THREAT ANALYSIS AND SECURITY OF PERSONAL DATA USING USER DEVICES WITH EYE-TRACKERS

DOI: 10.36724/2072-8735-2023-17-8-56-62

Ilya Safonov,
Moscow Technical University of Communications and Informatics, Moscow, Russia

Mikhail Vyatkin,
Moscow Technical University of Communications and Informatics, Moscow, Russia

Olesya Hizhenkova,
Moscow Technical University of Communications and Informatics, Moscow, Russia

Kseniya Nezhivleva,
Moscow Technical University of Communications and Informatics, Moscow, Russia, ***k.i.nezhivleva@mtuci.ru***

Igor Vlasuyk,
Moscow Technical University of Communications and Informatics, Moscow, Russia

Manuscript received 08 June 2023;
Accepted 07 July 2023

Keywords: *data personalization, data protection, privacy, eye-tracking, information security*

Eye-tracking technology has been extensively used in web development, marketing, and gaming mechanics because of the ability to obtain data regarding the trajectory and gaze fixation points. Eye movement information may be effectively used to study complex cognitive processes and human visual perception. However, a significant issue of leaking user privacy has arisen with the expansion of eye-tracking technology. Since the technology can obtain highly sensitive information regarding user behavior and preferences, measures for protecting personal data are required. At the current stage of the development of technology, research on threats and means to ensure the security of personal data has become a high priority in this field. Proper diligence in the development and use of eye-tracking devices is becoming an integral part of the process. Potential threats associated with collecting, storing, and transmitting information about users' gaze should be considered. Various methods have been proposed to ensure the security of personal data through the use of eye-tracking devices. The anonymization of data, which is the removal or replacement of personal identifying elements, appears to be among these. Transparency and user agreement to the collection and use of gaze data has also been an important aspect. This can be accomplished by explicitly providing information about the purpose of the data collection and the ability to control privacy. Threats related to the use of eye-tracking technology were considered, providing methods of ensuring the security of personal data. These are important steps in the development of the field to protect user privacy while improving the safety and ethics of using eye-tracking devices.

Для цитирования:
Илья Сафонов, Михаил Вяткин, Олеся Хиженкова, Ксения Неживлева, Игорь Власюк. Анализ угроз и средств обеспечения безопасности персональных данных при использовании пользовательских компьютеров со встроенными устройствами отслеживания взгляда // T-Comm: Телекоммуникации и транспорт. 2023. Том 17. №8. С. 56-62.

For citation:
Ilya Safonov, Mikhail Vyatkin, Olesya Hizhenkova, Kseniya Nezhivleva, Igor Vlasuyk. Threat analysis and security of personal data using user devices with eye-trackers. *T-Comm*, vol. 17, no.8, pp. 56-62.

Introduction

The ubiquitous use of eye-tracking technology enables novel methods of interaction across a variety of devices. However, a possible privacy problem arises related to the collection of a considerable amount of personal information. Modern eye-tracking technologies have been available for decades and have been used in neuroscience, psychology, marketing studies, and simulations, as well as in game development and various research studies [1, 2, and 3]. Since 2009, the prices of eye-tracking devices have been falling, which has contributed to the rapid spread of the technology. Although eye-tracking devices are increasingly becoming popular, the loss of privacy is not transparent and evident to the average user and requires special attention. In accordance to statistics, more than 96 billion data records have been compromised on the Internet since 2009, and the number of users exposed to identity theft will increase every year [4].

The human gaze is unique for revealing subconscious activity which is complicated to control. Other human activity signals can be easily masked. The person can change voice, appearance, and force by pressing keys, however, the gaze can be controlled only partially [5, 6, 7]. The complexity of falsification demonstrates the considerable significance of user data being collected by third-party websites without the subject's agreement. The problems associated with understanding the privacy consequences of the ubiquitous usage of eye-tracking technology and the compromise between the accuracy and velocity of gaze-based authentication require an urgent solution to ensure the information security of subjects on the Internet.

The principle of operation of the eye tracking device

The eye tracker is a device which is installed or embedded in a user's equipment for measuring the position and movement of a human's eyes, or in other words, for determining the position of a user's gaze on a screen.

The eye tracker consists of cameras, light sources, and algorithms. A schematic representation of the positioning of the eye-tracking device is shown in Figure 1. The light sources produce a pattern of near-infrared light on the eyes. The cameras perceive an image of the user's eyes and the model. The image processing algorithm analyzes the peculiarities of the user's eyes and the reflection model. On the basis of the data, mathematical algorithms compute the eye position and gaze position.

