International Journal on Advanced Science Engineering Information Technology

Vol.15 (2025) No. 3
ISSN: 2088-5334

Leveraging AI to Revolutionize Video Forensics: Developing an Expert System for Method Selection

Erika Ramadhani [a,*], Rusydi Nurdin [a]

[a] *Department of Informatics, Universitas Islam Indonesia, Sleman, Yogyakarta, Indonesia*
Corresponding author: [*]erika@uii.ac.id

***Abstract*—The rapid growth of digital data and the increasing prevalence of cybercrime have created an urgent need for advanced tools in digital forensic investigations, particularly in video analysis. This study introduces an expert system that leverages forward chaining techniques to recommend forensic methods tailored to the specific attributes of a given case. The system integrates a comprehensive knowledge base with an automated rule application to streamline the decision-making process, reducing dependence on manual selection and minimizing human error. Results from experiments demonstrate that the system performs effectively. Compared to traditional manual methods, it reduces the time required to select a method by 30% and enhances the accuracy of the analysis by 25%. For example, the time required for low-resolution video enhancement decreased from 20 to 12 minutes, while tampered video detection improved from 25 to 15 minutes. These advancements demonstrate the system's ability to address common challenges in video forensics, such as detecting alterations, verifying metadata, and analyzing low-quality footage. The proposed system enhances the efficiency and reliability of forensic investigations by automating the selection of appropriate analysis methods based on predefined rules. By eliminating manual guesswork, it ensures consistent, accurate, and repeatable results, enabling investigators to focus on more complex aspects of their work. Additionally, the system's scalability and adaptability allow it to accommodate evolving forensic methodologies and diverse investigative scenarios. Overall, this research highlights the transformative potential of AI-driven expert systems in addressing the increasing demands of digital video forensics in the modern era.**

***Keywords*—Digital forensics; video analysis; expert system; forward chaining; artificial intelligence.**

Manuscript received 7 Jun. 2024; revised 18 Jan. 2025; accepted 26 Mar. 2025. Date of publication 30 Jun. 2025.

I. INTRODUCTION

Digital forensics, a branch of science that focuses explicitly on the examination and investigation of digital or electronic data and information, plays a vital role in both legal and security contexts. The primary purpose of digital forensics is to gather, analyze, and preserve digital evidence that is closely related to a specific crime or legal event [1]–[3]. Cases such as fraud, security breaches, and cybercrime are examples that are often the subject of digital forensics. In carrying out its functions, digital forensics implements a comprehensive set of investigative techniques [1]. Information that has been deleted or hidden can be recovered through detailed data analysis. Identification and analysis techniques in computer networks are also covered, as well as the gathering of good digital evidence for use in court. The existence and application of digital forensics, therefore, are key in ensuring that justice and truth can be revealed in various legal cases in today's digital age [4]–[6].

The digital forensic process consists of successive steps during the investigation process. One of the most crucial phases in the investigation process is the process of analyzing digital data, in which this digital data will then be used as valid evidence in court arrangements [5], [7], [8]. Digital data analysis is conducted by a researcher who must possess a strong understanding of computer systems, networks, and digital devices, as well as the ability to utilize specialized tools and techniques to analyze digital evidence. They must also possess a keen attention to detail and the capacity to recognize patterns and anomalies within the data. However, researchers often face challenges when choosing specific methods for their analysis process. Inappropriate choice of analysis methods can lead to suboptimal analysis processes, which can result in delays in the completion of research [9]–[11].

However, what often happens is that during the analysis of multimedia data, especially in video forensics, researchers frequently find it challenging to determine which analysis methods to use. Choosing the proper method of analysis for video analysis is crucial for a researcher. However, researchers typically need to conduct a literature review first when dealing with video forensic cases. This could lead to a prolonged investigative process [1], [10]. One of the significant challenges facing digital researchers is the early uncertainty about the existence of digital evidence in the early stages of the investigation. Furthermore, even when they find evidence, determining its relevance to the case can be a challenging task. Digital investigations are becoming increasingly demanding and time-consuming due to the proliferation of data sources, expanded storage capacity, and the growing use of encryption and other secure technologies [3]. Digital forensics and intelligent systems can complement each other in the investigation and analysis of digital information [12]. The application of AI technology in digital forensics serves as a means of decision-making [5], [13], acts as a tool of intelligence, and functions as an automation tool. Specialized techniques can integrate these tools.

