Harith H. Thannoon

Dept. of Electrical Engineering,
University of Technology, Iraq.
harthaltai90@gmail.com

Wissam H. Ali

Dept. of Electrical Engineering,
University of Technology,
Baghdad, Iraq.

Ivan A. Hashim (iD)

Dept. of Electrical Engineering
University of Technology,
Baghdad, Iraq.

A Survey on Deceptive Detection Systems and Technologies

Abstract-*There are many types of indicators that have been proven to be useful clues for deceptive detection techniques, and most of this indicators that have been presented and proven by psychology to be signs of lying. This paper presents a survey of most popular deceptive detection systems. Many techniques for lie detection have been presented by researchers; most of them are reviewed in this paper. This study focus on the algorithms, which are presented in some pervious work, and how the database has been collected for each technique, furthermore explain the adopted cues for each deception detection technique. The accuracy of each proposed technique is included in this paper, then this study shows the advantage and disadvantages for each deception system with the useful and robust cues here.*

Keywords- *deceptive detection, clues, database.*

1.   Introduction

High stack lie detection became more popular in the last years especially in the police investigations, security agencies such as the UK border agency, airport and law enforcement in the United States. High stack mean when life of people depends on their answers or may they will have punished with great penalties such as imprisonment. The researcher presented two ways for deceptive detection invasive and non-invasive. Invasive require wires to connect to the human body while non-invasive does not require. There are many types for deception indicators like facial expression, eye blink, blood pressure, heartbeats, temperature, head movement, eye gaze, body language, pupil dilation and voice pitch. The study by one of the scientists of psychology De Paulo [1] showed when people are lying their behavior is different if they telling the truth, his study involve 1338 participants and he was able to identified 158 indicators. Three more techniques to detect a lie has been found by famous scientist Paul Ekman [2]. The datasets had been used in deception detection research were few and none of them made available in public. Researchers in this area often collect their dataset and use it in their own experiment.

The main challenges of deception detector, in general, are the number of participants and accuracy. From the Table 1 that contains the summary of some previous work, where the high accuracy was in [4] when they used facial micro-expressions, but the number of participants was small when compared with others [5]. The highest number of participant is shown in table 1 with reasonable accuracy and both of them used facial expression (Eye blink is part of facial expression).

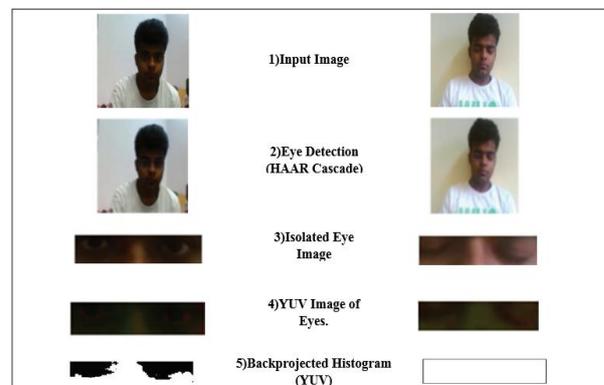**Table 1: Summary of the previous work**

Technique	year	No. of participants	Features Details	Detection Accuracy
Thermal Imaging[3]	2012	16	Inner and outer edges of eyes, nostrils outer edge, nose tip, mouth outer edges	83.5%
Facial Micro-Expressions [4]	2012	4	Five expression	85%
Brain activity [5]	2013	18	Beta wave	---
Facial Expressions [6]	2014	37(Database collect from YouTube 324 video)	Two Emotion (sadness and happiness)	76.92%.
Temperature Change [7]	2014	11	Nose area	84%
Eyeblink Count [8]	2015	5	Eye close and open during the interview	---
Head movement [9]	2015	10	Head position and movement during an interview	58.25%
Brain Activities [10]	2015	11	Event Related Potentials (ERP) based on signal P300	70.83%
Brain Activities [11]	2016	5	Functional Near Infrared Spectroscopy (FNIRS) and NeuroImage	60%
Voice Analysis [12]	2016	12	fundamental frequency(F0) and Formants frequencies	72%
Eyeblink [13]	2017	50	Eyeblink count and duration	70%

1. General Block Diagram of the Deception Detection System

The general block diagram for the deception detection system is shown in Figure 1. The first stage is the input such as video recorded of a subject, audio recording, brain signal, or heart rate signal…etc. The second stage is the data acquisition system, in order to transform the real world signals (physical state) into electrical signals that are measured and converted into a digital format for processing, analysis, and storage by a computer. The pre-processing is used to prepare the signals (that obtain from data acquisition system) to the feature extraction stage, for instance if the input was video in the pre-processing step needs to cut a portion of the video and define the regions of interested that content features like face or eyes. In feature extraction stage the cues that used to discriminate lies from honesty needs to be extract for example if the deception detection system based on facial expressions in feature extraction step the appearance and geometry features of the subject's face are extract. Where, these features are the input to the final stage. Decision maker, which is a classifier, that used the input feature to make decision if the subject was lying or telling the truth.

