Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 08 | Issue 02 | October-2025

Exploring the Effect of Mode of Crime - Online vs. Offline on Detection of Deception by Eye Detect System (EDS)

Rohini Kumar[1]

Available online at: www.xournals.com

Received 30th October 2025 | Revised 30th October 2025 | Accepted 31st October 2025

Abstract:

The present study aimed to explore the effect of the mode of crime, online versus offline, on the detection of deception by the Eye Detection Test (EDS) from a forensic psychological perspective. Participants were divided into two groups: Group A, instructed to commit a mock crime offline and lie during the EDS test, and Group B, instructed to commit a mock crime online via a social media platform (Instagram) and lie during the EDS test. Sampling was conducted using a random sampling method, resulting in a total of 12 participants divided equally between the two groups. Participants were tasked with performing the mock crime within a specified time frame and were subsequently evaluated using the EDS test. Analysis of the collected data suggests that the Eye Detection Test is efficient in detecting various types of deception. Given the limited existing research in this area, there is significant scope for further investigation. This research could potentially aid in preventing the wrongful punishment of innocent individuals who may falsely confess under pressure.

Keywords: Eye Detection Test, Forensic psychology, deception detection, online crime, offline crime, mock crime, lie detection, social media, investigative psychology, criminal behavior.

Authors:

1. *Sri Ramachandra Medical College and Reseach Institute*

Introduction

Deception Detection system is widely applied in different areas related to security, hiring new employees for business, criminal investigation, law enforcement, anti-terrorism, and others. The available detection of deception technology is either verbal or non-verbal. The verbal detection of deception technology and methods use speech, while non-verbal features are related to facial expressions, eye gaze, head moments, eye blinking and other body gestures. The non-verbal technology of Detection of Deception is important as it is difficult to manipulate the non-verbal communication like eye-behaviour, micro-expressions, etc. According to Ford (2006) one of the first methods to prove the veracity of a statement uttered by the accused was described in China circa 1000 BC (3). According to Forensic Psychological perspective, there are two types of deceptions, which are low-stakes (face saving) and high-stakes (malicious deception). Deception happens in both small and big situations, making it tricky in forensic and security work. It involves showing fake information by copying reality, making up new things, or diverting attention. Understanding these tricks is important for catching lies in investigations and keeping things safe and secure. (1)

In forensic psychology, detecting deception involves investigating whether someone is lying or telling the truth. Deception is divided into three types:

1) Stating Untruths - The act of providing false information.

2) Concealing the truth- it refers to the act of omission, choosing not to voice the truth by concealing at least some relevant facts. Purposefully concealing of the truth.

3)Paltering-it falls in the middle between deceiving by an act of commission and deceiving by omission. In Forensic Psychology, common deception detection techniques include polygraph tests, eye-tracking, speech analysis, and emotional response analysis.

Understanding these types helps experts analyse behaviour and statements to uncover deception during investigations. (2)

Deception frequently stems from three primary emotions: fear, guilt, or delight. These emotions can drive individuals to conceal or manipulate the truth in various situations, whether to avoid consequences, cover up wrongdoing, or gain advantage. Understanding the underlying emotions can provide insight into why someone might engage in deceptive behaviour.

In the present study, we explored the effect of the mode of crime, specifically online versus offline, on the detection of deception using the Eye Detect System (EDS). Our aim is to determine the efficiency of this deception detection tool in distinguishing between online and offline modes of crime. Cybercrime covers a wide range of illegal activities done using computers or the internet, like stealing information or money, threatening people, or bullying online. It's been increasing over the past 20 years, causing a lot of trouble, and costing a ton of money. Besides financial losses, cybercrime also hurts people emotionally and mentally through things like cyberbullying and online threats.Integrity-related cybercrimes involve actions that mess with the trust or accuracy of information, like changing data or spreading lies online. Perpetrators might do it for money, revenge, or just to cause chaos.