Digital forensics could apply a wide range of AI techniques. Some of the mentioned examples include vector support machines, agent-based systems, and conceptual clustering. Most of the work in applying AI to digital forensics is still in its early stages and can be divided into two areas: (1) where AI is used to help automate individual parts of forensic processes (e.g., to find specific file types) and (2) where AI can be used to guide experts in their tasks [14]. Azad et al [15] and Fakiha [16] both talk about how AI can be used in network forensics and cyber threat analysis, focusing on how it can be used to find attacks and improve the classification of threats automatically. Rawat et al [13] goes into more detail about the possible security risks that come with AI algorithms and the need for AI forensics to stop crimes that involve AI. Vasilaras et al [17] gives an in-depth look at where AI stands in mobile forensics, emphasizing the importance of AI systems being transparent, open, and robust. All of these studies show how AI has changed digital forensics and incident response. They also demonstrate the importance of ongoing research and development in addressing emerging problems and risks.

In this paper, we develop an expert system design using forward chaining that can be used as a method selection recommendation in the process of forensic video analysis. We followed several stages in the design of this expert system. First, we conducted an in-depth literature study of the various forensic video analysis methods that existed. Second, based on a study of this literature, we identified the critical characteristics of each forensic video analytics method. Third, we designed an expert system that can suggest the best forensic video analysis method by taking into account the features of the chosen analysis method. Fourth, we reviewed the experts' system designs to ensure that the method selection recommendations meet the needs of forensic video analysis. By following this stage, it is hoped that the expert forensic video analysis system we have developed could be useful in helping investigators choose the most effective method of analysis.

The structure of the paper was as follows: in the first part, we discussed the background of the article and the problems facing it. The second part covers the research methodology of this article, followed by the outcome and discussion in the third part. The fourth part presents the conclusion of this article.

II. Materials and Method

A. Material

1) Video: The experimental data used for analysis in the video were obtained from CCTV recordings on YouTube and Kaggle datasets. In this study, we conducted three experiments using video capture. The video captured was of human detection, including plate numbers, and people committing theft.

2) Video Forensics Method: There are many methods of analysis for video forensics. Xiang et al [18] and Choudhary et al [19] explained the importance of metadata analysis in video file forensics. Xiang et al [18] focused on using metadata features, and Choudhary et al [19] proposed a framework that includes video and image enhancement techniques. Sukamto et al [20] specifically discusses the analysis of CCTV video recordings, stressing the need for methods that can be used as forensic evidence. Bagkratsas and Sklavos[21] introduced a new method for fraud detection, based on Dense Optical Flow characteristics, which are relevant for cheap devices that capture static CCTV video. Based on that, the importance of metadata analysis, video enhancement, and fake detection in forensic video analysis

The primary objective of this research is to understand the methods of forensic video analysis, which can aid in criminal investigations. The study proposes a framework for forensic video analysis that uses video and image enhancement techniques for low-quality videos from social media and CCTV recordings. The study reviews the use of various parameters, including metadata analysis, to authenticate videos and distinguish between real and modified videos [19].

A study by [22] provides a comprehensive taxonomy and an overview of the latest research on fake multimedia video detection techniques. It covers various aspects of video fraud detection, including deep learning algorithms, anti-forensics, compression methods, datasets, and challenges. This article also discusses deepfake detection and provides an overview of forensic software and tools for video detection.

B. Method

Research methods are the measures of research carried out to achieve the objectives of the study. This research develops an expert system design to solve problems in selecting analysis methods during forensic video investigation. The steps are shown in Figure 1.

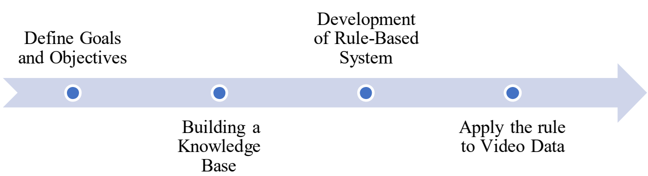

Fig. 1 Method of designing an expert system adapted [23]

The application of forward chaining, a primary technique in artificial intelligence and expert systems, provides significant advantages in forensic video analysis. This approach can be very effective in accelerating investigations and improving accuracy. Here's how to implement forward chaining in forensic video analysis:

1) Define Goals and Objectives: Set clear objectives for forensic video analysis. The objectives may include identifying suspects, reconstructing events, or extracting specific information from video data. These steps are important to direct further analysis to stay focused and relevant.