Eye-tracking is a technology for tracking eye positions, also called gaze line or gaze point tracking technology. Eye-tracking is a sensor technology that is required to determine the point of the user's gaze in real-time. Visual attention direction is a piece of valuable information, which can be applied to a variety of purposes. The experience has demonstrated that the gaze of a person immersed in reflection is independent of the focus of consciousness [8]. The technology converses eye movements into a data stream containing information including eye position, gaze vector for each eye, and gaze point.

The eye tracker uses near-infrared light which is projected onto the eye and then uses a high-resolution camera to record the direction where the light is reflected from the surface of the cornea. A schematic representation of the human eye and eye tracker is shown in Figure 2. The data collected from eye-tracking devices are often provided in the format of coordinates and time, while variations of the device also exist which provide additional information, such as changes in pupil size [9, 10].

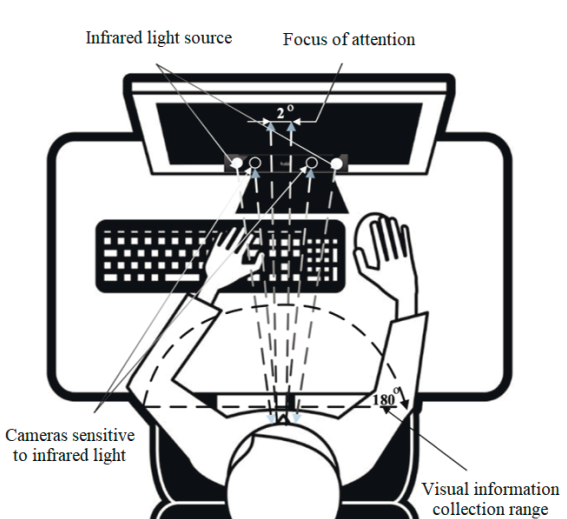

Fig. 1. Schematic representation of the positioning of the eye-tracker

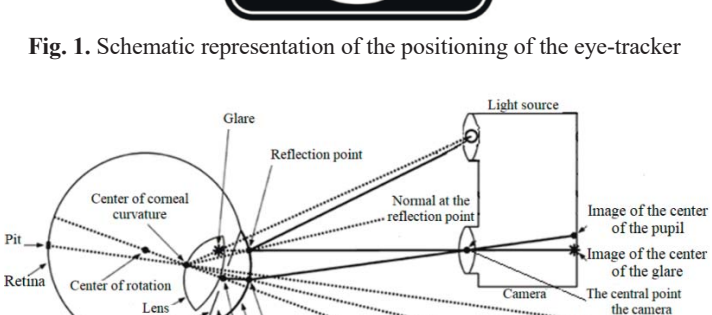

Fig. 2. Schematic representation of the human eye and the eye tracker

Information hidden in the gaze

On the basis of the data provided by the eye tracker, conclusions about human characteristics can be obtained. A brief description of several attributes determined by the gaze is presented in table 1.

The user's age can be indicated by the scanning trajectory, the change of interests, and the factors influencing the choice of an appropriate source. Assessment is formed with age and on the basis of prior knowledge and certain objectives. Age also affects saccades (rapid, strictly coordinated eye movements occurring simultaneously and in the same direction) during the execution of an assigned task [11]. On the basis of the obtained data, the approximate age of the user can be determined, as well as the symptoms of various neurological and behavioral disorders detectable in the existing eye movement disorders [12].

Multilingual users have a different reading pattern, since the fixation is on the dominant language and, as a consequence, different saccades [13]. Nutritional research has demonstrated that a person's body mass index can be estimated by presenting a set of food images with various nutrient contents, leading to a determination of the user's body mass index using pupil dilation fixation [14].

When people meet, attention is primarily directed to the person's face. By algorithmically tracking the user's gaze to the face image on the screen, conclusions can be deduced regarding the familiarity of the person with the user. The user's gaze is attracted to a group of people on the basis of race, social level, and gender [15]. Moreover, a person is also attracted to a visually appealing face, as a result of which identification of the gender to which the user is attracted is possible. An additional characteristic detectable by gaze is the user's health condition. As an example, people with autism have different facial scans and rely on other considerations when selecting an object of attention [16]. The change in the radius of a person's pupil can also contain information. A dilated pupil frequently indicates a degree of interest. Several studies have demonstrated that women's pupil changes while viewing illustrations with their partners are related to the hormonal cycle [17]. A pupil change may also identify the user's state of drowsiness or prostration. Generally, the normal pupil size is 2.0-4.0 millimeters (mm) in bright light and 4.0-8.0 mm in darkness. Pupil size in darkness and in natural light is illustrated in Figure 3. The pupil size in the usual human condition depends on the brightness of the monitor and natural light.

