

B. A. KUZENBAYEV*, **B. T. ZHUSSUPOVA**, **A. ZH. SARINA**,
D. ZH. ALIPPAYEVA, **G. A. BABULOVA**, **A. K. KARAGOZHINA**

Akhmet Baitursynuly Kostanay Regional University, Kostanay, Kazakhstan

**E-mail: becz@bk.ru*

***PRINCIPLES OF SUSPICIOUS ACTIVITY DETECTION AND PROGRAMS FOR
ANALYZING SUSPICIOUS ACTIVITY USING VIDEO
SURVEILLANCE CAMERAS.***

Kuzenbayev Batyrkhan Amanzholovich – PhD, Head of the Department of Information Systems, A. Baitursynov KRU, Kostanay, Kazakhstan;

E-mail: becz@bk.ru

Zhusupova Botagoz Tulegenovna – master of Natural Sciences, senior lecturer of the Department of Information Systems, A. Baitursynov KRU, Kostanay, Kazakhstan;

E-mail: botasha_zhan@mail.ru

Sarina Assel Zhumabayevna – master of technical sciences, senior lecturer of the Department of Information Systems, A. Baitursynov KRU, Kostanay, Kazakhstan;

E-mail: sarina.asel@mail.ru

Alipayeva Dinara Zhankabylovna – master of Natural Sciences, senior lecturer of the Department of Information Systems, A. Baitursynov KRU, Kostanay, Kazakhstan;

E-mail: alippaewi@mail.ru

Babulova Gulmira Aitghanovna – master of Natural Sciences, senior lecturer of the Department of Information Systems, A. Baitursynov KRU, Kostanay, Kazakhstan;

E-mail: gulmirab_1987@mail.ru

Karagozhina Anara Kuanyshbekovna – master of Natural Sciences, senior lecturer of the Department of information, Kostanay, Kazakhstan.

E-mail: anara31455@mail.ru

This article delves into the principles of detecting suspicious activity, meticulously examining both logical and psychological facets of human behavior. It places a primary focus on diverse programs for analyzing suspicious activity using video surveillance cameras. A comprehensive overview is provided for key categories of suspicious activity, encompassing crowd clustering, rapid movement, intrusion into secure areas, and unattended items.

Within the research framework, the advantages and drawbacks of leading programs for suspicious activity analysis through video surveillance are scrutinized. Furthermore, the article introduces the concept of an innovative program aimed at competing with existing solutions. This software aspires to amalgamate the strengths of competitors while avoiding their shortcomings. The research goal is to identify the potential for creating a highly effective software product capable of successfully competing and meeting the requirements of modern surveillance systems.

Keywords: *suspicious activity, video surveillance cameras, human behavior analysis, security, machine learning, artificial Intelligence, machine Learning.*

Б. А. КУЗЕНБАЕВ*, **Б. Т. ЖУСУПОВА**, **А. Ж. САРИНА**,
Д. Ж. АЛИППАЕВА, **Г. А. БАБУЛОВА**, **А. К. КАРАГОЖИНА**

*Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті,
Қостанай, Қазақстан
E-mail: be kz@bk.ru

КҮДІКТІ ӘРЕКЕТТІ АНЫҚТАУ ПРИНЦИПТЕРІ ЖӘНЕ БЕЙНЕБАҚЫЛАУ КАМЕРАЛАРЫНЫҢ КӨМЕГІМЕН КҮДІКТІ ӘРЕКЕТТІ ТАЛДАУ БАҒДАРЛАМАЛАРЫ

Кузенбаев Батырхан Аманжолұлы – PhD докторы, Ақпараттық жүйелер кафедрасының менгерушісі, А. Байтұрсынұлы атындағы ҚРУ, Қостанай, Қазақстан;
E-mail: be kz@bk.ru

Жүсіпова Ботагөз Төлегенқызы – жаратылыстану ғылымдарының магистрі, Ақпараттық жүйелер кафедрасының аға оқытушысы, А. Байтұрсынұлы атындағы ҚРУ, Қостанай, Қазақстан;
E-mail: botasha_zhan@mail.ru

Сарина Әсел Жұмабайқызы – техника ғылымдарының магистрі, Ақпараттық жүйелер кафедрасының аға оқытушысы, А. Байтұрсынұлы атындағы ҚРУ, Қостанай, Қазақстан;
E-mail: sarina.asel@mail.ru