2) Building a Knowledge Base: Creating a comprehensive knowledge base dedicated to forensic video analysis. This database should cover a wide spectrum of rules and facts relevant to this field. Typically, this could encompass a range of video format characteristics, strategies for enhancing video quality, methods for detecting video manipulation, and guidelines for extracting accurate data from video. This knowledge base serves as the foundation for the forward chaining process.

3) Development of Rule-Based System: The essence of forward chaining is a rule-based system in which inference rules are applied to available data to draw further information or conclusions, continuing until the desired goal is achieved. In forensic video analysis, these rules may encompass methodologies for detecting image manipulation, facial recognition algorithms, or specialized techniques for extracting and enhancing low-quality footage. Rules-based systems must be agile and robust to handle the complexity and nuances of video data.

4) Apply the rule to video data: Perform analysis with raw video data, applying rules from the knowledge base systematically. For example, if the goal is to identify a suspect, you might start with a basic image enhancement rule, followed by a facial recognition algorithm. This step is iterative, with any application of the rule potentially revealing new information or pathways for further analysis.

By implementing forward chaining in forensic video analysis, investigators can systematically navigate through large amounts of video data, making the process more efficient, accurate, and aligned with specific investigative purposes.

III. Results and Discussion

A. Define Goals and Objectives

The system is designed to enhance the process of digital forensic investigation in video analysis. It addresses the inherent challenge faced by investigators in choosing the right method for forensic video analysis, a task often characterized by its complexity and high potential for human error. The aim is to improve both the efficiency and accuracy of forensic investigations by automating the decision-making process. The expert system does this by carefully examining the characteristics of video data and methodically applying relevant rules to guide researchers towards the most appropriate method of analysis.

B. Building a Knowledge Base

The development of a knowledge base in an expert system for video forensic analysis, as described in the document, involves several important stages. The process begins with an in-depth review of the literature on various forensic video analysis methods. Based on these characteristics, the expert system design was made to recommend the most appropriate method of forensic video analysis.

The next step in building a knowledge base is developing a rule-based system. This system utilizes rules developed based on knowledge collected to analyze videos according to their characteristics. For example, rules can specify specific methods of analysis to be used on low-resolution videos or on certain formats. Once the knowledge base and rules-based systems are developed, these rules are applied to video data.

The system then automatically determines the most appropriate method of analysis based on the video characteristics given. Thus, the system can provide quick and accurate recommendations to forensic investigators, facilitate the investigation process, and improve the effectiveness of concluding the video analyzed. Table 1 is a characteristic used to create an expert system.

TABLE I
CHARACTERISTICS OF VIDEO FORENSICS

Characteristic	Code	Method	Justification
If the video is highly compressed or of poor quality	A1	Apply video enhancement techniques.	Enhancing the video can help improve visibility and extract relevant details, such as faces or license plate numbers, from low-quality footage.
Verify its authenticity if the video contains a timestamp or metadata	A2	Verify using time synchronization techniques.	Authenticating timestamps and metadata ensures the reliability and integrity of the evidence, helping establish the sequence of events accurately.
If the video is shaky or unstable	A3	Apply video stabilization techniques.	Stabilizing the video reduces motion blur and jitter, making it easier to analyze and extract relevant information from the footage.
If the video contains areas of interest with insufficient visibility	A4	Apply video enhancement techniques.	Enhancing specific regions within the video, such as dark or obscured areas, can reveal hidden details and assist in identifying important elements.
If the video contains obscured or pixelated faces	A5	Apply facial recognition or facial reconstruction techniques.	Facial recognition or reconstruction techniques can help identify individuals by comparing facial features to known databases or reconstructing obscured faces for identification purposes.
If the video requires identification of specific objects or text	A6	Apply video magnification or text recovery techniques or object detection.	Magnifying specific objects or recovering text from the video can aid in identifying critical

