JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2026, VOL 9, NO 4

A Human-AI Collaborative Framework For Forensic Video Evidence Analysis In Law Enforcement

Rohith Kannanore Natarajan

Independent Researcher USA
ORCID iD: 0009-0001-6131-3145
rohith.kannanore.natarajan@gmail.com

Abstract—The rapid growth of digital surveillance systems has led to an unprecedented increase in video data used in criminal investigations, making forensic video analysis a critical component of modern law enforcement. However, traditional manual analysis methods are time-consuming, error-prone, and inefficient when handling large-scale data. While artificial intelligence (AI) techniques such as deep learning have improved automation and detection accuracy, they often lack interpretability, contextual reasoning, and legal reliability. This paper proposes a human–AI collaborative framework for forensic video evidence analysis that integrates machine intelligence with expert validation. The framework employs Discrete Fourier Transform (DFT) for feature extraction and a Support Vector Machine (SVM) optimized using Bayesian Optimization for classification of manipulated and authentic video frames. Human-in-the-loop validation ensures improved reliability and reduces false interpretations. Experimental results demonstrate high performance, achieving 94.68% accuracy and strong precision-recall balance. The proposed approach enhances transparency, efficiency, and trustworthiness, making it highly suitable for real-world forensic applications and legal admissibility.

Keywords—Forensic Video Analysis, Human–AI Collaboration, Digital Forensics, Video Evidence Analysis, Law Enforcement.

I. INTRODUCTION

The rapid growth of crimes in the digital era has changed the terrain of law enforcement and the process of investigation dramatically. Contemporary crimes tend to be digital in nature, producing copious amounts of data that can be valuable evidence [1][2]. Consequently, the field of forensic science has emerged as an invaluable asset in investigations conducted by the criminal justice system, as it allows gathering evidence, preserving it, and analyzing it in an organized and systematic manner [3]. Digital forensics specifically is crucial in investigating computer, mobile, network, and cloud-based data to facilitate a court case and deliver justice [4].

Video evidence has become one of the biggest sources of forensic data within this field. The proliferation of surveillance technologies, such as CCTV, body-worn cameras, drones, and other systems, has led to a rise in the amount of video data available to law enforcement agencies rise exponentially [5][6]. To a large extent, these recordings are utilized to recreate the events, suspect them and confirm their investigation results. But with the increasing size and complexity of video data, the old-fashioned forensic practices become a challenge.

Traditional methods of analyzing video evidence are based on manual examination of the material, something both time-consuming and subject to human error. Most of the time, investigators are asked to watch and analyze wide-ranging footage within the rigid time limits, which causes cognitive overloading and the possibility of interpretation inconsistencies [7][8]. These constraints make the investigative procedure less efficient and reliable, especially when working on large-scale or time-consuming cases. To overcome them, artificial intelligence (AI) has been increasingly incorporated into forensic processes [9][10]. Machine learning and deep learning are AI methods where automated processes that can be

performed include detecting objects, recognition of faces, recognizing activities, and detecting anomalies [11]. These capabilities can contribute greatly to the speed, scalability and efficiency of video analysis. Although such benefits exist, it is clear that AI-only systems have a number of drawbacks, such as the inability to provide a contextual understanding, reduced explainability [12], and bias and error vulnerability, particularly when utilizing low-quality or unprocessed data [13]. The concerns presented by these issues are the credibility and legality of AI-generated results.

To address such difficulties, a human-AI joint system is suggested as a possible solution. This method is a fusion of human expertise and AI capabilities, as AI enables data processing and pattern identification, whereas human investigators can add their contextual, legal, and ethical insights. The proposed framework will reduce errors, enhance the overall reliability and transparency of forensic video analysis in law enforcement settings, and improve the quality of the results by leveraging the framework's mutual advantages.

A. Motivation and Contributions of the Study

The growing use of video evidence in criminal investigation has underscored the weaknesses of the traditional processes of forensic analysis that have been found to be largely manual, slow and have a high propensity to error. Even though AI-based solutions are automatable and can be scaled, they do not provide a contextual understanding and transparency, which casts doubts on trust and legal acceptability. It is clear that there is a dire need to have a balanced approach that incorporates both computation efficiency, and human knowledge. This research is driven by the fact that there is need to have a reliable, interpretable, and scalable forensic framework that can improve decision making and at the same time provide accuracy and accountability in law enforcement investigations. The major study contributions are as follows:

- Proposes a novel human–AI collaborative framework for forensic video evidence analysis.
- Combines DFT-based feature extraction in order to detect inconsistency of manipulated videos in the frequency domain.
- Uses SVM model whose optimization is done by Bayesian Optimization to enhance better classification.
- Uses the human-in-the-loop validation to increase reliability and minimize false positives/negatives.
- Improves legal acceptability and understandability of forensic analysis systems.