Table 1

A brief description of several attributes determined by the gaze

Attribute	Source
Age	Gaze trajectory, eye tremor
Gender	Gaze trajectory
Race	Gaze trajectory
Body mass index	Pupil dilation
Sexual preferences	Pupil dilation, gaze trajectory
Hormonal cycle	Pupil dilation
Health condition	Any changes

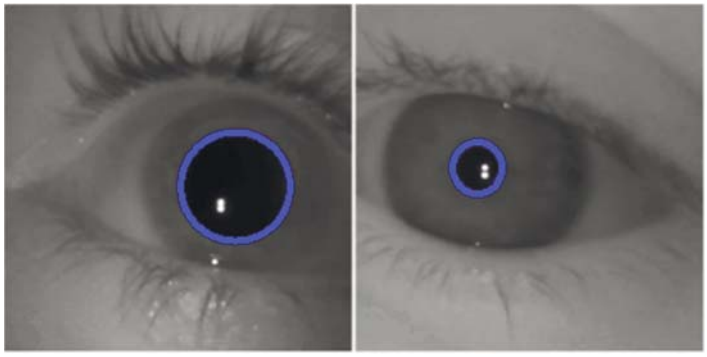

Fig. 3. The left side is the human pupil in darkness and the right side in natural light exposure

Threats and means of ensuring the security of personal data while using custom computers with integrated eye-trackers

Information leakage of identity and interests violates the principle of confidentiality of information self-identification. Users become unable to independently determine the way information about them is shared with others [18]. In accordance with statistics, the amount of leakage has been increasing annually and is expected to remain on the rise. The number of leaks and the volume of compromised records in the world are presented in table 2.

The identification and authentication methods restrict access to network resources. Biometric data is used for the implementation of access opening, the leakage of which would cause the impossibility of reuse because of the impossibility of replacement. Figure 4 represents a graph of leakage from 2009 to 2025.

For instance, patients' medical records contain a lot of personal information which is nearly impossible to anonymize. Information leakages are associated with the identification of a person in 99 instances of 100.

During the mid-1990s, Massachusetts published medical records summarizing the medical files of every state employee. The governor publicly assured the data remained anonymous, removing the identifying details - name, address, and social security number. In a short time thereafter, the governor received the medical records including personal information through the mail. In 2022, about 20% of all healthcare-related organizations in Russia had experienced information leaks, 45% of which were non-anonymous, personal data [19]. Information about the city, sex, and date of birth can be used to identify 50% of the people, and with additional information about the zip code, the possibility arises to identify about 85% of the people [20].

Table 2

Amount of leakage and compromised records worldwide

Year	Amount of leakage	Volume of compromised data records in billions	Amount of records per leakage
2009	747	0.07	93 708
2010	794	0.65	818 639
2011	801	0.22	274 656
2012	934	0.37	396 145
2013	1143	0.56	489 938
2014	1395	0.77	551 971
2015	1505	0.97	644 518
2016	1556	3.15	2 024 421
2017	2131	13.29	6 236 508
2018	2253	7.28	3 231 247
2019	2509	13.7	5 460 342
2020	2395	11.06	4 617 954
2021	4145	22.1	5 331 724
2022	4100	21.8	5 317 073
Estimated leakage			
2023	3760	19.75	5 252 659
2024	4095	22.24	5 431 013
2025	4435	24.9	5 614 430

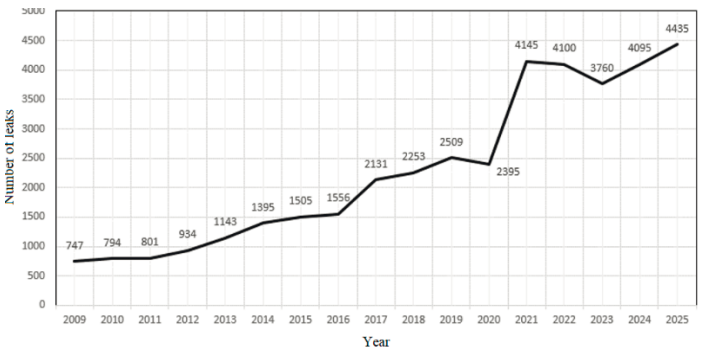

Fig. 4. Amount of leakage from 2009 to 2025

The Netflix database of 100 million records with people evaluating movies has contributed to the realization of identifying 70% of people using only ratings for 2 movies and approximate time [21]. On the basis of the data collected by the eye tracker, a person may be identified with a 90% probability, knowing only 3 parameters: age, sex and medical conditions.