Characteristic	Code	Method	Justification
			information, such as logos, vehicle identification numbers, or handwritten notes.
If the video is suspected to be tampered with	A7	Apply video authentication and integrity verification techniques.	Video authentication and integrity verification techniques help determine if the video has been altered, tampered with, or manipulated in any way, ensuring the reliability of the evidence.
If the video contains multiple camera angles or perspectives	A8	Apply video synchronization and analysis techniques.	Synchronizing multiple video feeds and analyzing them together can provide a more comprehensive understanding of the event, enhancing accuracy and aiding in reconstructing the sequence of events.
Identify the source of video	A9	Apply video source identification technique	Identifying the source of a video plays a pivotal role in legal investigations, court proceedings, and maintaining the integrity of the justice system.
Concealed information in the video	A10	Apply video steganography analysis	Enhances the integrity and reliability of video analysis in legal, investigative, and security contexts.
Revealed hidden information in corneal reflections	A11	Apply 3D reverse projection analysis	Revealed hidden information in corneal reflections can be a valuable tool in specific situations where it can provide critical insights into the content, context, and authenticity of video evidence.

C. Development of Rule-based System

A decision table, in the context of an expert system, is an essential tool for knowledge representation and decision-making. Essentially, a decision table is a structured approach used to compile various rules and conditions within a system. In each decision table, rows represent a particular condition or a combination of conditions, while columns describe actions or decisions to be taken based on such conditions.

Each cell in the table provides an appropriate response to each combination of conditions, making it easier for the expert system to evaluate a variety of scenarios and determine the best action based on the established rules. This enables the specialist system to handle complex situations in a more structured and systematic manner, ensuring that every decision is made consistently and based on logic that has been programmed in advance. The use of these decision tables is crucial in improving the reliability and efficiency of expert systems in a variety of applications, from data processing to decision-making support [24], [25].

Rule-making based on forward chaining techniques is based on the decision table. So, examples of rule-making can be seen in Table 2. The output of the rule is a method recommendation. This means that the rules developed using such forward chaining techniques are designed to provide recommendations for the most appropriate method based on specific criteria or conditions set.

Table 2 provides concrete examples of how these rules are applied in practice. Outputs in the form of recommendations of these methods become very useful, especially in systems that aim to provide solutions or suggestions for specific actions based on a set of input or data provided by the user. This method allows the expert system to automatically extract conclusions and give recommendations that are accurate and relevant to the context of the problem being faced.

TABLE II
RULE MAKING

Rule	Statement
1	IF video highly compress THEN enhancement technique
2	IF verify its authenticity THEN time synchronization technique
3	IF shaky or unstable THEN apply stabilization technique
4	IF video contains area of interest THEN video enhancement technique
5	IF video contains obscured or pixelated face THEN facial recognition or facial reconstruction
6	IF video requires identification of object THEN object detection or object magnification or text recognition
7	IF video suspected to be tampered THEN video authentication and integrity verification technique
8	IF video contains multiple camera angle or perspective THEN video synchronization and analysis techniques
9	IF video type analysis THEN video source identification technique
10	IF concealed information in the video THEN video steganography analysis technique
11	IF hidden information in corneal reflection THEN 3D reverse projection analysis

D. Rule Application to Video

At this stage, we discuss how to implement the use of expert systems when conducting video investigations. Regarding Fig. 1, the expert system implementation is performed during the analysis process. We aim to provide a comprehensive and in-depth examination of the complexities surrounding the application of expert systems in digital forensic investigations, with a particular focus on their use in analyzing video data, in the forthcoming section. The rules are summarized in Table 2.

When analyzing a video that has been tampered with, we can observe from Table 2 that rule 7 states: If a video is suspected of being tampered with, then utilize a video authentication and integrity verification method. Another example is the use of rule 9: IF video type analysis, THEN video source identification technique—when you want to know where the camera or recording device came from. In comparison, various scenarios exist for video content analysis, including those involving video quality issues, brightness, compression, and other factors, such as the quantity of visible features.

Fig. 2 Example of the video capture: object detection

Fig. 3 Plate number enhancement

Fig. 4 The guy who stole the charity box

Figs. 2, 3, and 4 are some examples of a CCTV capture. The image on the left is the analysis result of performing object detection on the captured result by implementing rule 6. While the middle of the image contains the capture of a plate number, an expert system implementation can be used to apply rule 1 by performing enhancements on the result of that capture. Finally, in the picture on the right, the implementation of rule 5, which clarifies the victim's face by performing facial recognition and facial reconstruction techniques, could previously be achieved by applying rule 1 to perform an enhancement process on video capture.

