Int. J. Advanced Networking and Applications
Volume: 16 Issue: 02 Pages: 6311– 6317 (2024) ISSN: 0975-0290

3-Step Risk Assessment and Dissemination Framework with CCTV Video for Crime Prevention

Yeonsu Kim, Seeun Kim
Division of AI Computer Science and Engineering, Kyonggi University, Suwon 16227, Korea
Email: {yeonsu0329, ssky601}@kyonggi.ac.kr
Jinho Ahn (Corresponding Author)
Division of AI Computer Science and Engineering, Kyonggi University, Suwon 16227, Korea
Email: jhahn@kyonggi.ac.kr

ABSTRACT

Existing crime prediction systems have limitations in crime prevention, lack of monitoring personnel compared to the number of installed CCTV cameras, and reliance solely on conventional investigation data and experience for determining crime risk levels. To overcome these limitations, this paper introduces a novel machine learning-based CCTV video analysis and dissemination framework for crime prevention. The framework is developed for providing swift and accurate compressed data sets of CCTV videos through risk assessment and analysis algorithms for behavior and target recognition, time-based crime occurrence rates, and detection of abnormal behavior. In addition, it can resolve the blind spot issue of the traditional CCTV video systems by our breadth-first search mechanism.

Keywords - **Crime Prevention, Risk Assessment, Video Analysis, Abnormal Behavior Recognition.**

Date of Submission: May 19, 2024 Date of Acceptance: June 16, 2024

I. INTRODUCTION

The existing crime prediction systems face several challenges such as difficulties in crime prevention, insufficiency of monitoring personnel compared to the number of installed CCTV cameras, and reliance solely on traditional investigative data and experience to assess crime risk[1]-[4]. To overcome these limitations, this paper proposes an active CCTV video analysis and delivery framework to predict crimes like in Fig. 1. The framework analyzes CCTV footages in real-time to measure the risk of each crime in three steps, behavior and target recognition, time-based crime occurrence rates, and detection of abnormal behavior in order. Then, in case of recognizing a high probability that it is a crime, it sends its relevant CCTV video dataset to monitoring personnel to facilitate immediate dispatch of police officers to the potential crime scene.

II. RELATED WORK

2.1 Legal and Integrity in Video Collection

The COVID-19 pandemic has limited direct investigative activities, increasing reliance on CCTV for crime

