cognition, Vol. 5, No. 2, pp. 302-307, 2016.

[24] Grubin, D., & Madsen, L., "Lie detection and the polygraph: A historical review". The Journal of Forensic Psychiatry & Psychology, vol. 16, no. 2, 357-369, 2005.

[25] John Synnott, David Dietzel and Maria Ioannou, "A review of the polygraph: history, methodology and current status", Crime Psychology Review, vol. 1, no. 1, pp. 59–83, 2015.

[26] Meijer, E. H., & Verschuere, B., "The polygraph: Current practice and new approaches", Detecting deception: Current challenges and cognitive approaches, Chichester, UK: Willey, pp. 59-80, 2015.

[27] Bruno Verschuere, Ewout H Meijer, "What's on Your Mind? Recent Advances in Memory Detection Using the Concealed Information Test", European Psychologist, Vol. 19, No. 3, pp. 162-171, 2015.

[28] Bruno Verschuere, Ewout Meijer and Armand De Clercq, "Concealed information under stress: A test of the orienting theory in real- life police interrogations", Legal and Criminological Psychology, vol. 16, no. 2, pp. 348-356, 2011.

[29] George Visu-Petra, Miclea, M., Visu-Petra, L. "Reaction time-based detection of concealed information in relation to individual differences in executive functioning". Applied Cognitive Psychology, Vol. 26, pp.342–351, 2012.

[30] George Visu-Petra, Mihai Varga, Mircea Miclea, and Laura Visu-Petra, "When Interference Helps: Increasing Executive Load to Facilitate Deception Detection in the Concealed Information Test", Frontiers in Psychology, vol. 4, no. 146, pp. 1-11, 2013.

[31] Lin Su, Martin D. Levine, "High-Stakes Deception Detection Based on Facial Expressions", 22nd International Conference on Pattern Recognition (ICPR), Stockholm, Sweden, 24-28 Aug. 2014.

[32] Xiang Yu, S. Zhang, Zhennan Yan, Fei Yang, Junzhou Huang, Norah E. Dunbar, Matthew L. Jensen, Judee K. Burgoon, and D. N. Metaxas, "Is Interactional Dissynchrony a Clue to Deception? Insights from Automated Analysis of Nonverbal Visual Cues", IEEE Transactions on Cybernetics, Vol. 45, No. 3, pp. 492-506, 2015.

[33] Sarah D. Gunnery, Judith A. Hall, Mollie A. Ruben, "The Deliberate Duchenne Smile: Individual Differences in Expressive Control", Journal of Nonverbal Behavior, Vol. 37, No. 1, pp. 29-41, 2012.

[34] Moi Hoon Yap, Hassan Ugail and Reyer Zwiggelaar, "Facial Behavioral Analysis: A Case Study in Deception Detection" British Journal of Applied Science & Technology, Vol. 4, No. 10, pp: 1485-1496, 2014.

[35] Senya Polikovsky, Yoshinari Kameda and Yuichi Ohta, "Facial Micro-Expression Detection in Hi-Speed Video Based on Facial Action Coding System (FACS)", IEICE Transactions, vol. E96-D, no.1, pp. 81-92, 2013.

[36] Michel Owayjan, Ahmad Kashour, Nancy Al Haddad, Maurice Fadel, and Ghinwa Al Souki. "The design and development of a lie detection system using facial micro-expressions". 2nd International Conference on Advances in Computational Tools for Engineering Applications, 12-15 Dec. 2012, pp. 33–38, 2012.

[37] W.-J. Yan, Q. Wu, Y.-J. Liu, S.-J. Wang, and X. Fu, "CASME database: A Dataset of Spontaneous Micro-expressions Collected from Neutralized Faces", FG. IEEE, pp. 1–7, 2013.

[38] Kyosuke Fukuda, "Eye blinks: new indices for the detection of deception", International Journal of Psychophysiology, Vol.40, pp. 239-245, 2001.

[39] Thonney J, Kanachi M, Sasaki H, Hatayama T "Eye blinking as a lie detection index in an emotionally arousing context." Tohoku Psychologica Folia 64:58-67, 2005.

[40] Travis L. Seymour, Christopher A. Baker and JoshuaT. Gaunt, "Combining blink, pupil, and response time measures in a concealed knowledge test", Frontiers in Psychology, Vol. 3, No. 614, pp. 1-15, 2013.

[41] Sharon Leal, Aldert Vrij, "Blinking During and After Lying", Journal of Nonverbal Behaviour, Vol. 32, pp. 187-194, 2008.

[42] Leal S, Vrij A , "Blinking during and after lying". Journal of Non-verbal Behaviour, vol. 32, no.2, pp. 187-194, 2008.