Computer-related cybercrimes target computer systems or networks, like hacking or spreading malware. Motives can include making money, spying, or pushing certain beliefs. Content-related cybercrimes involve sharing harmful or illegal stuff online, like cyberbullying or spreading hate speech. People do these crimes to harass others, push their beliefs, or intimidate people. The division of crimes related to the use of the internet into cyber-enabled crimes and cyber-dependent crimes may seem easy, but the types and forms of offenses within each category can vary significantly. In this article, we will explore the meanings of both cyber-enabled crimes and cyber-dependent crimes, as well as provide examples of each.

Cyber-enabled crimes are basically traditional crimes, but computers or the internet make them bigger or able to reach more people. Unlike cyber-dependent crimes, you don't always need computers to commit them. Fraud and theft are two common examples of cyber-enabled crimes that you might have heard about a lot. (4)

There are various types of cyber-enabled frauds:

Electronic Financial Frauds: This includes online banking frauds and internet-enabled card-not-present (CNP) fraud. CNP fraud happens when transactions occur remotely over the internet, without the physical presence of the card or the cardholder. E-commerce frauds, which involve fraudulent financial transactions related to online retail sales, also fall into this category. Both businesses and customers can be victims of these frauds. (4)

Fraudulent Sales on Online Platforms: This involves scams on online auction or retail sites or through fake websites. Sellers may offer goods or services that they never provide, or they may sell counterfeit products while claiming they are authentic. Online ticketing fraud is another example of misrepresentation in online retail. (4)

Mass-Marketing Frauds and Consumer Scams: These include advance fee scams like the infamous 419 frauds, inheritance frauds, fake charity or disaster relief scams, fake lotteries, and pyramid schemes. In these scams, individuals are tricked into giving money upfront with the promise of receiving a larger sum later. (4)

Phishing Scams: Phishing scams involve fraudulent emails that pretend to be from legitimate sources and ask for personal or corporate information, such as passwords or bank account details. These emails aim to deceive recipients into revealing sensitive information. In some cases, attackers personalize their phishing attempts by gathering specific information about their targets, a tactic known as spear-phishing, to increase the likelihood of success.

Cybercriminals may target access credentials to corporate accounts, including usernames, passwords, and other authentication details. Once they gain access, they can perpetrate fraud through unauthorized transactions, manipulation of financial records, or even business email compromise (BEC) schemes.Protecting these types of data requires robust cybersecurity measures, including encryption, multi-factor authentication, regular security audits, employee training, and implementing best practices for data handling and storage. Additionally, organizations should stay vigilant for emerging threats and continuously update their defences to mitigate the risk of cyber-enabled data theft.

Cyber-dependent crimes are illegal activities that can only happen using computers or other tech gadgets. These crimes involve using these devices to carry out the offense and targeting them to cause harm. For example, making and spreading harmful software to make money, or breaking into computer systems to steal, mess up, or delete data or disrupt online activities.

Cyber-dependent crimes can be divided into two main types:

- Illicit intrusions into computer networks - refers to unauthorized access or breaches into computer systems or networks. This involves entering digital spaces without permission, often for malicious purposes such as stealing sensitive information, disrupting operations, or causing damage. E.g.: hacking
- Disrupting or damaging computer functions and online spaces, such as using malware or launching Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks.
- Cyber-dependent crimes are carried out by various entities for different motives, such as:
- Skilled individuals or groups who create and distribute software to attack computer systems for criminal purposes or to assist others in doing so.
- Individuals or groups with advanced skills but non-malicious intentions, like hacktivists using cyber means to protest.
- Individuals or groups with limited skills who utilize cyber tools developed by others.
- Organized crime syndicates.