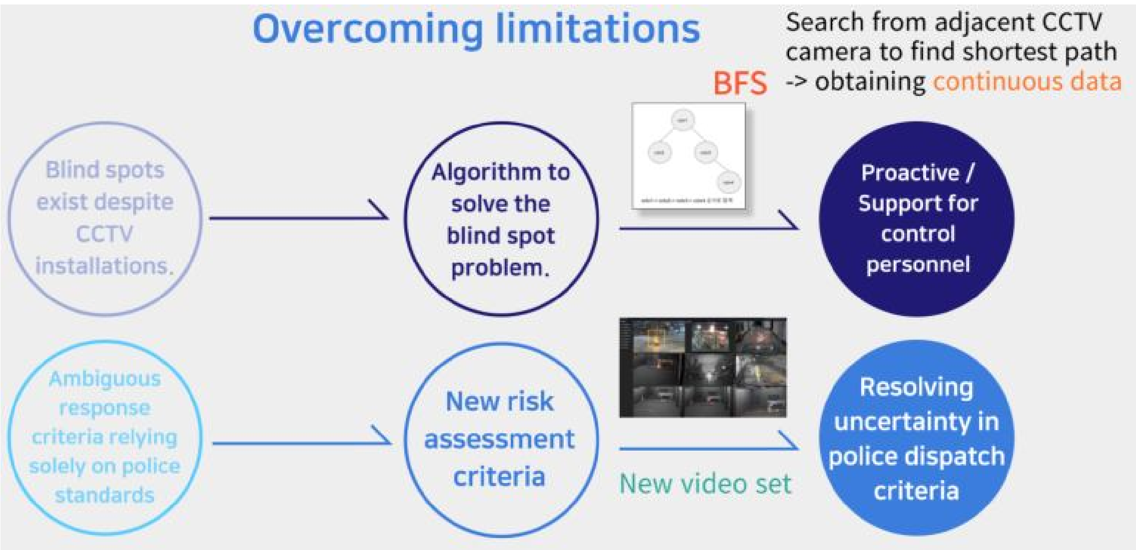

Fig. 1: Research idea

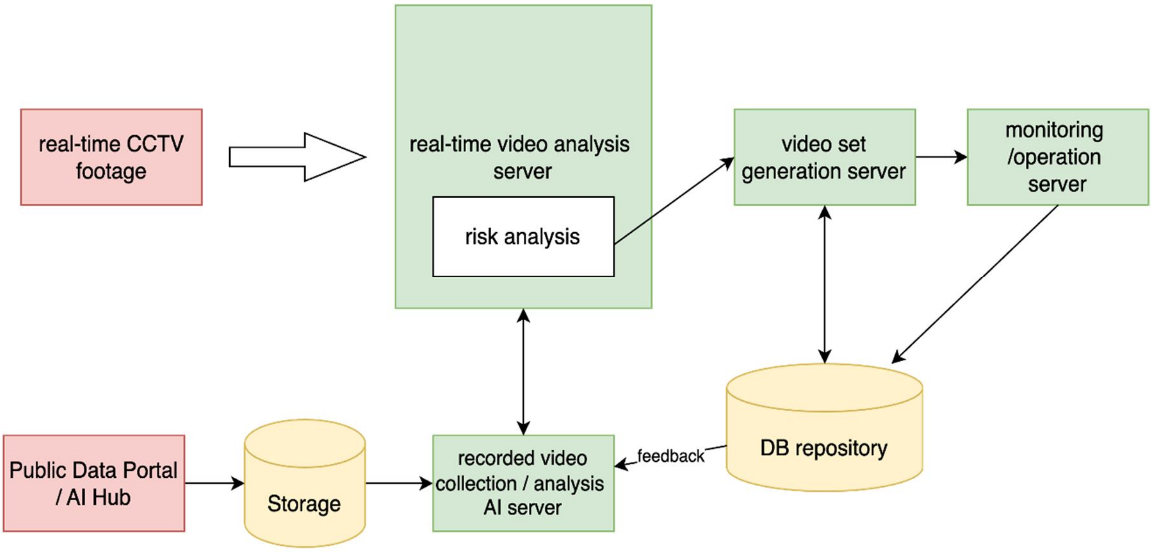

Fig. 2: Organization of the framework

prevention. However, concerns arise regarding potential infringement of citizens' rights[5]. Regulations such as the Personal Information Protection Act govern video collection by investigative agencies, emphasizing lawful and minimal intrusion. The Criminal Procedure Act outlines procedures for warrant-based and voluntary video collection, ensuring integrity and legal admissibility. Balancing investigative needs and privacy rights, adherence to legal procedures is crucial for maintaining the credibility of digital evidence.

2.2 Efficient CCTV Video Information Management

This study suggests implementing integrated video relay centers to streamline CCTV operations[6]. By consolidating independently operated monitoring centers regionally, it aims to boost management efficiency and propose collaboration policies among relevant agencies. Historically, disparate agencies managed CCTV systems independently, leading to investment duplication and maintenance challenges. Hence, the need for integrated centers has emerged, necessitating research on inter-agency coordination and platform integration. This study provides foundational insights for reducing duplicate investments and ensuring efficient CCTV control center operations.

2.3 Crime Deterrence Effect and Utilization Strategies

There still lacks precise scientific research and empirical analysis on the crime prevention and spillover effects of CCTV in Korea[7]-[9]. It is necessary to provide a comprehensive vision on the effects of CCTV installation and operational strategies that the public can understand. Accurate promotion is also needed.

2.4 Effectiveness of CCTV and its Utilization Methods

This research analyzes the effectiveness of CCTV for crime prevention and offender apprehension, along with discussing its utilization methods. The study compares crime trends before and after the installation and operation of CCTV in the Gangnam and Gangbuk areas[10]-[11]. The findings suggest that while CCTV is effective in crime prevention, its effectiveness diminishes over time. Additionally, CCTV has proven helpful in offender apprehension, and legal provisions are suggested to address regional disparities and ensure balanced utilization. Finally, continuous improvements are recommended to maximize the benefits of CCTV while minimizing human rights violations.