B. Justification and Novelty of the paper

This study addresses critical limitations in existing forensic video analysis methods by introducing a hybrid framework that balances automation and human expertise. Unlike purely deep learning-based approaches, the proposed method combines lightweight machine learning with frequency-domain feature extraction and human validation. The novelty lies in integrating Bayesian-optimized SVM with a human-in-the-loop mechanism, improving interpretability, efficiency, and reliability. This approach ensures practical applicability in real-world law enforcement scenarios while maintaining high accuracy and supporting legal admissibility of forensic evidence.

C. Structure of the Paper

The paper has the following structure. Section II discusses the existing literature and considers the main gaps in the research. In section III, the suggested human-AI collaborative framework and methodology are presented. Section IV explains the experiment results and performance evaluation. Lastly, Section VI summarizes the paper and provides future research directions.

II. LITERATURE REVIEW

The literature addresses deepfake video detection and forensic analysis through machine and deep learning methods, with the emphasis on the improvement of accuracy, feature mining, object detection, and the challenge of real-world problems.

Sandhya and A. Kashyap (2025) offer a novel method to deepfake video detection via the use of a DL algorithm and temporal differences in the video's statistical data at the pixel level. This study examines spatial information inside individual frames as well as temporal correlations between succeeding frames in order to identify minute aberrations characteristic of deepfake manipulations. Next, fine-tuning of InceptionResNetV2 with the addition of a dense layer is trained FaceForensics++ for

deepfake detection. The proposed fine-tuned model outperforms the existing techniques as its testing accuracy on unseen data outperforms the existing methods [14].

N. Jain et al. (2024) explore the area of deepfake detection by focusing on the application of ML methods to the analysis of audio, video, and images. The effectiveness of several machine learning models—Random Forests, Gradient Boosting Machines, Support Vector Machines, Neural Networks, and CNN, among others—in identifying deepfakes is compared and contrasted. This study provides a rundown of the pros and cons of each model, as well as performance insights based on research and real-world case studies[15].

I. Sudha et al., (2023) study looks into the use of deep neural networks to improve object detection in surveillance films for crime scene analysis. The study's findings are extensive, including detection accuracy metrics for numerous item classes such as "Person," "Vehicle," and "Suspicious Item." Precision values range from 0.78 to 0.92, recall values range from 0.82 to 0.90, and F1 scores range from 0.80 to 0.90, demonstrating the models' ability to recognize objects accurately, but with variances among item categories. Inference times for ResNet-50 and YOLOv3 are 15 ms and 20 ms, respectively, with GPU use percentages of 75% and 90% [16].

N. T. J. and K. Thinakaran (2023) introduced a deep reinforcement learning model based on Deep Q-networks (DQN) to detect the crime scene objects to improve the forensic analysis. The model is trained to recognize and categorize objects with real and synthetic data with reward mechanisms directing attention to the important aspects. According to experimental outcomes, one can improve performance compared to Faster R-CNN and YOLO using precision, recall, and F1-score [17].

X. Jin et al. (2022) proposed a video splicing detection system through a video segmentation video object modeling problem. The technique combines the EXIF-consistency prediction, region tracking and semantic segmentation to identify tampered regions. The method has an F1-score of 0.623 on GRIP dataset, which is better than the current forensic methods [18].

S. Lee et al., (2021) presented a digital forensic tool to identify various references of deepfakes video using a Transfer Learning-based Autoencoder with Residuals (TAR). The model is expected to have high accuracy and be usable in real life with minimal training data. It applies an autoencoder with residual blocks and uses a transfer learning sequence to identify different types of deepfakes. The method has better generalization results on the FaceForensics++ dataset, and 89.49% 0-shot accuracy on real-world Deepfake-in-the-Wild videos, which is 10.77% higher than the baseline models [19].

Table I contains a comparative study of the current approaches, describing their methods, results, and limitations, and defining the major gaps in research on forensic video analysis.