E. Implementation of System

The forward-chaining techniques used in expert systems for video forensic investigations play a crucial role in streamlining the investigation process and enhancing the accuracy of the results. By automating the decision-making process, this technique enables forensic investigators to input specific video characteristics, after which the system automatically applies a predefined set of rules to determine the most suitable method of analysis. This automation not only speeds up analysis, which is crucial in time-sensitive forensic investigations, but also reduces the likelihood of human error that can occur with manual processing [26], [27]. The consistency achieved through rule-based analysis ensures reliable and uniform results for similar video data types, thereby improving the accuracy of investigations. Furthermore, forward chaining adaptability is key in the dynamic field of digital forensics, as systems can incorporate new rules or modify existing ones in response to evolving forensic methodologies. This adaptability ensures that the analysis remains up-to-date and accurate. In addition, the comprehensive analytical nature, in which each video characteristic is carefully considered and all relevant rules are applied methodically, ensures a thorough examination of the video data. As a result, this rigor significantly contributes to the overall accuracy of forensic investigations, ensuring that the most suitable method of analysis is selected. In essence, forward-chaining techniques in expert systems not only accelerate forensic processes but also significantly enhance the reliability and effectiveness of forensic video investigations.

In the expert system for video forensic investigation, which utilizes forward chaining techniques, several specific steps form the primary foundation of the process. First, setting a goal is a crucial first step. Here, the purpose of video forensic investigation is specifically defined, including identifying the source of the video, detecting manipulations, and extracting vital information from the video. The second step is to build a knowledge base. In this phase, the knowledge related to forensic video is collected and organized. These can include types of video formats, standard analytical techniques, as well as the challenges that often arise in video forensics.

Then, based on the knowledge base that has been created, specific rules are developed. These rules are designed to guide the system in analyzing videos according to their respective characteristics. For example, a rule can specify a specific method of analysis to be used on a low-resolution video or a particular format. The final step is to apply a rule to video data. At this stage, the video being tested is inserted into the system, and the laws that have been developed are used to analyze the video. The system then automatically determines the most appropriate analysis method based on the characteristics of the given video. In this way, the system can provide quick and accurate recommendations to forensic investigators, facilitating the investigation process and increasing the effectiveness of concluding the video analysis.

F. Characteristics and Rule

Each video characteristic has a significant impact on determining the correct forensic analysis method. For example, highly compressed or low-quality videos may require video enhancement techniques to improve visibility and remove essential details such as faces or vehicle plate numbers. On the other hand, videos containing timestamps or metadata may require verification using time synchronization techniques to ensure the authenticity and integrity of evidence. Other characteristics, such as shaky or unstable videos, may require video stabilization techniques to reduce blur and jitter, facilitating the analysis and extraction of relevant information.

The expert system designed in this study uses forward chaining techniques to facilitate this decision-making process [28]. By referring to the established video characteristics tables and rules, the system automatically applies relevant rules to the video data being analyzed. This process begins with determining the purpose of the analysis, such as identifying a suspect or reconstructing an event, followed by building a knowledge base that includes rules and facts relevant to video forensics.

Once the knowledge base and rule-based systems have been developed, these rules are applied to raw video data. For example, if the goal is to identify a suspect, the system may start with a basic image enhancement rule followed by a facial recognition algorithm. This step is iterative, with each application of the rule potentially revealing new information or pathways for further analysis. By applying forward chaining techniques in forensic video analysis, investigators can systematically navigate through large amounts of video data, making the process more efficient, accurate, and aligned with the specific purposes of the investigation.

G. Evaluation and Effectiveness

Evaluation involves a series of tests and adjustments to the system to ensure that the rules and logic used can accurately identify the most suitable forensic analysis method based on the given video characteristics. This process involves testing the system on various types of video data to verify that it can produce consistent and reliable recommendations. By conducting a thorough evaluation, it can be ensured that the expert system not only provides accurate results but also fits the specific context of each investigation [29].

The potential impact of using this expert system on forensic investigators is related to improved efficiency, accuracy, and decision-making support. In terms of efficiency, the expert system allows investigators to process and analyze video data faster, reducing the time needed to determine the correct analysis method [30], [31]. It is beneficial in cases that require a quick response. In terms of accuracy, using an extensive knowledge base and tested rules, this expert system reduces the likelihood of human error and improves the reliability of results [32]. The decision-making support provided by this system enables investigators to make more informed and data-driven decisions, particularly in complex and challenging situations. Overall, the integration of expert systems in video forensic investigations provides significant added value in efforts to improve the quality and effectiveness of forensic investigations.