III. THE PROPOSED SYSTEM

3.1 Organization of the Framework

The system proposed in this paper consists of a set of components as illustrated in Fig. 2: a storage system for storing data provided by public data portals and AI Hub, an AI server for collecting and analyzing recorded video data from the storage, a server for analyzing real-time CCTV footage and measuring risk using trained AI models, a server for generating video sets, a database (DB) repository for storing generated video sets, and a monitoring/operation server. The results of the video sets transferred to the monitoring/operating server are compared with the results trained on the AI server, and these results are then reflected back to the video recording and analysis AI server.
Real-time CCTV footage is processed and stored using the openCV (Open-Source Computer Vision Library)[12] technology, aimed at open-source computer vision. Additionally, AutoML (Automated Machine Learning) technology, which automatically optimizes machine learning models, is employed to directly train for criminal behaviors. For the video data related to criminal behavior, the CCTV video data containing abnormal behavior provided by AI-Hub[13] is utilized, and the training video data for distinguishing the gender of individuals in the footage is utilized from the human action video data provided by AI-Hub[14].

Fig. 3: 3-Step risk analysis algorithm

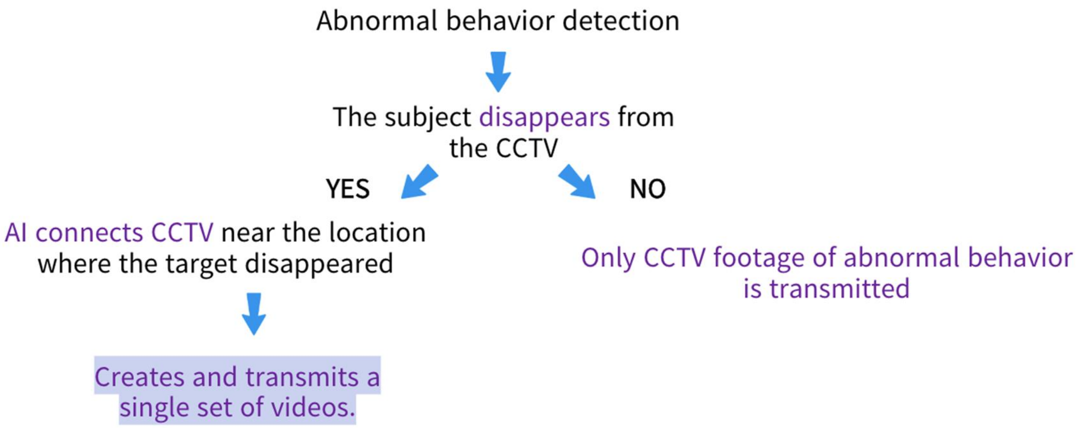

Fig. 4: CCTV video set generation algorithm

Risk is measured by analyzing the current situation, deriving characteristics and assigning weights through three criteria like in Fig. 3: behavior and target recognition, time-based crime occurrence rates, and abnormal behavior detection. If the risk exceeds a certain score and abnormal behavior is detected, a video set is created by connecting CCTV footage from the location where the target moved. This video set is then transmitted to the monitoring center, where experts confirm the risk. If deemed the target is in a dangerous situation with a certain high probability, the relevant police station is alerted for urgent response.

3.2 Key Features

3.2.1 CCTV Video Set Generation

One of the key functions of the system is the CCTV video set creation algorithm shown in Fig. 4.

If the object in the CCTV image disappears from the CCTV after abnormal behavior is detected, one image set is created by connecting CCTV videos near the location where the object disappeared. At this time, the adjacent CCTV is toured through Breadth First Search (BFS), and AI sequentially connects the images of the CCTV where the object is detected to create one image set.

If the target does not disappear from CCTV and continues to be in the video, only one CCTV footage of abnormal behavior is transmitted.

The video set is transmitted to the control center, and if the risk is high after an expert checks the video at the control center, the police station is notified to enable emergency dispatch.

Here is an example of creating a video set in Fig. 5. This figure depicts the sequential generation of a video set assuming that the target moved in the order of CCTV 1, CCTV 2, and CCTV 4. CCTV 1 acts as the root, searching for the target in adjacent CCTV 2 and CCTV 3.

Once the target is found in CCTV 2, CCTV 2 becomes the new root and searches for the target in adjacent CCTV 4 and CCTV 5. Eventually, the target is detected in CCTV4. This method sequentially combines CCTV 1, CCTV 2, and CCTV 4 into a set.

3.2.2. Risk Assessment on Crime

One of the key functions of the system is the risk assessment on crime like in Fig. 6. Based on behavioral monitoring and time-zone data, we analyze the current situation and derive characteristics.