TABLE I. COMPARATIVE ANALYSIS OF EXISTING METHODS FOR FORENSIC VIDEO EVIDENCE ANALYSIS METHODS

References	Study On	Methods Used	Key Outcomes	Limitations	Recommendations
Sandhya and Kashyap (2025)	Deepfake video detection using temporal and spatial features	Statistical feature extraction + fine-tuned InceptionResNetV2	Achieves high detection accuracy on unseen video data	High computational complexity and dependence on deep learning; lacks interpretability	Incorporate lightweight ML models and human-in-the-loop validation for practical use
N. Jain et al. (2024)	Comparative analysis of ML models for deepfake detection (image, video, audio)	Random Forest, SVM, Gradient Boosting, Neural Networks, CNN	Provides comparative performance insights across multiple ML models	No unified or optimized framework; limited real-time applicability	Develop integrated frameworks combining efficiency and accuracy

I. Sudha et al. (2023)	Object detection in surveillance videos for crime scene analysis	Deep neural networks (ResNet-50, YOLOv3)	Good detection performance (Precision: 0.78–0.92, F1-score: 0.80–0.90)	Performance varies across object categories; high GPU usage	Improve model consistency and reduce computational cost
N. T. J and Thinakaran (2023)	Crime scene object detection using reinforcement learning	Deep Q-Network (DQN) with reward-based learning	Outperforms Faster R-CNN and YOLO in object detection tasks	High training complexity and reliance on large datasets	Combine reinforcement learning with supervised ML and expert feedback
X. Jin et al. (2022)	Video splicing and tampering detection	EXIF consistency, region tracking, semantic segmentation	Achieves F1-score of 0.623 on GRIP dataset	Moderate detection accuracy and complex multi-stage pipeline	Improve accuracy using optimized feature extraction and simpler models
S. Lee et al. (2021)	Deepfake video detection with limited data	Transfer Learning-based Autoencoder with Residuals (TAR)	Achieves 89.49% zero-shot accuracy on real-world videos	Requires deep learning resources and lacks explainability	Enhance interpretability and reduce model complexity for real-world deployment

A. Critical Gaps in Existing Research

Current literature mainly uses deep learning models, which are both highly accurate, but also consume high computational resources and are not interpretable. Most methods mainly deal with spatial or temporal characteristics, but not both. Also, the majority of models are tested in controlled settings, which restricts their real-world applicability. They also lack frameworks that integrate human knowledge to validate and make decisions. In addition, conventional machine learning is investigated less effectively despite efficiency. Thus, a collaborative framework between humans and AI that is accurate, efficient, interpretable, and practically applicable to forensic video evidence analysis is necessary.

III. METHODOLOGY

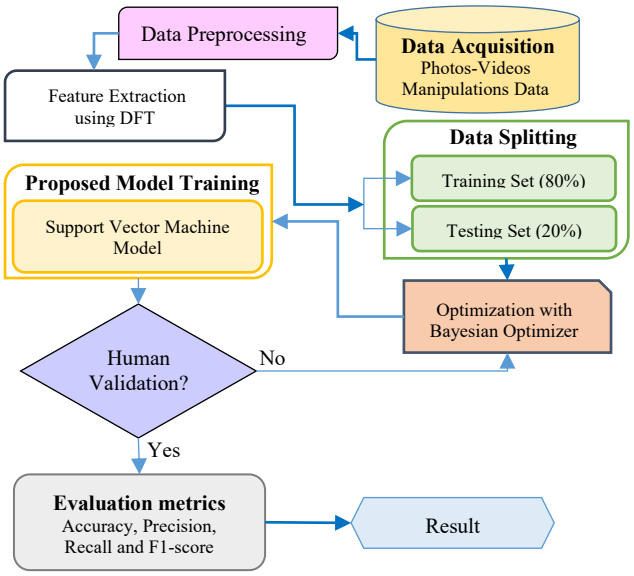

Fig. 1. Proposed Human-AI Collaborative Framework for Forensic Video Evidence Analysis

The suggested methodology suggests an organized human-AI collaborative system of forensic video evidence processing illustrated in Figure. 1. The first step is the data collection where the Photos-Videos Manipulations dataset will be gathered which comprises of real and manipulated video data. This is preceded by data preprocessing to clean and prepare the data to be analyzed further. This is followed by the extraction of features with the help of Discrete Fourier Transform (DFT) that transforms video frames to the frequency domain and extracts components of the image that are used to detect anomalies. The resulting processed data is then split into training (80%) and testing (20%) sets to provide appropriate model testing. The proposed model training step involves the use of Support Vector Machine (SVM) to identify video frames as either real or manipulated. Bayesian Optimization is used to ensure that hyperparameters are efficiently tuned to improve the performance of the model. The framework also involves a human validation process, which involves the experts reviewing the predictions of the model to verify the model results and minimize errors. Lastly, the system compares performance with accuracy, precision, recall, and F1-score and generates the final results.