Most cyber criminals possess relatively low levels of technical expertise. However, their attacks are becoming more prevalent due to the expanding online criminal marketplace. This platform offers easy access to advance the knowledge, empowering less skilled cybercriminals to exploit various vulnerabilities effectively. (5)

Cyber-dependent offenders rely on samples drawn from either student populations or organizational employees. Consequently, many of these studies focus on relatively low-level acts of cyber-dependent crimes. These offenses include activities such as guessing passwords to computers, emails, and social media accounts, misusing computers, and computer networks, and violating information security policies. These provide valuable insights into the behaviours and motivations of individuals engaging in cyber-dependent offenses, it's essential to recognize the limitations of generalizing findings from these populations to more serious cybercrimes. Cyber-dependent offenses committed by individuals may not fully capture the complexity and severity of cybercrimes such as hacking, malware distribution, online fraud, and cyberstalking, which can have significant societal and economic impacts.

Studies identify various key actors who facilitate the illicit activities of cyber-dependent criminals. These enablers encompass coders or programmers of malicious software, distributors and vendors who trade and sell hacking tools and stolen data, teachers who exchange information regarding cyber-dependent crime techniques and tools, as well as moderators and administrators of online marketplaces who maintain the criminal infrastructure, vouch for the goods, and enforce social norms in these marketplaces.

Online offenders and enablers of cyber-dependent crimes often convene in both offline and online environments. For instance, Leukfeldt and colleagues (2017) examined Dutch police records involving investigations of cybercriminal groups and found that cyber-dependent crime offenders residing in nearby neighbourhood's often gather in various locations throughout the city. However, despite these offline interactions, online forums and markets remain central to facilitating interactions and recruitment efforts between offenders and enablers (Hutchings & Holt, 2015).

Under the Information Technology Act (IT) Act 2000 stated that both cyber-dependent and traditional crimes are recognized, and it outlines certain actions that are considered unlawful:

a) Unauthorized Access: If an individual, without permission from the owner or any authorized person, accesses a computer, computer system, or computer network, and downloads, copies, or extracts any data, computer database, or information from it, it is deemed an offense.

b) Source Code Theft or Alteration: Similarly, if someone steals, conceals, destroys, or alters any computer source code used for a computer resource with the intention to cause damage, it constitutes a violation under the IT Act.

These provisions aim to safeguard digital assets and prevent unauthorized access, theft, or manipulation of computer resources and data.

The National Crime Records Bureau (NCRB) has recently released its annual report titled "Crime in India for 2022," offering a comprehensive overview of crime trends in the country. Here's a summary of the key findings:

Total Cognizable Crimes: Over 58,00,000 cognizable crimes were registered in 2022, including offenses under the Indian Penal Code (IPC) and Special & Local Laws (SLL). This marked a 4.5% decline compared to 2021.

Crime Rate Decline: The crime rate per lakh population decreased from 445.9 in 2021 to 422.2 in 2022, indicating a drop in overall crime rates adjusted for population growth.

Safest City: Kolkata retained its position as the safest city in India for the third consecutive year, with the lowest number of cognizable offenses per lakh population among metropolises. Pune and Hyderabad secured the second and third positions, respectively.

Suicides and Causes: India witnessed a concerning increase in suicides, totalling over 1.7 lakh cases in 2022, reflecting a 4.2% rise compared to 2021. The suicide rate also increased by 3.3%. Major causes included family problems, marriage-related issues, bankruptcy, unemployment, and illness. Maharashtra reported the highest number of suicides, followed by Tamil Nadu, Madhya Pradesh, Karnataka, Kerala, and Telangana. Daily wage earners, agricultural workers, farmers, and unemployed individuals were among the most affected groups. Additionally, over 12,000 student suicides were reported in the year.

These findings highlight both improvements and challenges in the realm of crime and public safety in India, emphasizing the need for continued efforts to address emerging threats such as cybercrime while tackling underlying socio-economic issues contributing to suicides.

MATERIALS AND METHODOLOGY:

Materials Required: EDS INSTRUMENT, CONSENT FORMS, DEMOGRAPHIC DATA

Site of the study: Department of Forensic Psychology, CFSL KOLKATA.