2. Deception Detection System Based on Eye Blink Cues

The increase in the cognitive demand leads to decrease in eye blink rate which is shown by biopsychology sciences [14,15]. When participants were asked to memorize an 8-digit number, blinked less compared to when they memorized a 4-digit number [15]. Deception detected using blink rate is presented in [8], this technique was implemented by using image processing with MATLAB, HAAR Cascade algorithm was used to detect eyes, by using skin detection algorithm can identify the state of eye open or close in the next step blink rate has been calculated. Finally, the result compares with threshold value and decide the participant was lying or telling truth. Five subjects were chosen to test the system and they minimize the complexity of the system by using a very good quality camera such that it must be directly facing the face of subject and he/she not be wearing any glasses were the lighting conditions are sufficiently bright. Figure 2 show simulation results of the proposed technique

Figure 1: General block diagram of deception system

(a) Open eyes detection.   (b) Close eyes detection.

Figure 2: The simulation results and the steps of the proposed method

Eye blink count and eye blink duration were used for deception detection as presented in [13]. Fifty subjects were participant in their study. The subjects were selected based on the General Health Questionnaires (GHQ-5) score should be less than 1 on 5-item, any subject who has neurological disorder was not selected. High-speed camera used that capture 66 frames per second, the image size set to 640*480. Various facial muscles were presented using Action Units (AUs), AU45 is represent eye blink. Viola Jones algorithm was used for face detection. Active Shape Model (ASM) algorithm was used in their experiment for detect landmarks and for analysing AU45. The results showed for most participants their eye blink count and duration were increase when they are lying. Table 2 show the summary results for the proposed system. The flow chart of the deception detection system based on eye blink is shows in Figure 3.

Table 2: Results of the proposed system

Gender	Blink Type	Blink Duration	Blink Count
Male	No blink detected	21.98%	
	Blink detected (Truth)	30.01%	25.99%
	Blink detected(Lie)	48.01%	52.03%
Female	No blink detected	20%	
	Blink detected (Truth)	34%	31.3%
	Blink detected(Lie)	46%	48.7%

```
┌─────────────────────────────────┐
│     Input Image From Camera     │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│          Eye Detection          │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│        Thresholding Image       │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│      Morphological Filtering    │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│     Open/Closed Eye Detection   │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│  Threshold Value Of Blink Rate Is Set │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│  Blink Rate in Target Period Measured │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│   Comparison With Threshold Value │
└─────────────────────────────────┘
                 ↓
┌─────────────────────────────────┐
│          Lie Detection          │
└─────────────────────────────────┘
```
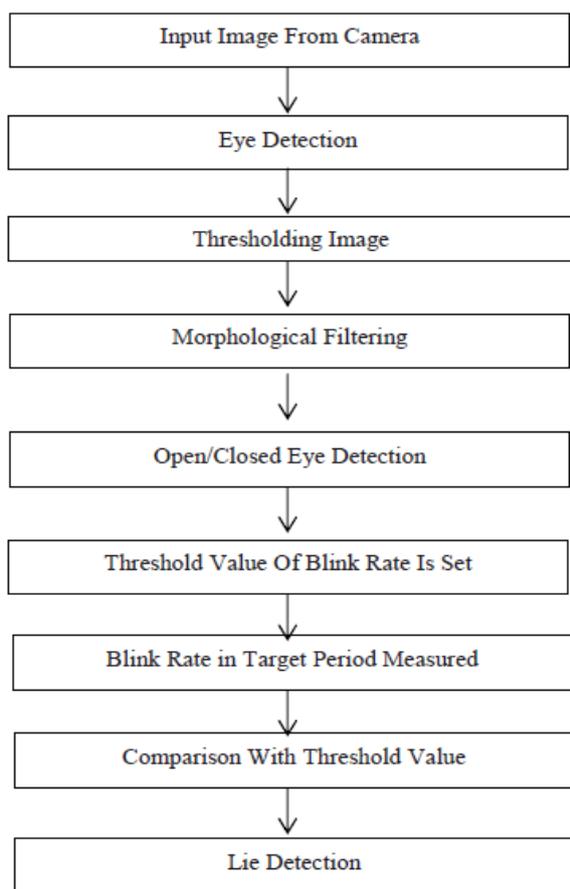
Figure 3: Overview of Lie Detection Technique