A. Data Collection

The Saraferreirascf/Photos-Videos Manipulations Dataset 1 is a publicly available benchmark of multimedia forensic studies, which comprises 40,588 images and 12,400 video frames taken out of real and manipulated videos. In this study, the video portion, consisting of 12,400 frames, has been used to train and test ML models for detecting tampered videos. The data will include authentic (real) and fake (manipulated) videos, with a variety of scenes, lighting, and types of manipulation.

B. Data Preprocessing

Pre-process of data is a critical process in the process of preparing data to be utilized in the machine learning algorithms, which involves cleaning and converting data into numerical form. This is done by the following steps:

C. Feature Extraction Using DFT

The Discrete Fourier Transform (DFT) based method "Unmasking Deepfake using Simple Features" is used to extract features. In this stage, each video frame is transformed into the frequency domain rather than the spatial domain to enable processing of underlying frequency patterns that are not readily apparent in raw pixel data. DFT breaks the frame down into sine and cosine components, which contain high- and low-frequency information, respectively. Distorted videos tend to cause anomalies in such frequency distributions, which can be easily identified using this method. A total of 50 frequency-based features are derived from the transformed data per frame, yielding an information-rich, compact representation for machine learning models.

D. Data Splitting

In this analysis, the data is subdivided into two with an 80:20 ratio. 80% of the data is utilized in order to train the model, whereas the other 20% is set aside to test the model's performance.

E. Optimization with Bayesian Optimizer

The processing step uses the Bayesian Optimization technique to find the minimum or maximum of a noisy black-box function. This approach uses an acquisition function to determine the next best query point and depends on Bayes' theorem to update a prior distribution on the objective function sequentially.

Bayesian Optimization is notably useful for selecting the best hyperparameters to utilize in improving the performance of ML models. The foundation of this method is a probabilistic model that finds optimum solutions by approximating the goal function and an acquisition function. A widely applied formulation is a maximization of the objective, which is formulated in Equation (1):

$$X^* = arg\max_{x \in X} f(x) \qquad \square\square\square$$

In which, X is the search space, arg max is the value of the input that maximizes the function, and X^* is the optimal solution to this global maximum.

3 We combined whole (8) MachineLearningCSVs data of the
4 CICIDS-2017 to make a dataset. After combining we ob-
5 tained 79 columns as features and 2,830,743 rows as instances
6 of traffic as present in Table 1

[1]https://github.com/saraferreirascf/Photos-Videos-Manipulations-Dataset

7 We combined whole (8) MachineLearningCSVs data of the
8 CICIDS-2017 to make a dataset. After combining we ob-
9 tained 79 columns as features and 2,830,743 rows as instances
10 of traffic as present in the T

F. Implementation of Support Vector Machine

The state-of-the-art in classification and regression performance may be found in the family of Supervised Learning algorithms known as SVM. SVM is a well-liked technique that finds extensive use in many domains, including image processing. SVMs search a high-dimensional feature space for the optimal hyperplane that maximally separates the two classes [20]. The primary equation for determining the best hyperplane in linearSVM is given by Equation (2):

$$f(X, w, b) = sign(wx + b) \quad \square\square\square$$

The direction of the input vector x is represented by the weight w; b is bias, which reflects the distance from the origin and x is an Input Vector. Furthermore, class A is specified if wx + b > 0; class B is specified if wx + b < 0; and the hyperplane is specified if wx+b=0. Equation (3) defines the margin band, which is the space between hyperplanes.

$$\gamma = \frac{2}{||w||} \quad \square\square\square$$

where w denotes 2-norm of w.

G. Human-in-the-Loop Validation

The machine learning models produce outputs that are validated and interpreted by human experts. Although the optimized model automatically identifies suspicious video frames, analysts will go through the results of the optimized model to identify authenticity and minimize errors. Model performance can also be improved based on their feedback, resulting in more accurate and reliable forensic video analysis.