Әліппаева Динара Жанқабылқызы – жаратылыстану ғылымдарының магистрі, Ақпараттық жүйелер кафедрасының аға оқытушысы, А. Байтұрсынұлы атындағы ҚРУ, Қостанай, Қазақстан;
E-mail: alipraewi@mail.ru

Бабулова Гүлмира Айтжанқызы – жаратылыстану ғылымдарының магистрі, Ақпараттық жүйелер кафедрасының аға оқытушысы, А. Байтұрсынұлы атындағы ҚРУ, Қостанай, Қазақстан;
E-mail: gulmirab_1987@mail.ru

Қарағожина Анара Қуанышбекқызы – жаратылыстану ғылымдарының магистрі, ақпарат кафедрасының аға оқытушысы, Қостанай, Қазақстан.
E-mail: anara31455@mail.ru

Бұл мақалада күдікті әрекеттерді анықтау принциптері қарастырылады, адам мінез-құлқының логикалық және психологиялық аспектілері мұқият зерттеледі. Қауіпсіздік камераларын қолдана отырып, күдікті әрекеттерді талдауға арналған әртүрлі бағдарламаларға назар аударылады. Күдікті әрекеттердің негізгі санаттарына жан-жақты шолу, соның ішінде адамдар көп жиналуы, жылдам қозғалу, қорғалатын аймақтарға ену және қараусыз қалған заттар.

Зерттеу бейнебақылау арқылы күдікті әрекеттерді талдауға арналған жетекші бағдарламалардың артықшылықтары мен кемшіліктерін мұқият зерттейді. Сонымен қатар, мақалада қолданыстағы шешімдермен бәсекелестікке бағытталған инновациялық бағдарлама тұжырымдамасы ұсынылған. Бұл бағдарламалық жасақтама бәсекелестердің кемшіліктерін болдырмай, олардың күшті жақтарын біріктіруге тырысады. Зерттеудің мақсаты-сәтті бәсекеге қабілетті және заманауи бейнебақылау жүйелерінің талаптарына жауап беретін жоғары тиімді бағдарламалық өнімді құру әлеуетін анықтау.

Түйін сөздер: күдікті әрекет, бейнебақылау камералары, адамның мінез-құлқын талдау, қауіпсіздік, машиналық оқыту, жасанды интеллект.

Б. А. КУЗЕНБАЕВ*, **Б. Т. ЖУСУПОВА**, **А. Ж. САРИНА**,
Д. Ж. АЛИППАЕВА, **Г. А. БАБУЛОВА**, **А. К. КАРАГОЖИНА**

*Костанайский региональный университет имени Ахмет Байтұрсынұлы,
Костанай, Казахстан
E-mail: be kz@bk.ru

ПРИНЦИПЫ ОБНАРУЖЕНИЯ ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ И ПРОГРАММЫ АНАЛИЗА ПОДОЗРИТЕЛЬНОЙ АКТИВНОСТИ С ИСПОЛЬЗОВАНИЕМ КАМЕР ВИДЕОНАБЛЮДЕНИЯ

Кузенбаев Батырхан Аманжолович – доктор PhD, заведующий кафедрой информационных систем, КРУ имени А. Байтұрсынұлы, Костанай, Казахстан;

E-mail: be kz@bk.ru

Жусупова Ботагөз Тулегеновна – магистр естественных наук, старший преподаватель кафедры информационных систем, КРУ имени А. Байтұрсынұлы, Костанай, Казахстан;

E-mail: botasha_zhan@mail.ru

Сарина Асель Жумабаевна – магистр технических наук, старший преподаватель кафедры информационных систем, КРУ имени А. Байтұрсынұлы, Костанай, Казахстан;

E-mail: sarina.asel@mail.ru

Алиппаева Динара Жанкабыловна – магистр естествознания, старший преподаватель кафедры информационных систем, КРУ имени А. Байтұрсынұлы, Костанай, Казахстан;

E-mail: alippaewi@mail.ru

Бабулова Гульмира Айтжановна – магистр естественных наук, старший преподаватель кафедры информационных систем, КРУ имени А. Байтұрсынұлы, Костанай, Казахстан;

E-mail: gulmirab_1987@mail.ru

Карагожина Анара Куанышбековна – магистр естественных наук, старший преподаватель кафедры информационных систем, КРУ имени А. Байтұрсынұлы, Костанай, Казахстан.