Therefore, with reference being made to the information presented previously, the conclusion can be made that the necessity of developing identity theft protections is indisputable. The user should be allowed to limit data collection and be informed about the collection of confidential information and the potential consequences. Several methods are available to reduce the collection of personal data while using custom computers with embedded eye-tracking devices.

However, the possibility for users of viewing and storing all the output from the eye-tracking device remains an option. Operating system providers or the software developers of the eye tracker would create an interface proprietary to the eye tracker which would display a person's emotional state on the screen in real-time based on the eye tracker's output.

The majority of modern eye-tracking devices use infrared light to function. The method of physical barriers should be able to overcome the problem of data leakage. The proposed method is exceptionally straightforward, however, effective. The shielding relies on the use of glasses with lenses with infrared light filtering. Through software, eye-tracking data can be gathered from a conventional camera [22, 23, and 24]. The use of hidden cameras as eye-tracking devices entails the unauthorized collection of personal information. A shielding method is available to restrict the collection of personal information from conventional and hidden devices. However, the method has a problem if the technology becomes ubiquitous. Therefore, infrared light-filtered glasses would become irrelevant because of the necessity of constant interaction with eye-tracking devices.

The other method is the recognition of personal information related to gaze, and biometric data [25]. The user has to be aware of the scope, purpose of the collection and further manipulation of confidential information. All the data from the eye tracker will be particularly protected because a person can be identified on the basis of this data. The other method worth consideration is based on the use of a database of diligent content, including a variety of scenes of content viewing outcomes with areas of interest being marked by humans using eye-tracking devices. The database simulates personal data from a real-time eye tracker. Simulation can be achieved through the use of visual-motor system simulation [20]. In the presented method, the User Content block includes the user database containing the user's content.

The Regions of Interest (ROI) block contains the real regions of interest of users simulating human behavior while viewing content. Regions of interest represent areas in which the user focuses the most attention while viewing the content. The Virtual Area block creates a virtual area with a resolution several times higher than the actual size of the main monitor. Content from the average content base is transmitted to the virtual area. The installed eye-tracking system captures the user's gaze point and transmits the data to the coordinate displacement block. The vision model block generates points and saccades of the human gaze, considering the physiological features of vision, and replicating the vision of a real person.

The coordinate displacement block receives the original resolution of the monitor with the content, the human visual system model, and the regions of interest for the content, followed by the creation of acceptable displacement coordinates and transmitted to the virtual area. The pixel selection block displaces the main content with the original resolution over the virtual area by the coordinate calculated by the displacement block. Throughout the manipulation, the intruder would encounter intermingled data, the minority of which is real data, when attempting to steal the data. A schematic representation of the eye-tracking data simulation method is shown in Figure 5.

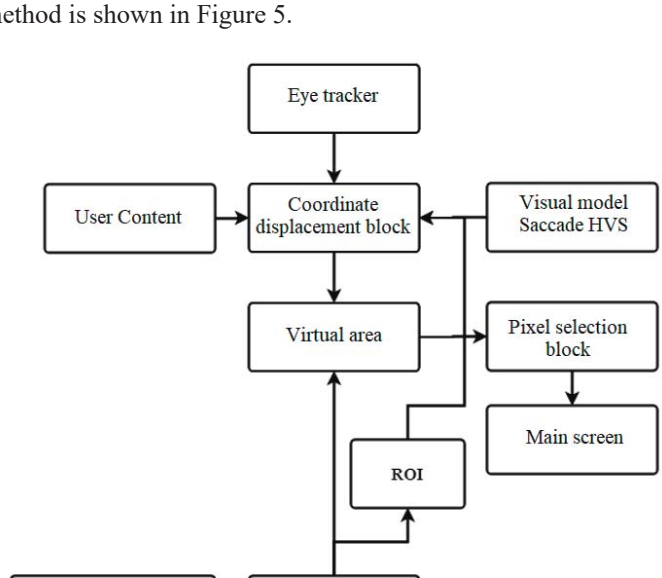

Fig. 5. Schematic representation of the method of simulating eye-tracking data

The most recent method being proposed is the implementation of a hardware-level status indicator in the eye tracker, enabling the unauthorized collection of confidential information to be avoided. Applying an indicator with multiple states, more significant information can be determined, in particular, whether the eye tracker is powered on, whether eye tracking is active, and the number of people in the collection boundaries [5].