H. Evaluation Metrics

This section presents metrics that are used to evaluate the effectiveness of the proposed approach. Based on these values, among the key performance measures are Accuracy which is the ratio of correct predictions to the total cases. The precision of positive forecasts is a measure of their accuracy. Recall assesses how well the model can find every relevant example. F1 Score is especially applicable when there is class imbalance because it accounts for both FP and FN. The Mathematical computation is shown in Equations (4) to (7).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad \square\square\square$$

$$Precision = \frac{TP}{TP+FP} \quad \square\square\square$$

$$Recall = \frac{TP}{TP+FN} \quad \square\square\square$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad \square\square\square$$

where:

- **TP (True Positive):** The model correctly identifies a manipulated (fake) video frame as manipulated.
- **TN (True Negative):** The model correctly identifies a genuine (real) video frame as genuine.
- **FP (False Positive):** The model incorrectly classifies a genuine (real) video frame as manipulated.
- **FN (False Negative):** The model incorrectly classifies a manipulated (fake) video frame as genuine.

IV. Result Analysis & Discussion

Experiments are conducted on a system with a multi-core processor, 8–16 GB RAM, and optional GPU support. Implementation uses Python with NumPy, Pandas, OpenCV, and Scikit-learn in Jupyter Notebook. Table II displays the metrics for the performance of the SVM model that was tuned for video forgery detection using Bayesian Optimization. The model achieves an accuracy of 94.68%, prec of 97.61%, rec of 92.2%, and an F1score of 94.83%, demonstrating effective classification of real and manipulated video frames.

TABLE II. PERFORMANCE METRICS OF SVM WITH BAYESIAN OPTIMIZATION FOR FORENSIC VIDEO CLASSIFICATION

Metric	SVM and Bayesian Optimizer
Accuracy	94.68
Precision	97.61
Recall	92.2
F1-Score	94.83

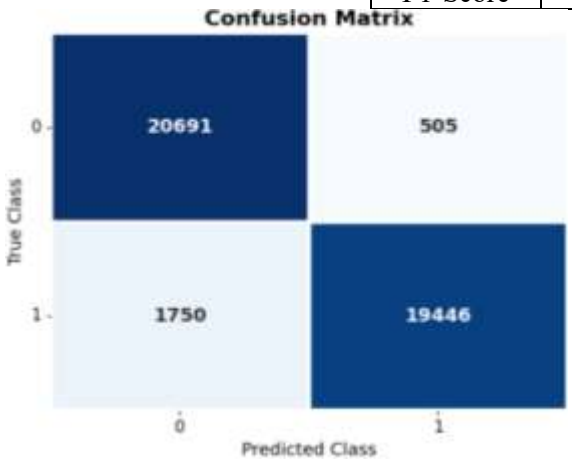

Fig. 2. Confusion Matrix of Bayesian-Optimized Support Vector Machine (SVM) Model

The Confusion Matrix shows the results of the Bayesian-optimized SVM model classification in comparison with the predicted and actual class labels in the Figure. 2. It gives the actual positives, actual negatives, misclassification, and misclassification by class, which gives an understanding of the accuracy of the model as well as the misclassification and the performance of the model per class. The analysis is essential to ensuring reliability in the analysis of forensic video evidence as part of a human-AI collaborative structure in law enforcement.

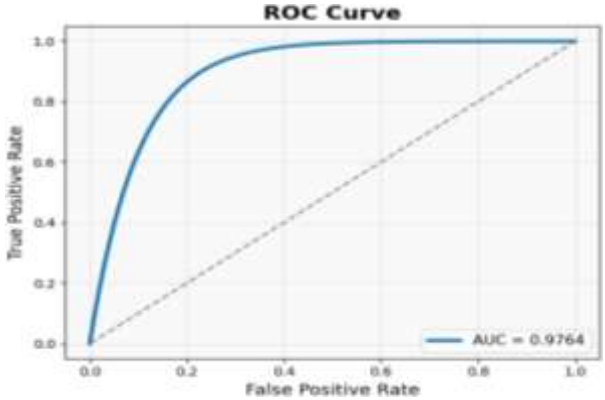

Fig. 3. Receiver Operating Characteristic (ROC) Curve of Bayesian-Optimized Support Vector Machine (SVM) Model

Figure 3 illustrates the Recurve, which compares the TPR with the FPR, to demonstrate the performance of the Bayesian-optimized SVM model at various classification thresholds. The AUC ≈ 0.9764 is strong evidence of good discriminating power. This shows that the model has been effective in classifying classes, thereby enabling sound decision-making in forensic video evidence analysis systems.

A. Comparative Analysis

The comparison shows the performance analysis of the proposed SVM model with Bayesian Optimization with the current models, such as YIX, KNN, and CNN models. The proposed approach has the highest accuracy of 94.68%, which is far higher than the current techniques. This shows that it is better in predictive ability and strength, and thus indicates efficiency when it comes to working with human-AI collaborative framework when analyzing video evidence reliably.