E-mail: anara31455@mail.ru

В статье рассматриваются принципы обнаружения подозрительной активности, тщательно исследуются как логические, так и психологические аспекты поведения человека. Основное внимание уделяется различным программам для анализа подозрительной активности с использованием камер видеонаблюдения. Представлен всесторонний обзор ключевых категорий подозрительной активности, включая скопление людей, быстрое передвижение, проникновение в охраняемые зоны и оставленные без присмотра предметы.

В рамках исследования тщательно изучаются преимущества и недостатки ведущих программ для анализа подозрительной активности с помощью видеонаблюдения. Кроме того, в

статье представлена концепция инновационной программы, направленной на конкуренцию существующим решениям. Это программное обеспечение стремится объединить сильные стороны конкурентов, избегая при этом их недостатков. Цель исследования – выявить потенциал для создания высокоэффективного программного продукта, способного успешно конкурировать и отвечать требованиям современных систем видеонаблюдения.

Ключевые слова: подозрительная активность, камеры видеонаблюдения, анализ поведения человека, безопасность, машинное обучение, искусственный интеллект.

Introduction. In the modern world, where ensuring security is becoming increasingly crucial, technology plays a pivotal role in creating a safe environment for citizens. One of the most effective innovations contributing to public safety is the implementation of surveillance cameras. Surveillance cameras are indispensable tools for ensuring security in various facilities, from banks and shops to government institutions and residential buildings. However, many surveillance systems merely record video streams without providing information about suspicious events. To detect and respond to potentially dangerous situations, specialized programs are required to process video streams and automatically identify suspicious activities.

Developing such programs requires an understanding of the principles that can classify a person as suspicious, and ultimately, potentially dangerous. This article will explore the principles of identifying suspicious activity from the perspectives of logic and human psychology. Additionally, existing solutions for analyzing suspicious human activity through video surveillance will be investigated. As a result, a conceptual model of a program will be formulated, aiming to compete with other programs in this field, introducing innovations by leveraging the strengths of competitors and addressing their shortcomings.

Methods. The determination of suspicious activity can be subjective, as each person possesses a unique perspective on the surrounding world. According to a comprehensive dictionary, any actions expressing distrust or uncertainty towards something or someone can be considered suspicious [1]. Depending on an individual's life experience and knowledge, any activity may be labeled as suspicious.

However, in professions where any mistake can lead to severe consequences, it is imperative to train specialists in identifying suspicious behavior. For instance, airports worldwide employ the SPOT system [2], comprising 94 criteria for suspicious behavior, such as frequent blinking, yawning, whistling, nervous tics, and more. This enables airport personnel to ask questions and inspect the luggage of suspicious passengers, significantly reducing the number of incidents. Therefore, it is crucial to train professionals in effective communication with individuals and recognizing suspicious behavior to minimize the possibility of errors, particularly in critical sectors like law enforcement, healthcare, military, and security services.

Many security system developers continue to grapple with the question of how to teach machines to identify suspicious behavior. However, logical methods already exist and are successfully utilized for detecting suspicious activity. By studying suspicious activity from a logical and psychological standpoint, several methods for identifying suspicious behavior can be identified, including:

- Crowd Monitoring;
- Counting Ingress and Egress;

- Abandoned Object Detection;
- Restricted Area Intrusion Tracking;
- Recognition of Aimless Wandering (Loitering);
- Fast Movement Detection [3].

These methods are just some of the possible ways to detect suspicious activity and can be used in various combinations to ensure the most accurate threat detection.

One method of identifying suspicious activity is through crowd monitoring (see Figure 1). Such gatherings can indicate a potential security threat, prompting many security systems to incorporate this feature. For instance, the ObjectVideo situational video analytics by Avigilon [4] defines crowd gathering as the simultaneous presence of a specified number of people in the monitored area for a set duration. Parameters such as the scanned area, maximum number of people, and duration can be configured to identify suspicious activity.



Figure 1 – Example of a Suspicious Crowd

However, crowd gatherings are not always indicative of suspicious activity, as large events or crowded places like shopping centers might have normal congregations. Thus, in addition to crowd monitoring, security systems may employ other methods like behavior analysis and sound sensors to detect suspicious activity. Combining multiple methods enhances the accuracy of identifying suspicious actions and helps prevent potential security threats.