Although the various security methods deserve separate attention, two methods are worth mentioning: the shielding method and the method using a database of diligent content. The shielding method completely limits data collection, but has many disadvantages. Conversely, the method based on the use of a database provides sufficiently high results of hiding personal information without noticeable disadvantages. A brief description of the advantages and disadvantages of the presented methods and technologies of personal data security is presented in Table 3.

The above methods do not consider the dependence of tracking accuracy on illumination. Tracking accuracy decreases with strong room illumination, respectively:

$$P = 100\% - \frac{A*\tan\frac{\alpha}{2}}{D*0.5} * 100\%, \quad (1)$$

where

D – pupil diameter

A – maximum possible displacement of the pupil center position

P – accuracy of pupil detection

α – visual field of the eye tracker

Table 3

A brief description of the advantages and disadvantages of the presented methods and technologies of personal data security

A method or technology for the protection of personal data using eye-tracking devices	Advantages	Disadvantages
Glasses with facial recognition protection	Blocking up to 100% infrared light, easy in use	Continuous use causes discomfort, high cost
Recognition of personal information related to gaze, biometric data	More vigilant attention to eye-tracking data from law enforcement agencies	No physical deterrent for the intruder.
Implementing a hardware-level status indicator in the eye-tracking device	Facilitates detection of unauthorized personal data collection	The need for a new model of eye-tracking device with an embedded indicator
Software for controlling the output from the eye-tracking device	Provides the possibility to analyze all output data from the eye tracker	No deterrent for the intruder.
Database simulating eye-tracking data	High reliability of data hiding, prevention of data at the stage of defining the regions of interest	High resource intensity

The average luminance after gamma correction is 18% of the white luminance. The brightness of the displays is set in accordance with the physiological characteristics, the optimal value is considered to be 100 cd/m². In conditions of natural or artificial light, the optimum brightness varies from 150 to 250 cd/m².

Recommendations for optimal monitor settings for maximum tracking accuracy and convenience of application can be developed, by using the data on the correlation between the tracking accuracy and the illumination. Figure 6 demonstrates the correlation between pupil size and illumination brightness [26, 27].

Conclusion

With the passage of time and the cost decline, eye-tracking devices have become increasingly popular in a variety of areas of life. Eye-tracking technology is unique among input mechanisms because of the identification of individual user characteristics which are complicated to falsify and conceal. Users agreeing to the collection of personal data for the purposes of improving the service are unintentionally exposed to leaks of sensitive personal information. Using, processing, storing, and analyzing information required to complete a particular task can reduce the risk of leaks of confidential data.

This research has revealed a problem with the widespread use of eye-tracking technology, which may threaten the privacy of the technology's users. The advantages of using eye-tracking technology in different areas are important, although, without the use of policies and information security measures, the technology would not be able to function because of the unreliability of use and the security of personal data, despite the obvious superiorities.

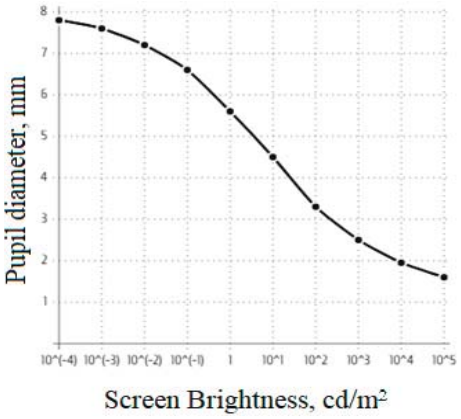

Fig. 6. Correlation between pupil diameter and illumination brightness

References

1. "Eye Tracking: The Complete Pocket Guide," *IMOTIONS*, 2022 [online] Available:https://imotions.com/blog/learning/best-practice/eye-tracking/

2. A. Egorova, R. Baryshev and A. Mozhaeva, "Methodology of Researching Perception Identity of Regions of Users' Interests While Viewing Streaming Video Containing Various Content and Compression Artefacts," *2023 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russia, 2023, pp. 1-7, doi: 10.1109/IEEECONF56737.2023.10092038.

3. A. Davydova, A. Mozhaeva, V. Hourani, "Methodology for studying the identity of perception of regions of user interests when watching streaming video containing various content and compression artifacts", *Synchronization, generation and signal processing systems*. 2022, vol. 13, no. 6, pp. 42-51.