Sampling: For the present research, samples were selected by simple random sampling method. A total of 12 participants will be selected and divided them into two groups Group A- 6 Offline participants and Group B – 6 Online participants.

Type of the study: Experimental Study

Period of the study: 1 month

Hypothesis – There is no significant difference in the detection of deception by EDS, identified in different modes of crime – Online Vs offline.

METHOD OF SAMPLE SELECTION : Random Sampling

Inclusion criteria: Able bodied and age criteria 18 to 60 years who had studied English till class 12 and are fluent in reading and understanding English.

Exclusion criteria: Participants with health issue or people with disability were not considered.

Procedure:

An Experimental research design with two groups was employed. The participants were divided into Group A and Group B, each consisting of 6 participants selected randomly. Group A comprised offline offender, and Group B comprised online offenders. A mock crime scenario was set up in the Psychological Division with a sample size of 12.

Group A, participants were instructed to steal a Rs. 500 notes placed in Room 1 within a time limit of 5 minutes, without carrying any items in hand. If successful, they were allowed to keep and use the Rs. 500 notes. If unsuccessful or exceeding the time limit, they did not receive the Rs. 500 notes. This task was designed to assess participants' proactiveness and problem-solving skills. Subsequently, the EDS test was conducted by the researcher, and the obtained results were noted for analysis.

For Group B, online offenders were randomly selected. Participants were tasked with committing the mock crime through Instagram, using the provided username and password on the computer. Information to be sent to the victim was available on the device, and participants had 5 minutes to complete the task. After completion, the EDS test was conducted by the researcher, and the obtained results were noted for analysis.

The study aimed to compare the deceptive behaviours of offline and online offenders using the EDS Direct Lie Comparison Test, and differences in deception levels based on the mode of crime.

Result and Discussion:

The results obtained from both Group A and Group B, indicate that the accuracy in online mode is higher compared to offline mode. Specifically, the accuracy in online mode was 100%, while in offline mode, it was 83%. However, it's important to note that this difference may be attributed to the limited sample size collected for the research.

In both online and offline crime scenarios, participants had a minimum education qualification of 12+ and possessed high reading skills. The age range of participants varied from 20 to 35 years, and all participants had a good understanding of computer usage.

In Group A, consisting of six participants, 5 were female and 1 was male. Only 1 participant out of the 6 was able to complete the mock crime scenario provided. The results from Group A indicated that 3 participants were deemed Not Credible, while 3 were deemed Credible.

In Group B, also consisting of six participants with 5 females and 1 male, 2 participants successfully completed the mock crime scenario. The results from Group B showed that 2 participants were deemed Not Credible, while 4 were deemed Credible. From the present study, it can be inferred that the accuracy rate for detecting deception online is 100%, whereas the accuracy rate for offline deception detection is 83%.

S.NO	NAME	AGE	GENDER	GROUP A OFFLINE	GROUP A ONLINE	TASK COMPLETED	RESULT
1	R	23	FEMALE	OFFLINE	-	NO	NOT CREDIBLE - DECEPTIVE
2	S	23	FEMALE	OFFLINE	-	NO	CREDIBLE- TRUTHFUL
3	P	23	MALE	OFFLINE	-	NO	CREDIBLE- TRUTHFUL
4	K	22	FEMALE	OFFLINE	-	NO	CREDIBLE- TRUTHFUL
5	H	21	FEMALE	OFFLINE	-	YES	NOT CREDIBLE - DECEPTIVE
6	G	22	FEMALE	OFFLINE	-	NO	NOT CREDIBLE - DECEPTIVE
7	D	26	FEMALE	-	ONLINE	NO	CREDIBLE- TRUTHFUL
8	R	24	FEMALE	-	ONLINE	YES	NOT CREDIBLE - DECEPTIVE
9	P	31	FEMALE	-	ONLINE	YES	NOT CREDIBLE - DECEPTIVE
10	R	22	FEMALE	-	ONLINE	NO	CREDIBLE- TRUTHFUL
11	R	21	MALE	-	ONLINE	NO	CREDIBLE- TRUTHFUL
12	K	23	FEMALE	-	ONLINE	NO	CREDIBLE- TRUTHFUL

Based on the provided data, the types of crime serve as the independent variable, while the classification of Truth/Deception acts as the dependent variable. Since the detection rates for both types of crimes were comparable, there appears to be no significant distinction in detecting deception based on the crime type.