Another method to identify suspicious activity is by using an inbound and outbound people counter. This tool allows monitoring the number of objects passing through a designated control line in specified directions. The direction and control line can be configured according to security requirements. A discrepancy in the count of incoming and outgoing individuals may indicate an intruder inside a secure area, either entering unlawfully or not exiting.

Searching for abandoned items is another method applied in video surveillance systems to enhance security. According to Macroscop [5], this feature helps reduce the risks of terrorist acts and other dangerous situations involving abandoned items. The program analyzes the scanned area, searching for objects left within it for a specified period. If an object remains stationary for a designated time, the system notifies the user. Although abandoned items are often the result of forgetfulness or loss, there's a risk that the item could be dangerous to the

surroundings. Hence, swiftly detecting abandoned items is a crucial tool for ensuring safety in public places like airports, transportation hubs, and other crowded areas.

Detecting intrusion into restricted areas is a critical function of video surveillance systems. In situations where access to a strictly guarded area is prohibited, the intrusion detection method (see Figure 2) can be a key element of security. According to a modern video analytics article [6], when an intrusion occurs in a user-defined forbidden zone, the system automatically records the moment of the breach in the database and notifies the administrator. This enables prompt action to prevent unwanted consequences and ensures maximum security.



Figure 2 – Example of Intrusion into a Restricted Zone

Detecting loitering is of great importance in video surveillance systems. If a scanned area is secure but accessible to people passing through, the loitering detection method (see Figure 3) can be used to enhance security. It identifies suspicious actions of individuals lingering in the controlled area for an extended period. The American company IRISITY [7] developed a video analytics system capable of detecting loitering. The term “loitering” is used to denote someone staying in a secure but passable area for an extended time. This behavior may indicate malicious actions or intentions. While merely passing through a secure area does not raise suspicion, lingering for an extended time may suggest that the person’s actions are directed within the zone, potentially posing a threat. Utilizing a loitering detection system can help increase the effectiveness of security measures and prevent potential threats.



Figure 3 – Example of Loitering Detection

Fast Movement Detection. While most people may hasten their movement for various reasons, such as rushing to work or engaging in sports, fast movement (see Figure 4) can be associated with unlawful activities like assault, theft, or fleeing a crime scene. Therefore, software uses a running detection method, determining when a person is moving above a specified threshold speed. If such an event occurs, it is recorded, and a notification is sent to the system administrator. This allows for a prompt response to potential unlawful actions and prevention thereof.



Figure 4 – Example of Running Detection

Results and Discussion. There are programs designed for analyzing suspicious activities using cameras, each with its own advantages and drawbacks. In this investigation, we've selected some of the popular ones.

Avigilon Control Center. This program utilizes video analytics technology to detect suspicious activities [8]. ACC can identify security breaches such as trespassing, unauthorized entry into restricted areas, and leaving items unattended.

Advantages:

- **High Precision Video Analysis:** The program leverages various machine learning algorithms and computer vision, enabling it to detect various security breaches.
- **Customization for Specific Needs:** It can be tailored to a specific object, such as a building, parking lot, or warehouse, enhancing its efficiency and analysis accuracy.
- **Real-Time Operation:** The program ensures swift and reliable video analysis, allowing quick response to potential security threats.

Disadvantages:

- **High Cost:** It is one of the more expensive programs on the market, which might pose challenges for small organizations or individuals.
- **High Sensitivity to Noise and False Alarms:** The program may react to normal human activities like walking on a road or leaving items on the ground, leading to false alarms and wasting time on verifying each one.
- **Limitation on Camera Quantity:** Each license restricts the number of cameras the program can use, potentially proving insufficient for larger facilities.

Senstar Symphony. Senstar Symphony is a program utilizing machine learning technologies for video analysis and the detection of suspicious activities such as intrusions and unattended items [9].

Advantages:

- High Precision Video Analysis: The program employs numerous machine learning algorithms and computer vision, allowing it to detect various security breaches.
- Customization for Specific Needs: It can be tailored to a specific object, such as a building, parking lot, or warehouse, enhancing its efficiency and analysis accuracy.
- Early Warning Capability Based on Data Analysis: The program analyzes data on movement and behavior captured in videos, enabling the identification of potential threats and issuing warnings in advance.