Volume: 16 Issue: 02 Pages: 6311– 6317 (2024) ISSN: 0975-0290

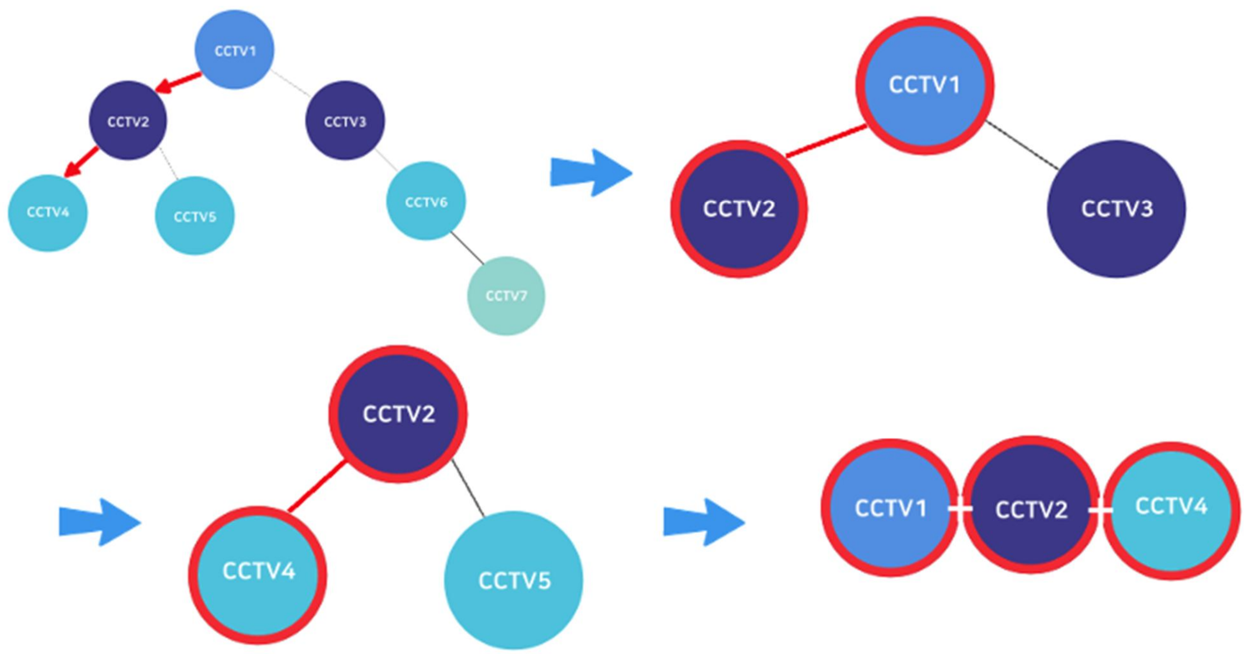

Fig. 5: Example of a video set generation process

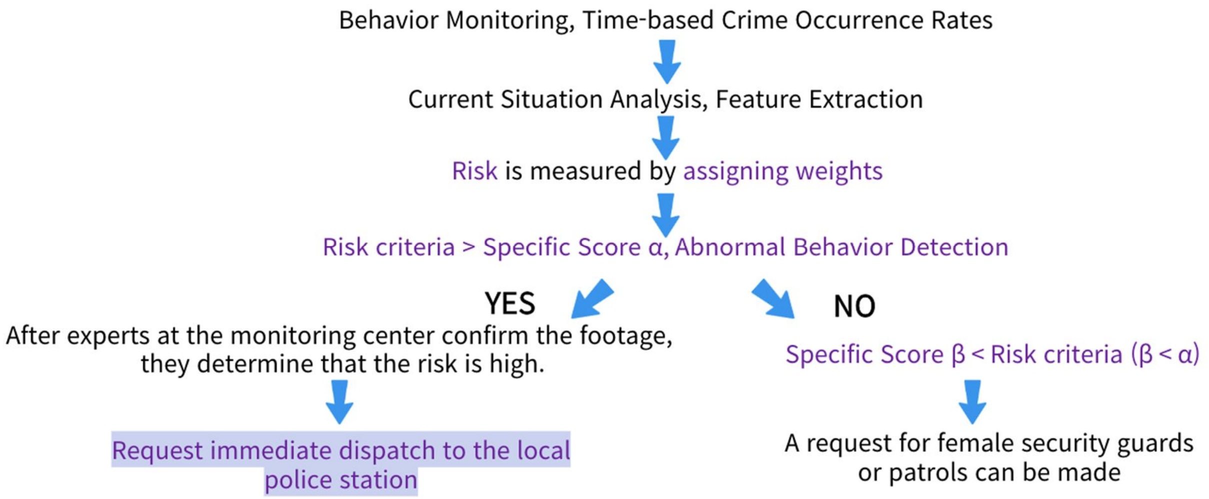

Fig. 6: Risk assessment on crime

After that, we measure the risk by weighting it. If abnormal behavior is detected and its risk level is greater than a certain score, the control center checks the video and determines the risk. If the risk is high, it automatically notifies the police station in charge to enable emergency dispatch.
If the risk level is less than the score, but greater than a designated baseline, you can request the women's guard or patrol.

3.3 Risk Analysis Algorithm

Fig. 7 is the risk analysis algorithm in which CCTV footages are collected in real-time, pertaining to the analysis of one video. The algorithm operates on the following three criteria. The first criterion is behavior and object recognition, which analyzes real-time CCTV videos to assign appropriate weights according to the existence of specific targets and their duration of action. When the total weight reaches a certain threshold γ, the process proceeds to the next criterion. Second, public data are used to calculate the crime rate for each time zone and assign the corresponding weights accordingly, and if the total weight value is greater than or equal to a certain level α, the process proceeds to the next criterion. Third, the designed AI model performs a procedure to detect abnormal behavior in the CCTV video. If it is determined to be an abnormal behavior, it is considered a high-risk situation and the current video is processed and transmitted to the integrated control center. The execution processes according to the three criteria,

Volume: 16 Issue: 02 Pages: 6311– 6317 (2024) ISSN: 0975-0290

which are the core elements of this algorithm, will be described in more detail in the next section.

3.3.1. Risk Analysis Criterion 1 – Behavior and Target Recognition

Criterion 1 for risk analysis involves analyzing the current situation and deriving characteristics from the human action video dataset (2020) provided by AI Hub[14], and assigning weights through this process. If, as shown in Table 1, there are no individuals other than the excluded two targets, consisting of at least one female, in the real-time CCTV footage, a weight is assigned.