TYPE OF CRIME	ONLINE	OFFLINE	TOTAL
TRUTHFUL	4	3	7
DECEPTIVE	2	3	5
TOTAL	6	6	12

DISCUSSION

The aim of this research was to evaluate the efficacy of the Eye Detect System in discerning various types of deception and to assess the levels of deception among offenders, regardless of whether their crimes were committed online or offline. The primary objective is to investigate how the mode of crime, whether it occurred in an online or offline setting, influences the detection of deception. A proper result was not able to be generated as the sample size was 12. In both online and offline crime scenarios, participants had a minimum education qualification of 12+ and possessed high reading skills. The age range of participants varied from 20 to 35 years, and all participants had a good understanding of computer usage. In Group A, consisting of six participants, 5 were female and 1 was male. Only 1 participant out of the 6 was able to complete the mock crime scenario provided. The results from Group A indicated that 3 participants were deemed Not Credible, while 3 seemed Credible. In Group B, also consisting of six participants with 5 females and 1 male, 2 participants successfully completed the mock crime scenario. The results from Group B showed that 2 participants were seemed Not Credible, while 4 were seemed Credible.

Limitations

The study consisted of only 12 samples. For more specific and generalization result , bigger sample size should be taken . The study was based on a mock crime scenario which may not have bought in genuine emotions. There is a possibility that a real case scenario would produce more genuine emotions. The study was conducted in the lab , so limited population were only called upon. If the study had more population the required results could be obtained

CONCLUSION

In this study, researchers evaluated the effectiveness of the Eye Detect System in detecting various forms of deception. This was a small-scale experiment conducted with a homogenous sample comprising individuals working or interning at CFSL, Kolkata. The findings suggest the need for further research to generalize the results and draw conclusions regarding the ability of the Eye Detect System to accurately detect different types of deception.

References:

Podlesny, John A., and David C. Raskin. “Effectiveness of Techniques and Physiological Measures in the Detection of Deception.” *Psychophysiology*, vol. 15, no. 4, July 1978, pp. 344–59. https://doi.org/10.1111/j.1469-8986.1978.tb01391.x.

Lee, So-Hyun, et al. “Understanding Cybercrime From a Criminal’s Perspective: Why and How Suspects Commit Cybercrimes?” *Technology in Society*, vol. 75, Sept. 2023, p. 102361. https://doi.org/10.1016/j.techsoc.2023.102361.

“Cyber Crime: A Review of the Evidence Summary | Exercises Statistics Docsity.” *Docsity.com*, 2022, www.docsity.com/en/docs/cyber-crime-a-review-of-the-evidence-summary/8800256/. Accessed 2 Nov. 2025.

Vicianova, Martina. “Historical Techniques of Lie Detection.” Europe’s Journal of Psychology, vol. 11, no. 3, 20 Aug. 2015, pp. 522–534, www.ncbi.nlm.nih.gov/pmc/articles/PMC4873061/, https://doi.org/10.5964/ejop.v11i3.919.

Maimon, David, and Eric R. Louderback. “Cyber-Dependent Crimes: An Interdisciplinary Review.” *Annual Review of Criminology*, vol. 2, no. 1, Oct. 2018, pp. 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

NCRB’s Crime in India 2022 Report.” Drishti IAS, www.drishtiias.com/daily-updates/daily-news-analysis/ncrbs-crime-in-india-2022-report