3. Deception Detection System Based on Head Movement

There are different patterns of head movement as a signs of lying. This technique was presented in [9], this paper included study of lie detection based on head movement and how the specific head movements patterns used as indicator to deception. They use C# as programming language to build their algorithms for detect and estimate head movement. After converting first frame into grayscale form the face was detected by apply Viola-Jones algorithm, then the interest region and the centroid were selected by calling the Convex Hull function. Face Tracking was done by Flavio's optical flow algorithm. Another centroid was computed to the next frame and the difference between these centroid is compute and compare with threshold, based on this difference between the centroid of two consecutive frame the head position can be detect and estimate. Ten volunteers were used for testing the algorithms, the algorithm should learn the patterns of head movement of lie and truth responses before testing it in order to give reliable result. Figure (4) show the detection points and the two centroids point.
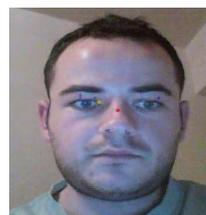

Figure 4: The red point is the centroid of the first frame, which is the reference point; the yellow point represents the centroid of the analyzed frame, which is used for computing actual position of the head, the blue points that are used as references to compute the centroids

4. Deception Detection System Based on Brain Function

Two technologies of lie detection based on brain activities Functional Near-Infrared Spectroscopy (FNIRS) and Event Related Potentials (ERP) were proposed. The ERP technique was proposed in [9] to detect lying. MATLAB used as program language to build the algorithms of the technique. Signal P300 is the most important signal for ERP to detect lying. Offset was remove from P300 signal as pre-processing step, band pass filter is used to specify the information of lying within the ranges from 0.3 Hz to 30 Hz. Independent Component Analysis (ICA) was used for separating data from being overlap at the electrodes. Five characteristics of signal P300 that obtain from applying feature extraction step: maximum amplitude, mean amplitude, minimum amplitude, median amplitude, and mode amplitude. Finally, Support Vector Machine SVM method used in classification by measuring the distance between the nearest pattern from each class and the corresponding hyperplane. Figure (5) show the different in P300 signals between a liar and non-liar subjects.

In [11] the FNIR technology and new method of mock lying protocol were presented. The Target of their study was to distinguish the difference in hemodynamic response of human brain activity while a subject answers lie and true. At the beginning, the head band FNIR was put on forehead, it had two rows of detectors the bottom row will be located just above the eye brows, the total activation of the brain (of the Prefrontal Cortex PFC) can be detect by these detectors. Sixteen positions of PFC activation can be identifying by 16 individual channel use for acquire the brain signal from PFC to calculate the Hemodynamic activation, the chromophore concentrations are taken.
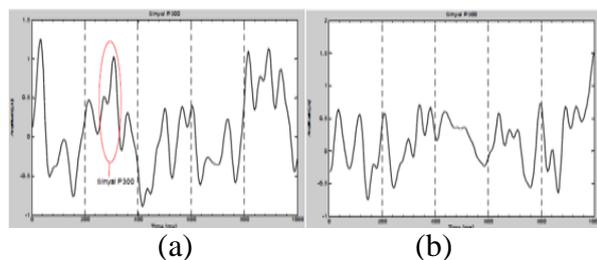
**Figure 5: P300 signals (a) Signal for lying subject
(b) Signal for innocent subject**

Low pass rectangular window FIR filter is used to make the signal smooth. The outcomes from this study first, the lying subject took more time than telling the truth. Second, the untruth signals are more standard deviation of the total oxygenation than that of truth answer. Third outcome the activation ranges of lie answer is much more than that of truth answers. Five healthy subjects were participated in this study; they asked to answer a set of questions by writing.