Table 1: Risk analysis criterion - behavior monitoring

Classification	Step	Evaluation criteria
Behavior monitoring	1	Are there any other individuals aside from the two targets on the screen?
	2	Has the situation where there are no other individuals aside from the two targets on the screen been maintained for x hours or more? (0 < x)
	3	Has the situation where there are no other individuals aside from the two targets on the screen been maintained for y hours or more? (x < y)

More weight is assigned when the situation persists for more than x hours without any individuals other than the two targets being present in the footage, and also when it persists for more than y hours (0 < x < y). Once the total assigned weight reaches a certain score γ, the analysis progresses to criterion 2 of the risk analysis. If the weight assigned at each step is less than γ, the algorithm terminates.

3.3.2. Risk Analysis Criterion 2 – Time-based Crime Occurrence Rates

The risk level of a crime increases according to the time slot when crimes are concentrated and repeatedly occur together. Therefore, criterion 2 of the risk analysis calculates the crime occurrence rate by time slot using the 'Crime Occurrence Time and Day of the Week' openAPI provided by the Public Data Portal and assigns weights accordingly.
Weights are assigned based on the crime occurrence rate by time slot. If the total score reaches α or higher, the analysis progresses to the third step. Additionally, if the total score is less than α but greater than or equal to β, a request for female security guards or patrols can be made, and if it is less than β, the algorithm terminates (γ < β < α).

3.3.3. Risk Analysis Criterion 3 – Abnormal Behavior Detection

An AI model is trained using AutoML with the CCTV video data containing abnormal behaviors[13] to detect individuals exhibiting abnormal behavior. The abnormal behavior CCTV video data is provided by AI Hub to detect 12 types of abnormal behaviors, including assault, fighting, theft, fainting, loitering, robbery, dating violence and harassment, kidnapping, intoxication, among others.
When certain abnormal behaviors are detected, there is a high risk of direct harm to the victim. Therefore, a CCTV video set is created and transmitted to the monitoring and operation center. Additionally, if no abnormal behavior is detected for *n* minutes, the algorithm terminates.