4. "30+ data breach statistics and facts," *Comparitech*, 2023 [online]. Available: https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts

5. J. Daniel, "Liebling and Sören Preibusch. Privacy considerations for a pervasive eye tracking world," *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication* (UbiComp '14 Adjunct). Association for Computing Machinery, New York, NY, USA, 2014, pp. 1169-1177. https://doi.org/10.1145/2638728.2641688

6. V. Mazin, M. J. Cree, L. Streeter, K. Nezhivleva and A. Mozhaeva, "Research and Application of the Adaptive Model of the Human Visual System for Improving the Effectiveness of Objective Video Quality Metrics," *2023 33rd Conference of Open Innovations Association (FRUCT)*, Zilina, Slovakia, 2023, pp. 192-197, doi: 10.23919/FRUCT58615.2023.10142993.

7. A. Mozhaeva, V. Mazin, M.J. Cree, L. Streeter, " Video Quality Assessment Considering the Features of the Human Visual System," 2013. In: Yan, W.Q., Nguyen, M., Stommel, M. (eds) Image and Vision Computing. IVCNZ 2022. Lecture Notes in Computer Science, vol 13836. Springer, Cham. https://doi.org/10.1007/978-3-031-25825-1_21

8. S. Uzzaman, S. Joordens, "The eyes know what you are thinking: Eye movements as an objective measure of mind wandering," *Consciousness and Cognition: An International Journal*, no. 20(4), 2011, pp. 1882-1886. https://doi.org/10.1016/j.concog.2011.09.010

9. How the eye production technology works and why it can be dangerous // RBC Trends, 2022[online] Available: https://trends.rbc.ru/trends/industry/635bbfb59a79477f31432b0d

10. Andreas Bulling, Jamie A. Ward, and Hans Gellersen, "Real-Time Eye Tracking and Blink Detection with Deep Neural Networks," *ACM Transactions on Interactive Intelligent Systems*. 2020.

11. A. Borji, L. Itti, “Defending Yarbus: Eye movements reveal observers’ task,” *Journal of Vision*, no. 14(3):29, 2014, pp. 1-21, http://www.journalofvision.org/content/14/3/29, doi:10.1167/14.3.29.

12. D. P. Munoz, et al., “Age-related performance of human subjects on saccadic eye movement tasks,” *Experimental brain research*, vol. 121, no. 4, 1998, pp. 391-400. doi:10.1007/s002210050473

13. “Privacy in Xbox One and Kinect,” *Microsoft*, 2014 [online] Available: http://www.microsoft.com/security/onlineprivacy/xbox.aspx.

14. Graham, Reiko et al., “Body mass index moderates gaze orienting biases and pupil diameter to high and low calorie food images,” *Appetite*, vol. 56, no. 3, 2011, pp. 577-86. doi:10.1016/j.appet.2011.01.029

15. Bar-Haim, Yair et al., “Nature and nurture in own-race face processing,” *Psychological science,* vol. 17, no. 2, 2006, pp. 159-63. doi:10.1111/j.1467-9280.2006.01679.x

16. Dalton, Kim M et al., “Gaze fixation and the neural circuitry of face processing in autism,” *Nature neuroscience*, vol. 8, no. 4, 2005, pp. 519-26. doi:10.1038/nn1421

17. Laeng Bruno, and Liv Falkenberg, “Women's pupillary responses to sexually significant others during the hormonal cycle,” *Hormones and behavior*, vol. 52, no. 4, 2007, pp. 520-30. doi:10.1016/j.yhbeh.2007.07.013

18. Reynolds, Osborne M., “Administrative Law Review,” vol. 22, no. 1, 1969, pp. 101-06. JSTOR, http://www.jstor.org/stable/40708684. Accessed 29 June 2023.

19. “Data leaks in medical institutions,” *ZDRAV.EXPERT*, 2023 [online] Available: https://zdrav.expert/

20. M. Vyatkin, A. Potashnikov, V. Selivanov, I. Vlasuyk, K. Nezhivleva, A. Mozhaeva, "Method of Preventing Leakage of Personal Data Through Eyetracking Modules of User Devices", *T-Comm*, vol. 16, no.7, pp. 44-51. (in Russian)

21. Ian H. Witten, E. Frank, M.A. Hall, “Data Mining: Practical Machine Learning Tools and Techniques”, *Elsevier Science & Technology*, Morgan Kaufmann Publishers is an imprint of Elsevier. 2016, pp 665.

22. Online Eye Tracking Software // Grabador de mirada [online] Available: https://redirect.gazerecorder.com/

23. E. Wood, A. Bulling, A. Schmidt, “Eye Tracking for Everyone,” *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2022, no. 4(2), pp. 1-23.