5. Deception Detection System Based on Temperature

Thermal imaging technology can be used to detect deceptive as proposed in [3]. The changes in skin temperature was captured using Thermal camera. Due to different in temperature between The face of the subject and background the thermal camera show difference color of the warm face and Cool background based on this difference face can be easy detect, after that the predefine landmarks were located on the face (the outer eye edges, the inner eye edges, the outer nostrils edges, the nose tip, and the outer mouth edges) the benefit of this landmarks is for calculating face dimensions. Window (50x100 pixel, height width) was selected as region of interest (ROI) including both tear ducts. The average of temperature of the 10% from the hottest pixels in the ROI was computed for every frame, which represent the main temperature changes in the inner eyes corners of the vasculature. Matched filter used to more clearly detect P-Thermal style that they discovered it in thermal signals of the liar subject. Bootstrapped Amplitude Comparison (BAC) method used to determine whether P-Thermal amplitude triggered by lie-probe(Pm) is higher than the amplitude triggered by an irrelevant set(Im).The decision depend on the disparity between the maximum values of Pm and Im with compare to threshold value, in this study they computed 100 Pm and 100 Im values for each subject and they calculate the maximum values for Pm and Im then compare it with threshold value to determine the subject was lying or telling the truth. They

reach an accuracy of 83.5%, 16 subjects were participants in this study.

In [7] lie was detect based on temperature change in the nose region. Eleven subjects were participant in this study. Thermo Vision infrared camera is used to record temperature change while subjects ask to answer equations. After the system was fully calibrated the subjects were asked to wear sunglasses and sit down to face the camera, the purpose from wearing sunglasses in order to easy nose detection. Subjects were asked to answer fifteen questions three different times, first for truth response, second for lie response, third for lie and truth response (lie in certain questions and tell the truth in others). Two different methods of deception detection were presented in the paper. First method they analyze the nose temperature by using time domain analysis. After acquire the temperature from the nose by infrared camera plotted it versus the time. The theory is that the temperature increase (corresponds to peaks in the graph) when a person lies, then peak detector algorithm is use to detect lies this method had an accuracy of 69%. The second method they analyze the nose temperature using frequency domain analysis by taking Fourier transform of the signal and plot magnitude versus frequency. Low pass filter used because high power noise seen, to implement this filter time domain convolution was used. Finally, peak detector algorithm is used to detect deceptive, number of lies was detected. They achieve an accuracy 84% by using second method.

6. Deception Detection System Based on Facial Expression

Facial behavior can indicate particular mental state. When one is being deceitful she/he is making up something in the brain, this results in increased brain activity, and this results in increased physiological responses which can be measured on the face(as cues to deception).Deception detection based on facial expressions was presented in[6].They presented an automated computer vision based on four cues for deception (eyebrow, eye-blink, mouth motion and winkle occurrence).The database were collected from high-stakes deception videos of real-world situations.

They distinguishing deception and honesty based on specific emotions (sadness and happiness), they used Facial Action Coding system (FACS) to distinguish between fake and genuine emotions of sadness and happiness regard to its facial Action Units (AUS) and they used these facial features as potential indicators for deception

detection. Accuracy was achieved 76.92% by using this technology.

Involuntary expressions can be used to detect deception as proposed in [4], these expressions appear on the human face when lying, and they designed an automated vision system to detect micro-expression that used to discriminate lying subjects from the innocent. Subject ask to sit in front the camera for detecting all possible muscle changes. LabVIEW program is used to convert video into frames for analysis. To make key features of the expression, templates of geometric based features on some parts of the face were used. Vision assistant block is used to save the frame as image, then processes this image based on to predefined templates.NI IMAQ Vision Assistant used to predefine the templates and represent some face regions on the: the eyebrows edges, the eyes edges, the mouth edges, and the cheeks. When the program fined templates, it measures nine various distances among the center points of the templates, then the program saves these distances individually into separate arrays. The system checks the distance difference for first element of each array to detect specific emotion. For instance, during a smile, the horizontal distance of mouth expands and the eyes close a bit. If the same expression is iterated less than five consecutive times, it is signed as a micro-expression, which indicates that the subject was lying.

7. Deception Detection System Based on Voice Analysis

Deception was detecting by identify the voice parameters which are reliable indicators of stress due to deception as proposed in [12]. They visited police station and record voice of twelve subject without knowledge of them. By using Audacity 2.0.3 software removed the voice of police inspector and background disturbances. They used PRAAT software (version 5.3.56) for further analysis. They selected parameters for measures were fundamental frequency of voice (F0), formants frequency F1 and F2, shimmer, jitter. Their results indicate that mean F0 was increase with stress due to deception. F1 and F2 were increase under stress but not for all subjects. Jitter was found decrease under stress. Shimmer did not show any noticeable impact of stress.