3.4 Algorithm for Resolving CCTV Blind Spot Issues

Despite the continuous increase in the number of CCTV installations and operations each year, blind spots still

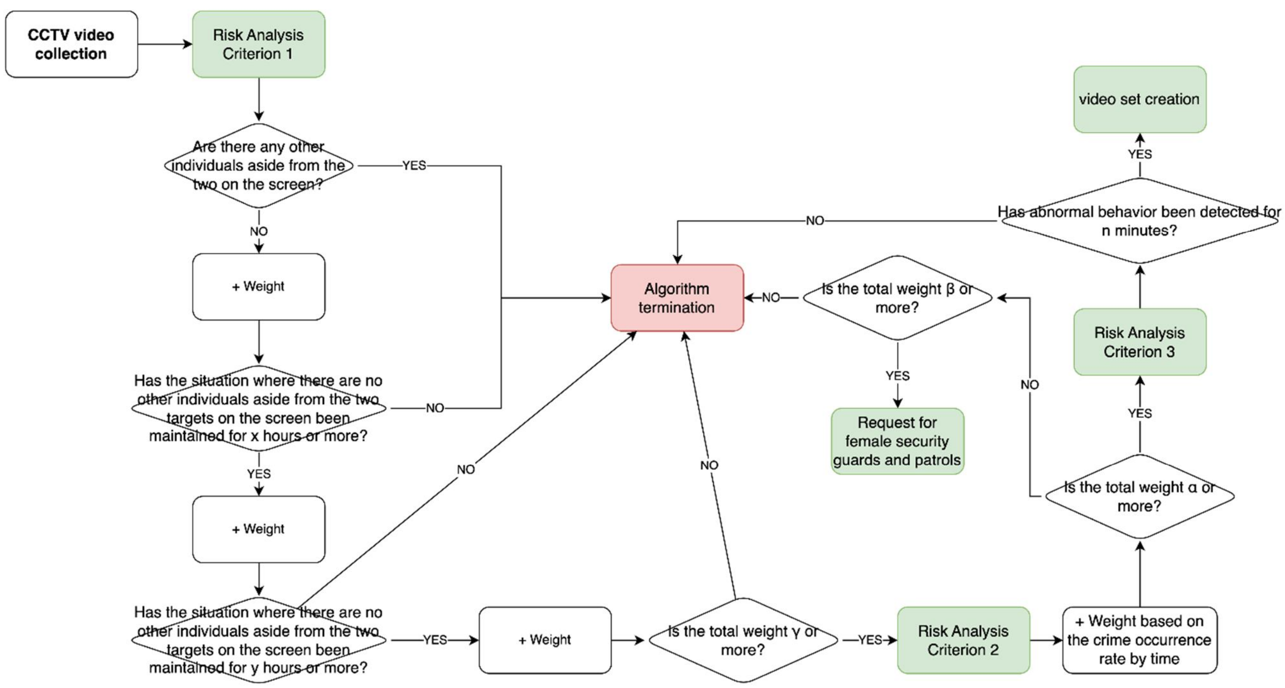

Fig. 7: Risk analysis algorithm

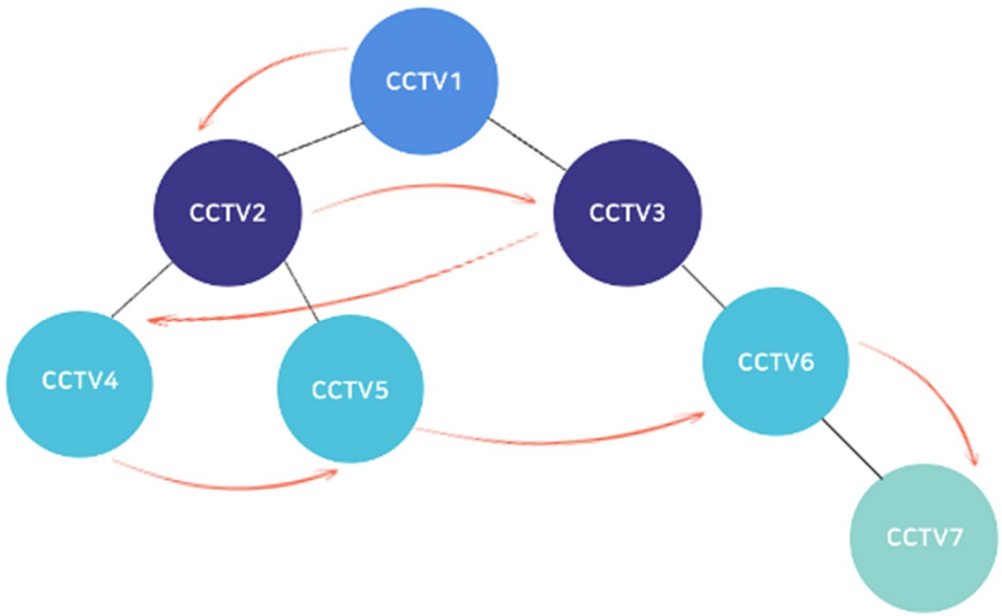

Fig. 8: Example of the CCTV BFS structure

persist. This issue stems from limitations in CCTV installation, and our system cannot completely eradicate this problem. Therefore, this system proposes measures to supplement this blind spot issue.

When a target disappears into a blind spot within the observation area of a CCTV, we utilize BFS to search from the nearest CCTV containing the target. Since it is necessary to check all CCTV cameras adjacent to the first CCTV where the target appeared, we opt for the BFS search method. Through BFS, individuals appearing on the selected screen are examined to determine if the target is present. If the target is not found, the system moves on to the next CCTV on the BFS search structure. Fig. 8 illustrates the structure for BFS search for CCTVs as described above.

IV. DISCUSSION

This section describes how the control algorithms used in the intelligent system designed in this paper can significantly improve crime prevention and damage mitigation effects compared to previously developed stand-alone CCTV-based control systems in two aspects. Most existing systems deployed in each country for crime prevention worldwide were generally developed that police personnel in the integrated control center fully monitor videos acquired from them and carry out the analysis of the possibility of crime[15]. For this reason, a large number of crime possibility analysis personnel are deployed in the control center, increasing the cost, and there is insufficient number of police personnel to dispatch to the scene where the crime is likely to occur[16].

This practical difficulty may lead to a problem in that the results of determining the possibility of a crime derived by analyzing real-time images collected from CCTV cannot be properly utilized in the field[17]. The automated deep learning-based semi-real time crime likelihood analysis and video generation system designed in this paper can significantly alleviate the problem of on-site police personnel shortages by greatly reducing the cost of monitoring and analysis personnel.