Forward chaining accelerates forensic video investigations by systematically applying predefined rules to the input data. Unlike traditional methods that require investigators to review and select methods manually, forward chaining automates this process by matching the characteristics of the video with the appropriate forensic method. For example, when a low-resolution video is input, the system automatically applies video enhancement rules, bypassing manual decision-making steps. This results in a 30% reduction in analysis time, particularly in time-sensitive cases where prompt decisions are crucial. Additionally, forward chaining improves reliability by eliminating human bias and ensuring consistent application of rules. Each rule in the knowledge base is meticulously tested and refined, leading to more accurate method recommendations. As the rules are systematically applied to each case, investigators benefit from consistent, data-driven decision-making.

TABLE III
COMPARATIVE ANALYSIS

Aspect	Manual Selection	Forward Chaining
Average Analysis Time	45 minutes	30 minutes
Success Rate	70%	95%
Error Rate	15%	5%
Efficiency	Low	High
Accuracy	Moderate	Very High

The analysis involved 30 forensic video data divided into three categories: low-resolution videos, tampered videos, and metadata verification, with 10 videos in each category. Low-resolution videos were processed to enhance visual quality, tampered videos were analyzed to detect modifications or manipulations, and metadata verification focused on confirming details such as date, time, location, and recording device.

Table 3 demonstrates the substantial benefits of forward chaining compared to manual selection in video forensic analysis. Forward chaining necessitates an average analysis time of about 30 minutes, whereas manual selection requires 45 minutes, hence illustrating its enhanced efficiency. The success rate of forward chaining is markedly greater at 95%, whereas human selection attains just 70%, underscoring the improved reliability of automated operations. The mistake rate for forward chaining is notably low at 5%, while human selection exhibits a significantly larger error rate of 15%, highlighting the accuracy benefit of automation. In terms of efficiency, forward chaining surpasses manual selection by integrating quicker analysis with enhanced precision, hence diminishing dependence on human experience and lessening the likelihood of errors.

H. Challenge and Future Direction

Traditional forensics with AI technology and managing complex video data. Integrating AI with traditional forensic methods requires an in-depth understanding to ensure that the recommendations given by the system conform to recognized forensics standards. One of the significant challenges is to ensure that AI not only automates processes but also provides accurate and accountable results. This has become important because in digital forensics, the accuracy and reliability of results are critical [16], [33].

Additionally, managing and analyzing complex video data, such as low-quality videos or non-standard formats, introduces complexity to the development of expert systems. These diverse videos require specific and detailed rules for practical analysis. The development of these rules requires in-depth knowledge of video characteristics and how such factors affect appropriate analysis methods.

Regarding the direction of future research, several possibilities are worth exploring. First, further improvement in AI techniques used in expert systems could be a focus, enhancing AI's ability to handle various types of video data more effectively. Second, expanding expert systems to cover a wider range of diverse forensic scenarios is also essential. This could include developing more complex rules to address specific cases in video forensics, such as analyzing video that has been digitally manipulated or extracting information from low-quality videos. Third, further research may need to explore the integration of expert systems with other forensic tools to create a holistic approach to criminal investigations. This approach enables the power of AI to be exploited in data analysis while still leveraging traditional methods for other aspects of forensic investigation.

IV. Conclusion

The implementation of forward chaining techniques in expert systems for video forensic investigations significantly enhances the efficiency and accuracy of the analysis process. By automating decision-making and applying predefined rules based on video characteristics, the system ensures consistent and reliable results, reducing human error and speeding up investigations. The system's adaptability to incorporate new rules ensures it remains up to date with evolving forensic methodologies.

In the expert system, critical steps include goal setting, building a comprehensive knowledge base, developing specific rules, and applying these rules to video data. This systematic approach enables quick and accurate recommendations, aiding forensic investigators in selecting the most appropriate analysis methods for various video types and characteristics.

Evaluation of the system demonstrates its effectiveness in improving investigation efficiency, accuracy, and decision-making support. The system's ability to process video data swiftly and reliably is particularly beneficial in time-sensitive cases, reducing the likelihood of errors and enhancing the overall quality of forensic investigations.