8. Conclusions

Datasets must be collect from high-stake deception videos of real-word situations that can give accurate cues for deception detection. The use of invasive technique to detect deceptive probably leads to give inaccurate information because this technique required to connected wires to the participant body which makes him confused and afraid during the interview and this potentially giving false cues the misreading of the sensors that touch the human body lead to a miss prediction to detect deception.

Non-invasive technique does not have the problems that mentioned as in invasive system, but it needs to be careful when using this technique especially with facial expression because no single cue can be used as a reliable indicator for deception detection. It is possible to combine two methods or more to generate more convincing cues to deception and this will give more accuracy result. The combination of facial expression, micro-expression, eye gaze, facial thermal and some other methods in one system, this system expected to give high accuracy. Some people tend to move their eyes significantly and clearly during lying so when observing the eyes (during interview) of this type of people the probability to detect lie is high, while other people can be easily observed the change in temperature of their face during lying,while others their facial features change clearly and quickly when they lie. Therefore, the system that observe all these clues to detect deception will fit all these types of people and produce a reliable deception detection system.

Causal Productions is credited in the revised template as follows: "original version of this template was provided by courtesy of Causal Productions (www.causalproductions.com)".

References

[1] B.M. DePaulo, B.E. Malone, J.J. Lindsay, L. Muhlenbruck, K. Charlton, and H. Cooper, "Cues to Deception," Psychological Bulletin, Vol. 129, No. 1, pp. 79-118, 2003.

[2] P. Ekman, "Deception, lying, and demeanor," States of Mind: American and Post-Soviet Perspectives on Contemporary Issues in Psychology, pp. 93-105, 1997.

[3] U. Jain, B. Tan, Q. Li, "Concealed knowledge identification using facial thermal imaging," IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1677-1680, 2012.

[4] M. Owayjan, A. Kashour, N. Al-Haddad, M. Fadel, and G. Al-Souki, "The Design and Development of a Lie Detection System using Facial Micro-Expressions," IEEE International Conference on Advances in Computational Tools for Engineering Applications, pp. 33 – 38, 2012.

[5] S. Amir, N. Ahmed and B.S. Chowdhry, "Lie Detection in Interrogations Using Digital Signal Processing of Brain Waves," in 3rd International Conference on Instrumentation, Communications, Information Technology and Biomedical Engineering (ICICI-BME) IEEE, Indonesia, 2013.

[6] L. Su, M.D. Levine, "High-Stakes Deception Detection Based on Facial Expressions," IEEE International Conference on Pattern Recognition, pp.2519 – 2524, 2014.

[7] Y. Azar, and M. Campisi, "Detection of Falsification Using Infrared Imaging: Time and Frequency Domain Analysis," IEEE International Conference on Advances in Computing, Communications and Informatics, pp. 1021–1026, 2014.

[8] B. Singh, P. Rajiv and M. Chandra, "Lie Detection Using Image Processing," IEEE International Conference on Advanced Computing and Communication Systems, pp. 1-5, 2015.

[9] D. NOJE, R. MALUTAN, "Head movement analysis in lie detection," IEEE Conference Grid, Cloud & High Performance Computing in Science (ROLCG), pp. 1-4, 2015.

[10] A.I. Simbolon, A. Turnip, J. Hutahaean, Y. Siagian, and N. Irawati, "An Experiment of Lie Detection based EEG-P300 Classified by SVM Algorithm," IEEE International Conference on Automation, Cognitive Science, Optics, Micro Electro-Mechanical System, and Information Technology,pp. 68 – 71, 2015.

[11] M.A. Rahman, M. Ahmad, "Lie Detection from fNIR Signal and NeuroImage," IEEE International Conference onMedical Engineering, Health Informatics and Technology (MediTec), pp. 1-6, 2016.

[12] S. Sondhi, R. Vijay, M. Khan, and A. K. Salhan, "Voice Analysis for Detection of Deception," IEEE International Conference on Knowledge, Information and Creativity Support Systems, pp. 1 - 6, 2016.

[13] S. George, M. Pai, R.M. Pai, and S.K. Praharaj, "Eye Blink Count and Eye Blink Duration Analysis for Deception Detection," IEEE International Conference on Advances in Computing, Communications and Informatics, pp. 223-229, 2017.

[14] E.H. Rauch, "Cues to Decception: Eye Blinking," Master Thesis, San Francisco State University, California, 2015.

[15] M.K. Holland, G. Tarlow,"Blinking and Mental Load," Psychological Report, Vol. 31, No. 1, 1972.