Disadvantages:

- High Cost: Similar to other advanced programs, Senstar Symphony is among the more expensive options, potentially posing challenges for smaller organizations or individuals.
- Hardware Requirements: The program demands high-performance hardware, which may entail additional costs.
- Lack of Real-time Video Processing: Senstar Symphony requires preprocessing of video, which can consume time and delay responses to potential security threats.

Briefcam. Briefcam is a program utilizing machine learning technologies for video analysis and the detection of suspicious activities, including changes in the environment, movements of people and vehicles, and unattended items [10].

Advantages:

- High Volume Video Processing: The program can efficiently process a large volume of video material in a short period.
- Computer Vision Technology for Detecting Suspicious Actions: Briefcam utilizes computer vision to identify suspicious activities.
- Support for Various Video Qualities and Resolutions: It can work with videos of different qualities and resolutions.

Disadvantages:

- Occasional Inaccuracy in Identifying Suspicious Activity: Briefcam may not always accurately identify suspicious activities.
- Requires Extensive Time and Resources for Training: The program demands significant time and resources for training.
- High Price: Briefcam comes with a high price tag.

DeepCam. DeepCam is a program using artificial intelligence and machine learning to detect suspicious activities such as theft or violence. It can also identify missing persons and provide fire alerts [11].

Advantages:

- Detection of Specific Behaviors: DeepCam can detect specific behaviors, such as running or falling, and recognize faces and license plates.
- Use of Deep Learning for Efficient Data Processing: The program employs deep learning to process and analyze a large amount of data quickly and accurately.
- Real-time Detection of Suspicious Activity: DeepCam can detect suspicious activity in real-time.

Disadvantages:

- Requires High-resolution Video: The program can only work with high-resolution and high-quality video, which may pose challenges with older cameras.

- High Cost: DeepCam comes with a high cost.
- Demands Powerful Computational Resources: The program requires powerful computational resources for operation.

Having analyzed numerous existing programs for analyzing suspicious activity using surveillance cameras, it is possible to describe the functions and characteristics that would define an ideal program for analyzing suspicious activity. The ideal program should encompass the following functions and features:

- Wide Range of Functions: The program should have the ability to detect various types of suspicious activities, such as motion, facial recognition, object detection, traffic analysis, etc.
 - High Accuracy and Reliability: The program must provide precise and reliable video analysis, enabling the rapid and accurate identification of suspicious events.
 - Real-time Operation: The program should offer fast video analysis, allowing swift responses to potential security threats.
 - Integration with Other Security Systems: Easy integration with other security systems, such as access control and alarm systems, is essential for comprehensive security provision.
 - User-Friendly Interface: The program should feature a simple and intuitive interface, facilitating quick mastery of its use and management.
 - Flexible Customization: The program should allow customization to meet specific user requirements, ensuring optimal analysis results.
 - Economic Efficiency: The program should have a reasonable price, commensurate with its functionality and capabilities, ensuring maximum economic efficiency.
 - Support for a Large Number of Cameras: The program should enable the use of a large number of cameras, providing broad coverage and the ability to analyze various areas on the premises.
 - Cloud Data Storage: The program should offer the option of storing data in cloud storage, ensuring data availability and increasing its security.
- In addition to the listed characteristics and functions, it is important to consider the following aspects when choosing a program for analyzing suspicious activity:
- Data Processing System: The program should provide fast and efficient data processing for accurate video analysis and the identification of suspicious events.
 - Notification System: The program should have a notification system alerting users to suspicious events, such as sending notifications to mobile phones or email, enabling quick responses to threats.
 - Automatic Event Categorization: The program should be capable of automatically categorizing suspicious events, distinguishing, for example, between theft and assault, to ensure precise reactions.
 - Analytics System: The program should have the ability to analyze and track the behavior of people and objects over an extended period to detect recurring events and prevent potential threats.
 - Usability Flexibility: The program should be flexible in use, allowing application in different environments and conditions.
 - Program Training Support: The program should provide the option to train it for specific premises' conditions and people's behavior, enhancing the accuracy of analysis and the identification of suspicious events.