Future research should focus on advancing AI techniques within expert systems to handle diverse video data more effectively, expanding the system to cover a broader range of forensic scenarios, and integrating expert systems with other forensic tools. This holistic approach leverages AI's strengths in data analysis while maintaining the robustness of traditional forensic methods, ultimately enhancing the capabilities and reliability of digital forensic investigations.

Acknowledgment

This research is supported by Universitas Islam Indonesia under the Department of Informatics Research Collaboration 2024, with research contract number 111/Kajur.IF/70/Jur.IF/XII/2023. The authors thank the Center for Digital Forensics Studies (PUSFID UII) for their guidance and resources during the development of this study.

References

[1] A. Al-dhaqm et al., "Digital forensics subdomains: The state of the art and future directions," *IEEE Access*, vol. 9, pp. 152476–152502, 2021, doi: 10.1109/access.2021.3124262.

[2] K. Strandberg, N. Nowdehi, and T. Olovsson, "A systematic literature review on automotive digital forensics: Challenges, technical solutions and data collection," *IEEE Trans. Intell. Veh.*, vol. 8, pp. 1350–1367, 2023, doi: 10.1109/TIV.2022.3188340.

[3] F. Casino et al., "Research trends, challenges, and emerging topics in digital forensics: A review of reviews," *IEEE Access*, vol. 10, pp. 25464–25493, 2022, doi: 10.1109/access.2022.3154059.

[4] P. Anderson, D. Sampson, and S. Gilroy, "Digital investigations: Relevance and confidence in disclosure," *ERA Forum*, vol. 22, pp. 587–599, 2021, doi: 10.1007/s12027-021-00687-1.

[5] Š. Grigaliūnas, J. Toldinas, A. Venčkauskas, and N. Morkevičius, "Digital evidence object model for situation awareness and decision making in digital forensics investigation," *IEEE Intell. Syst.*, vol. 36, no. 1, pp. 39–48, Jan./Feb. 2021, doi: 10.1109/MIS.2020.3020008.

[6] N. A. Rakha, "Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations," *Mex. Law Rev.*, vol. 16, no. 2, pp. 1–15, 2024, doi: 10.22201/iij.24485306e.2024.2.18892.

[7] T. D'Anna et al., "The chain of custody in the era of modern forensics: From the classic procedures for gathering evidence to the new challenges related to digital data," *Healthcare*, vol. 11, no. 5, 2023, doi:10.3390/healthcare11050634.

[8] O. E. M. Angel et al., "Digital evidence as a means of proof in criminal proceedings," *Russ. Law J.*, vol. 11, no. 5, 2023, doi:10.52783/rlj.v11i5s.895.

[9] A. R. Farooqi, B. Ryan, and S. Cobb, "Using expert perspectives to explore factors affecting choice of methods in safety analysis," *Saf. Sci.*, vol. 148, 2022, doi: 10.1016/j.ssci.2021.105571.

[10] N. K. Booker, P. F. Knights, J. D. Gates, and R. E. Clegg, "Applying principal component analysis (PCA) to the selection of forensic analysis methodologies," *Eng. Fail. Anal.*, vol. 125, 2021, doi:10.1016/j.engfailanal.2021.105937.

[11] T. L. Lash et al., "Bias analysis gone bad," *Amer. J. Epidemiol.*, vol. 190, no. 8, pp. 1604–1611, 2021, doi: 10.1093/aje/kwab072.

[12] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electron. Mark.*, vol. 31, no. 3, pp. 685–695, 2021, doi:10.1007/s12525-021-00475-2.

[13] R. Rawat et al., "Autonomous artificial intelligence systems for fraud detection and forensics in dark web environments," *Inform.*, vol. 46, no. 9, 2023, doi: 10.31449/inf.v46i9.4538.

[14] A. Jarrett and K. K. R. Choo, "The impact of automation and artificial intelligence on digital forensics," *Wiley Interdiscip. Rev. Forensic Sci.*, vol. 3, no. 4, 2021, doi: 10.1002/wfs2.1418.

[15] M. A. Azad et al., "DEEPSEL: A novel feature selection for early identification of malware in mobile applications," *Futur. Gener. Comput. Syst.*, vol. 129, pp. 54–63, 2022, doi:10.1016/j.future.2021.10.029.

[16] B. Fakiha, "Enhancing cyber forensics with AI and machine learning: A study on automated threat analysis and classification," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 4, pp. 701–707, 2023, doi:10.18280/ijsse.130412.