24. S. Ahuja, P. Rao, and V. Sarode. "Real-Time Eye Gaze Tracking with Webcam and Image Processing". 2021.

25. DIN Deutsches Institut für Normung e. V. DIN 33450. “Graphical symbol for information about surveillance with optical-electronic devices (video-info signs),” 2014, p. 11.

26. K. Krafka, A. Khosla, P. Kellnhofer, H. Kannan, S. Bhandarkar, W. Matusik, A. Torralba, “Eye tracking for everyone with robust pupil detection,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 2021, pp. 602-611.

27. L. Fan, X. Wei, H. Fu, T. Liu, “Accurate eye gaze estimation with a 3D eyeball model and calibration refinement,” *Neurocomputing*, 2021, no. 449, pp. 264-274.

АНАЛИЗ УГРОЗ И СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ПОЛЬЗОВАТЕЛЬСКИХ КОМПЬЮТЕРОВ СО ВСТРОЕННЫМИ УСТРОЙСТВАМИ ОТСЛЕЖИВАНИЯ ВЗГЛЯДА

Илья Сафонов, Михаил Вяткин, Олеся Хиженкова, Ксения Неживлева, Игорь Власюк,

Московский технический университет связи и информатики, Москва, Россия, ***k.i.nezhivleva@mtuci.ru***

Аннотация

Технология отслеживания взгляда широко используется в веб-разработке, маркетинге и игровых механиках благодаря возможности получения данных о траектории и точках фиксации взгляда. Эта информация о движениях глаз может быть эффективно использована для изучения сложных когнитивных процессов и визуальной восприимчивости человека. Однако, с распространением технологии отслеживания взгляда возникает серьезная проблема утечки конфиденциальности пользователей. Поскольку данная технология может получать высоко чувствительную информацию о пользовательском поведении и предпочтениях, необходимы меры для защиты персональных данных. На данном этапе развития технологий исследования угроз и средств обеспечения безопасности персональных данных становятся приоритетными задачами в данной области. Проявление должной осторожности при разработке и использовании устройств отслеживания взгляда становится неотъемлемой частью процесса. Необходимо учитывать потенциальные угрозы, связанные с сбором, хранением и передачей данных о взгляде пользователей. Для обеспечения безопасности персональных данных при использовании устройств отслеживания взгляда предлагаются различные методы. Одним из них является анонимизация данных, то есть удаление или замена идентифицирующих личность элементов. Также важным аспектом является обеспечение прозрачности и согласия пользователей на сбор и использование данных о взгляде. Это может быть достигнуто путем ясного предоставления информации о целях сбора данных и возможности контроля за своей конфиденциальностью. В данной работе рассмотрены угрозы, связанные с использованием технологии отслеживания взгляда, и предложены методы обеспечения безопасности персональных данных. Это важные шаги в развитии данной области, которые помогут защитить конфиденциальность пользователей и сделать использование устройств отслеживания взгляда более безопасным и этичным.

Ключевые слова: *персонализация данных, защита информации, конфиденциальность, отслеживание взгляда, информационная безопасность.*