[43] Mann S, Vrij A, Bull R, "Suspects, lies, and videotape: an analysis of authentic high-stake liars", Law Human Behavior, vo. 26, no.4, pp. 365-376, 2002.

[44] Frank M. Marchak, "Detecting false intent using eye blink measures", Frontiers in Psychology , Vol. 4, No. 736, pp. 1-9, 2013.

[45] Brandon S. Perelman, "Detecting deception via eyeblink frequency modulation", PeerJ Vol. 2 No. e260, pp. 1-12, 2015.

[46] Kevin K.Park, Hye Won Suk, Heung sun Hwang and Jang-HanLee, "A functional analysis of deception detection of a mock crime using infrared thermal imaging and the Concealed Information Test", Frontiers in Human Neuroscience, vol. 7, no. 70, pp. 1-17, 2013.

[47] Bashar A. Rajoub and Reyer Zwiggelaar, "Thermal Facial Analysis for Deception Detection", IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, 2015.

[48] Mohamed Abouelenien, Rada Mihalcea and Mihai Burzo, "Analyzing Thermal and Visual Clues of Deception for a Non-Contact Deception Detection Approach", "Proceedings of the 9th ACM International Conference on PErvasive Technologies related to Assistive Environments, Corfu, Island, Greece June 29 - July 01, 2016

[49] Buccino AP, Keles HO, Omurtag A, "Hybrid EEG-fNIRS Asynchronous Brain-Computer Interface for Multiple Motor Tasks", PLoS ONE, vol. 11, no.1, pp. 1-16, 2016.

[50] P. Bhuvaneswari and J. Satheesh Kumar, "Influence of Linear Features in Nonlinear EEG Signals", Procedia Computer Science. vol. 47, no. 1, pp. 229-236, 2015.

[51] H Wang , W Chang and Chi Zhang, "Functional brain network and multichannel analysis for the P300-based brain computer interface system of lying detection", Expert Systems with Applications, vol. 53, no. 2, pp. 117-128, 2015.

[52] Rumeysa Cakmak and Akram M. Zeki, "Determining the state of truthfulness and falsehood by analyzing the acquired EEG signals", IEEE 12th International Colloquium on Signal Processing & Its Applications (CSPA), Malacca City, Malaysia, 4-6 March 2016.

[53] D Wang, Duoqian Miao, and Gunnar Blohm, "A New Method for EEG-Based Concealed Information Test", IEEE Transactions on Information Forensics and Security, vol. 8, no. 3, pp. 520-527, 2013.

[54] Anna Caterina Merzagora, Scott Bunce, Meltem Izzetoglu and Banu Onaral, "Wavelet analysis for EEG feature extraction in deception detection", Proceedings of the 28th IEEE EMBS Annual International Conference, New York City, USA, Aug 30-Sept 3, 2006.

[55] Vahid Abootalebi, M Hassan Moradi and Mohammad Ali Khalilzadeh, "A new approach for EEG feature extraction in P300-based lie detection", Computer Methods and Programs in Biomedicine , vol. 94, no. 2, pp. 48–57, 2009.

[56] Artha Ivonita Simbolon, Arjon Turnip, Jeperson Hutahaean, Yessica Siagian and Novica Irawati, "An experiment of lie detection based EEG-P300 classified by SVM algorithm", International Conference on Automation, Cognitive Science, Optics, Micro Electro-MechanicalSystem, and Information Technology, Bandung, Indonesia, 29-30 Oct. 2015.

[57] Syed Kamran H, Malik I Daud, Aimin Jiang and Zubair Khan, "Evaluation of P300 based Lie Detection Algorithm", Electrical and Electronic Engineering, vol. 7, no – 3, pp. 69-76, 2017.

[58] Lawrence A. Farwell, Drew C. Richardson and Graham M. Richardson, "Brain fingerprinting field studies comparing P300-MERMER and P300 brainwave responses in the detection of concealed information" Cogn Neurodyn., Vol. 7, No.4, pp. 263-99, 2012.

[59] Martha J. Farah, J. Benjamin Hutchinson, E A. Phelps and Anthony D. Wagner, "Functional MRI-based lie detection: scientific and societal challenges", Neuroscience and The Law Science and Society, vol. 14, no. 2, pp. 123-131, 2015.

[60] Tatia M. C. Lee, Tiffany M. Y. Lee, ARaine and Chetwyn C. H. Chan, "Lying about the Valence of Affective Pictures: An fMRI Study", PLoS ONE, vol. 5, no. 8, pp. 1-10, 2010.

[61] V. Rodellar-Biarge, D. Palacios-Alonso, V. Nieto-Lluis and P. Gómez-Vilda, "Analysis of emotional stress in voice for deception detection", 2015 International Work Conference on Bio-inspired Intelligence (IWOBI), pp. 127-132, 2015.