- **Technical Support:** The program should have robust technical support from the manufacturer, ensuring a quick resolution of potential issues during usage.
- **Integration of Artificial Intelligence and Machine Learning:** Implementing artificial intelligence and machine learning will enable programs to detect suspicious events faster and more accurately, even predicting potential threats based on anomalous behavior data.
- **Development of Mobile Applications:** Developing mobile applications will allow users to receive quick notifications about suspicious events and control the security of their premises from any location worldwide.

In general, programs designed for analyzing suspicious activity through surveillance cameras serve as crucial tools for ensuring public safety. Each program comes with its own set of advantages and disadvantages that can impact their effectiveness and utility in specific situations. Therefore, it is crucial to select a program that aligns best with the needs and objectives of the organization.

The application of surveillance cameras to enhance safety in public spaces has proven to be effective. For instance, in London, the «Blue Eye» system utilizes computer vision to monitor public areas and identify suspicious situations. This has resulted in a reduction in crime rates and a more rapid response to incidents.

Chicago has also successfully implemented surveillance cameras in public areas. The system analyzes the flow of people and traffic, detecting anomalies and aiding law enforcement in more effectively coordinating their actions.

These examples illustrate the positive impact of utilizing surveillance cameras and analysis programs to enhance public safety. The combination of technology, such as computer vision, and strategic monitoring contributes to a proactive approach in crime prevention and incident.

Conclusion. In conclusion, the use of surveillance cameras and software for analyzing suspicious activity is a crucial component in security systems across various types of facilities. Modern technologies enable the automatic detection of suspicious activity based on video stream analysis, allowing real-time response. However, it is essential to recognize that all technologies have limitations and cannot replace human oversight in ensuring security. Therefore, the effective approach involves combining surveillance cameras and suspicious activity analysis programs with qualified personnel.

The application of security technologies is an ongoing process that requires continuous improvement and adaptation to new threats and challenges. Research and development in the field of programs for analyzing suspicious activity and the use of surveillance cameras are essential for advancing security measures at different facilities.

The deployment of surveillance cameras in public spaces significantly contributes to enhancing overall safety levels. Nevertheless, it is crucial to maintain a balance between security and citizens' privacy to ensure the positive impact of such systems on society.

REFERENCES

1 Search through dictionaries and encyclopedias. [Electronic resource]. URL: <https://ozhegov.slovaronline.com/> (accessed 02/12/2023)

2 SPOT (Screening of Passengers by Observation Techniques). [Electronic resource]. URL:

<https://www.dhs.gov/publication/screening-passengers-observation-techniques-spot-program#:~:text=The%20Screening%20of%20Passengers%20by,potential%20transportation%20security%20risks%20by> (accessed 02/12/2023)

3 Situational video analytics SECUROS. [Electronic resource]. URL: <https://iss.ru/pub/uploads/fb0506c2-89ff-4b29-93fb-219250699fc4/securos-computer-vision-overview-ru.pdf> (Accessed 02.12.2023)

4 ObjectVideo Labs - Video Analytics and Computer Vision. [Electronic resource]. URL: <https://objectvideolabs.com/> (accessed 03/11/2023)

5 Detector of abandoned objects Macroscop. [Electronic resource]. URL: <https://macroscop.com/produkty/programma-dlya-ip-kamer/detektor-ostavlennyh-predmetov> (accessed 03/13/2023)

6 Video analytics terms, scopes, technologies Video Content Analysis. [Electronic resource]. URL:

[https://tadviser.com/index.php/Article:Video_analytics_\(terms,_scopes_of_application,_technologies\)](https://tadviser.com/index.php/Article:Video_analytics_(terms,_scopes_of_application,_technologies)) (03/14/2023)

7 Irisity - Security beyond human intelligence. [Electronic resource]. URL: <https://irisity.com/> (03/15/2023)

8 Products - Avigilon [Electronic resource]. URL: <https://www.avigilon.com/products> (accessed 04/03/2023)

9 Senstar Symphony Common Operating Platform [Electronic resource]. URL: <https://senstar.com/products/video-management/senstar-symphony-common-operating-platform/> (accessed 04/10/2023)

10 VIDEO ANALYTICS INNOVATION UNLEASHED [Electronic resource] URL: <https://www.briefcam.com/> (accessed 04/13/2023)

11 AI Powered SmartCam [Electronic resource] URL: <https://wirakom.com/DeepCAM> (accessed 04/28/2023)