Литература

1. Eye Tracking: The Complete Pocket Guide // IMOTIONS, 2022 [online] Available:https://imotions.com/blog/learning/best-practice/eye-tracking/
2. *Egorova A., Baryshev R., Mozhaeva A.* Methodology of Researching Perception Identity of Regions of Users' Interests While Viewing Streaming Video Containing Various Content and Compression Artefacts // 2023 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russian Federation, 2023, pp. 1-7, doi: 10.1109/IEEECONF56737.2023.10092038.
3. Давыдова А., Можаева А., Хурани В. Методика исследования идентичности восприятия областей интересов пользователя при просмотре потокового видео, содержащего различный контент и артефакты сжатия // Системы синхронизации, формирования и обработки сигналов. 2022. Т. 13, № 6. С. 42-51. EDN IZCJOE.
4. 30+ data breach statistics and facts // Comparitech, 2023[online] Available: https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/
5. *Daniel J.* Liebling and S?ren Preibusch. Privacy considerations for a pervasive eye tracking world // Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp '14 Adjunct). Association for Computing Machinery, New York, NY, USA, 2014, pp. 1169-1177. https://doi.org/10.1145/2638728.2641688
6. *Mazin V., Cree M. J., Streeter L., Nezhivleva K., Mozhaeva A.* Research and Application of the Adaptive Model of the Human Visual System for Improving the Effectiveness of Objective Video Quality Metrics // 2023 33rd Conference of Open Innovations Association (FRUCT), Zilina, Slovakia, 2023, pp. 192-197, doi: 10.23919/FRUCT58615.2023.10142993.
7. *Mozhaeva A., Mazin V., Cree M.J., Streeter L.* Video Quality Assessment Considering the Features of the Human Visual System. 2023. In: Yan, W.Q., Nguyen, M., Stommel, M. (eds) Image and Vision Computing. IVCNZ 2022. Lecture Notes in Computer Science, vol 13836. Springer, Cham. https://doi.org/10.1007/978-3-031-25825-1_21
8. *Uzzaman S., Joordens S.* The eyes know what you are thinking: Eye movements as an objective measure of mind wandering // Consciousness and Cognition: An International Journal, 2011, no. 20(4), 1pp. 882-1886. https://doi.org/10.1016/j.concog.2011.09.010
9. How the eye production technology works and why it can be dangerous // RBC Trends, 2022 [online] Available: https://trends.rbc.ru/trends/industry/635bbfb59a79477f31432b0d
10. *Andreas Bulling, Jamie A. Ward, Hans Gellersen.* Real-Time Eye Tracking and Blink Detection with Deep Neural Networks // ACM Transactions on Interactive Intelligent Systems. 2020.
11. *Borji A., Itti, L.* Defending Yarbus: Eye movements reveal observers' task // Journal of Vision, 2014, no. 14(3), pp. 29, 1-21, http://www.journalofvision.org/content/14/3/29, doi:10.1167/14.3.29.
12. *Munoz D P* et al. Age-related performance of human subjects on saccadic eye movement tasks // Experimental brain research vol. 121, no. 4. 1998, pp. 391-400. doi:10.1007/s002210050473
13. Privacy in Xbox One and Kinect // Microsoft, 2014. [online] Available: http://www.microsoft.com/security/onlineprivacy/xbox.aspx.
14. Graham Reiko et al. Body mass index moderates gaze orienting biases and pupil diameter to high and low calorie food images // Appetite vol. 56, no. 3, 2011, pp. 577-86. doi:10.1016/j.appet.2011.01.029
15. *Bar-Haim Yair* et al. Nature and nurture in own-race face processing // Psychological science vol. 17, no. 2, 2006, pp. 159-63. doi:10.1111/j.1467-9280.2006.01679.x
16. *Dalton Kim M.* et al. Gaze fixation and the neural circuitry of face processing in autism // Nature neuroscience vol. 8, no. 4, 2005, pp. 519-26. doi:10.1038/nn1421
17. *Laeng Bruno, Liv Falkenberg.* Women's pupillary responses to sexually significant others during the hormonal cycle // Hormones and behavior vol. 52, no. 4, 2007, pp. 520-30. doi:10.1016/j.yhbeh.2007.07.013
18. *Reynolds Osborne M.* Administrative Law Review, vol. 22, no. 1, 1969, pp. 101-06. JSTOR, http://www.jstor.org/stable/40708684. Accessed 29 June 2023.
19. Data leaks in medical institutions // ZDRAV.EXPERT, 2023. [online] Available: https://zdrav.expert/
20. *Vyatkin M., Potashnikov A., Selivanov V., Vlasuyk I., Nezhivleva K., Mozhaeva A.* Method of Preventing Leakage of Personal Data Through Eyetracking Modules of User Devices // T-Comm, vol. 16, no.7, pp. 44-51.
21. *Ian H. Witten, E. Frank, M.A. Hall.* Data Mining: Practical Machine Learning Tools and Techniques // Elsevier Science & Technology, Morgan Kaufmann Publishers is an imprint of Elsevier. 2016, pp 665.
22. Online Eye Tracking Software // Grabador de mirada. [online] Available:https://redirect.gazerecorder.com/
23. *Wood E., Bulling A., Schmidt A.* Eye Tracking for Everyone // Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), 2022, no. 4(2), pp. 1-23.
24. Ahuja S., Rao P., Sarode V. Real-Time Eye Gaze Tracking with Webcam and Image Processing. 2021.
25. DIN Deutsches Institut f?r Normung e. V. DIN 33450. symbol for information about surveillance with optical-electronic devices (video-info signs), 2014, p. 11.
26. *Krafka, K., Khosla, A., Kellnhofer, P., Kannan, H., Bhandarkar, S., Matusik, W., Torralba, A.* Eye tracking for everyone with robust pupil detection // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2021, pp. 602-611.
27. Fan L., Wei X., Fu H., Liu T. Accurate eye gaze estimation with a 3D eyeball model and calibration refinement // Neurocomputing, 2021, no. 449, pp. 264-274.