Secondly, violent crime types such as murder, assault, and arson are instantaneous and dynamic, making it difficult for the conventional CCTV control systems to significantly enhance the effectiveness of reducing this type of crime damage in the event of a crime due to their lack of proactivity. However, to address the limitation, the proposed system quickly identifies CCTV devices on the route from the start of the crime, using a BFS tree, and then connects them to generate and deliver a set of crime progress videos, enabling continuous real-time tracking of on-going crime situations.

V. CONCLUSION

This paper proposes an AI-based video analysis system for swift crime tracking to overcome the limitations of existing systems, such as the challenges in crime prevention, lack of monitoring personnel compared to the number of CCTV installations, presence of blind spots, and unclear criteria for police dispatch relying solely on the police's existing investigative data and experience. The proposed method is as follows:

First, crimes are directly trained using AutoML with abnormal behavior CCTV video data[6] and human action video data [7] provided by AI Hub. Subsequently, real-time CCTV footage is processed and stored using OpenCV technology. Second, the risk level is measured by analyzing the current situation and deriving characteristics through three risk analysis criteria: behavior and target recognition, time-based crime occurrence rates, and abnormal behavior detection. If the weight exceeds a certain score and abnormal behavior is detected, a video set is created by connecting CCTV footage from the location where the target moved using the blind spot resolution algorithm, traversing adjacent CCTV cameras with BFS to sequentially connect footages from cameras where the target is detected. If the target continues to remain in one video without disappearing, only one CCTV footage where abnormal behavior is detected is transmitted. When the total weight reaches α or higher, the generated video set is transmitted to the monitoring center, and if experts determine that the risk is high, the local police station is notified for urgent response. If the weight exceeds β but is less than α, a request for female security guards or patrols is made instead of creating a video set.

For future works, we intend to expand the system designed in this paper so that the accident site can be continuously tracked to drive the damage to minimize through traffic accident crime prediction[18]. Also, we consider the specificity of these potential crime scene video data while developing an improved security mechanism similar to the one[19] to deliver and manage them more safely and efficiently, applying it to our system.