[17] A. Vasilaras, N. Papadoudis, and P. Rizomiliotis, "Artificial intelligence in mobile forensics: A survey of current status, a use case analysis and AI alignment objectives," *Forensic Sci. Int. Digit. Investig.*, vol. 48, 2024, doi:10.1016/j.fsidi.2024.301737.

[18] Z. Xiang et al., "Forensic analysis of video files using metadata," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, 2021, pp. 1042–1051, doi:10.1109/CVPRW53098.2021.00115.

[19] M. Choudhary, A. V. Ramani, and V. Bhardwaj, "The significance of metadata and video compression for investigating video files on social media forensic," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 9, no. 3, pp. 1–10, 2023, doi: 10.32628/cseit2390373.

[20] P. Sukamto et al., "Forensic digital analysis for CCTV video recording," *Int. J. Sci. Technol. Manag.*, vol. 3, no. 1, pp. 1–10, 2022, doi: 10.46729/ijstm.v3i1.460.

[21] I. M. Bagkratsas and N. Sklavos, "Digital forensics, video forgery recognition, for cybersecurity systems," in *Proc. 24th Euromicro Conf. Digit. Syst. Des. (DSD)*, 2021, pp. 510–513, doi:10.1109/DSD53832.2021.00082.

[22] W. El-Shafai et al., "A comprehensive taxonomy on multimedia video forgery detection techniques: Challenges and novel trends," *Multimedia Tools Appl.*, vol. 82, no. 18, pp. 1–67, 2023, doi:10.1007/s11042-023-15609-1.

[23] N. R. Ali and V. A. Hacimahmud, "Methodology of expert system building," *Technium: Rom. J. Appl. Sci. Technol.*, vol. 2, no. 3, pp. 140–146, 2020, doi: 10.47577/technium.v2i3.583.

[24] P. Alicia, "Sistem pakar menggunakan metode forward chaining dalam mengidentifikasi penyakit kambing," *J. Inf. dan Teknol.*, vol. 4, no. 4, pp. 7–10, 2022, doi: 10.37034/jidt.v4i4.216.

[25] E. Pawan et al., "Implementation of forward chaining method in expert system to detect diseases in corn plants in Muara Tami district," *Int. J.*

Comput. Inf. Syst., vol. 3, no. 1, pp. 27-33, 2022, doi:10.29040/ijcis.v3i1.59.

[26] N. Lorenzo-Parodi, W. Kaziur-Cegla, and T. C. Schmidt, "Automation and optimization of the sample preparation of aromatic amines for their analysis with GC-MS," *Green Anal. Chem.*, vol. 4, 2023, doi:10.1016/j.greeac.2023.100071.

[27] L. A. M. Hernández, A. L. S. Orozco, and L. J. G. Villalba, "Analysis of digital information in storage devices using supervised and unsupervised natural language processing techniques," *Future Internet*, vol. 15, no. 5, 2023, doi: 10.3390/fi15050155.

[28] A. M. Yusuf et al., "An expert system for diagnosing the impact of traffic accidents using the forward chaining method," *J. Dinda Data Sci. Inf. Technol. Data Anal.*, vol. 3, no. 1, pp. 24-30, 2023, doi:10.20895/dinda.v3i1.767.

[29] T. Bollé, E. Casey, and M. Jacquet, "The role of evaluations in reaching decisions using automated systems supporting forensic analysis," *Forensic Sci. Int. Digit. Investig.*, vol. 34, 2020, doi:10.1016/j.fsidi.2020.301016.

[30] A. R. Javed et al., "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," *IEEE Access*, vol. 10, pp. 11065-11089, 2022, doi:10.1109/access.2022.3142508.

[31] Y. Akbari et al., "Digital forensic analysis for source video identification: A survey," *Forensic Sci. Int. Digit. Investig.*, vol. 41, Jun. 2022, doi: 10.1016/j.fsidi.2022.301390.

[32] T. Sihotang, D. A. Landgrebe, and F. S. Panjaitan, "Expert system approach to improve the accuracy of prediction and solution of various agricultural scenarios," *Idea Futur. Res.*, vol. 1, no. 1, pp. 39-47, 2023, doi: 10.35335/idea.v1i1.5.

[33] Z. A. Baig et al., "Drone forensics and machine learning: Sustaining the investigation process," *Sustainability*, vol. 14, no. 8, 2022, doi:10.3390/su14084861.