ACKNOWLEDGEMENTS

This work is an extended version of a paper presented in the conference[20].

REFERENCES

[1] Y.G. Kang, and Y.H. Yeom, A Study on the Crime Prevention Effectiveness of CCTV, *Journal of Community Safety and Security by Environmental Design*, 11(2), 2020, 35-59.

[2] A.A. Adams and J. M. Ferryman, The future of video analytics for surveillance and its ethical implications, *Security Journal*, 28, 2015, 272–289.

[3] H. Idrees, M. Shah, and R. Surette, Enhancing camera surveillance using computer vision: A research note, *Policing: An International Journal*, 44, 2018, 292–307.

[4] E.L. Piza, J.M. Caplan, and L.W. Kennedy, CCTV as a tool for early police intervention: Preliminary lessons from nine case studies, *Security Journal*, 30, 2017, 247–265.

[5] G.M. Lee, *A Study on Securing Legality and Integrity for CCTV Video Information Gathering of Investigation Agency in Terms of Digital Forensics*, Sungkyunkwan University Graduate School, 2022.

[6] W. Park, *A Study on the implementation of integrated video relay center for the efficient management of CCTV video information resources*, Seoul: Hansei University Graduate School of Knowledge Services & Consulting, 2014.

[7] W.S. Yoon and J.H. Kim, A Study on the Effect of CCTV on Residents' Perception of Safety: National Data Analysis, *Korean Police Studies Review*, 19(4), 2020, 87-116.

[8] H. Lim and P. Wilcox, Crime-reduction effects of open-street CCTV: Conditionality considerations, *Justice Quarterly*, 34, 2017, 597–626.

[9] Y.S. Hwang, *A study on the effect of CCTV on the deterrence of crime and its efficient application scheme*, Master's thesis, Yonsei University Graduate School of Public Administration). Seoul, South Korea, 2009.

[10] M. Gerell, Hot spot policing with actively monitored CCTV cameras: Does it reduce assaults in public places?, *International Criminal Justice Review*, 26, 2016, 187–201.

[11] S.J. Lee, *Analysis of the Effectiveness of CCTV for Crime Prevention and Offender Apprehension, and its Utilization Methods*, Master's thesis. Graduate School of Policy Studies, Korea University, Seoul, 2010.

[12] OpenCV: Open Source Computer Vision Library, OpenCV, 2021, [Online]. Available: https://opencv.org/. Accessed: 2021.

[13] Abnormal Behavior CCTV Footage, AI-Hub, 2023, [Online]. Available: https://aihub.or.kr/aihubdata/data/view.do?currMenu=115&topMenu=100&aihubDataSe=realm&dataSetSn=171. Accessed: 2023.

[14] Human Motion Video (2020), AI-Hub, 2023, [Online]. Available: https://aihub.or.kr/aihubdata/data/view.do?currMenu=115&topMenu=100&aihubDataSe=realm&dataSetSn=61. Accessed: 2023.

[15] E. Piza, B. Welsh, D. Farrington, and A. Thomas, CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis, *Criminology & Public Policy*, 18(1), 2019, 135-159.

[16] E. Piza, CCTV Video Surveillance and Crime Control: The Current Evidence and Important Next Steps. In B. Welsh, S. Zane, & D. Mears (Ed.), *The Oxford Handbook of Evidence-Based Crime and Justice Policy* (New York: Oxford University Press, 2024) 265-285.

[17] E. Piza, S. Chu, and B. Welsh, Surveillance, action research, and community technology oversight boards: A proposed model for police technology research. In E. Piza & B. Welsh (Ed.), *The Globalization of Evidence-Based Policing: Innovations in Bridging the Research-Practice Divide* (London, UK: Routledge Press, 2022) 206-222.

[18] T. Almanie, Quantitative Study of Traffic Accident Prediction Models: A Case Study of Virginia Accidents, *International Journal of Advanced Networking and Applications*, 14(5), 2023, 5582-5589.

[19] A. Sunday, O. Olufunminiyi, An Efficient Data Protection for Cloud Storage Through Encryption, *International Journal of Advanced Networking and Applications*, 14(5), 2023, 5609-5618.

[20] Y. Kim, S. Kim, and J. Ahn, Near Real-time CCTV Video Analysis and Delivery Framework for Predicting Crimes, *Proc. 5th International Conference on Advanced Information Technology*, Phu Quoc, Vietnam, 2024, 24-27.