The comparison Table III presents the performance evaluation of the proposed SVM model integrated with Bayesian Optimization against existing approaches, including YIX, KNN, and CNN models. The proposed method achieves the highest accuracy of 94.68%, significantly outperforming the existing

techniques. This demonstrates its superior predictive capability and robustness, highlighting its effectiveness for reliable forensic video evidence analysis within a human–AI collaborative framework.

TABLE III. PERFORMANCE COMPARISON OF PROPOSED BAYESIAN-OPTIMIZED SVM MODEL WITH EXISTING APPROACHES

Reference	Models	Accuracy
Proposed	SVM and Bayesian Optimizer	94.68
[21]	YIX	90.73
[22]	KNN	81
[23]	CNN	83.87

B. Discussion

The experimental findings indicate that the proposed framework can balance accuracy, efficiency, and interpretability in video analysis for forensics. Combining DFT-based feature extraction used with Bayesian-optimized SVM helps a lot in improving the performance of detection at minimal cost. The proposed approach consumes fewer resources than deep learning models while maintaining accuracy. Human validation contributes to reliability by reducing false classifications and ensuring accurate interpretation of context. Nevertheless, performance can decrease when manipulations are very complex or the video quality is very low. Overall, the framework offers a feasible and scalable way to apply in real-world forensic settings, especially in law enforcement, which needs fast, accurate decision-making.

V. CONCLUSION & FUTURE WORK

An AI-human collaborative system of forensic video evidence analysis is proposed to overcome the main issues of scalability, accuracy, and interpretability of contemporary law enforcement investigations. The method combines the Discrete Fourier transform-based feature extraction with a Support Vector Machine that is optimized using a Bayesian approach to provide a high classification rate with low computational cost. Human-in-the-loop validation is an enhancement of reliability where the error is minimized and decisions made are contextually and legally correct. The results from the experiments are highly effective, with an accuracy of 94.68%, compared to some current methods. Nonetheless, one should take into account some limitations, such as sensitivity to sophisticated manipulation methods and dependence on high-quality input video data. The future studies will be directed to the improvement of the framework by hybrid models that utilize both ML and DL techniques. Additional enhancements will include real-time processing and adaptive learning mechanisms to increase scalability. Transparency and trust are expected to be enhanced by these advances in the usage of explainable AI approaches. Its efficacy and use in criminal investigations may be further enhanced by expanding datasets and evaluating the model across various real-world applications.

REFERENCES

[1] T. Holt and D. S. Dolliver, “Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes,” Forensic Sci. Int. Digit. Investig., vol. 37, p. 301167, Jun. 2021, doi: 10.1016/j.fsidi.2021.301167.

[2] S. Belshaw and B. Nodeland, “Digital evidence experts in the law enforcement community: understanding the use of forensics examiners by police agencies,” Secur. J., vol. 35, no. 1, pp. 248–262, 2022.

[3] Y. Fayyaz, A. Almehmadi, and K. El-Khatib, “A hybrid artificial intelligence framework for enhancing digital forensic investigations of infotainment systems,” Forensic Sci. Int. Digit. Investig., vol. 49, p. 301751, Jun. 2024, doi: 10.1016/j.fsidi.2024.301751.

[4] D. Quick and K.-K. R. Choo, “Big forensic data reduction: digital forensic images and electronic evidence,” Cluster Comput., vol. 19, no. 2, pp. 723–740, Jun. 2016, doi: 10.1007/s10586-016-0553-1.

[5] R. V Mante and R. Khan, “A Survey on Video-based Evidence Analysis and Digital Forensic,” in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), IEEE, Mar. 2020, pp. 118–121. doi: 10.1109/ICCMC48092.2020.ICCMC-00024.

[6] A. Axenopoulos, V. Eiselein, A. Penta, E. Koblents, E. La Mattina, and P. Daras, “A Framework for Large-Scale Analysis of Video \"in the Wild\" to Assist Digital Forensic Examination,” IEEE

Secur. Priv., vol. 17, no. 1, pp. 23–33, Jan. 2019, doi: 10.1109/MSEC.2018.2875851.
[7] R. Mandayam, "The Impact of Artificial Intelligence on Digital Forensic," J. Artif. Intell. Cloud Comput., vol. 3, no. 6, pp. 1–4, 2024.
[8] S. K. Chintagunta, "Generative AI Approaches to Automated Unit Test Case Generation in Large-Scale Software Projects," ESP J. Eng. Technol. Adv., vol. 4, no. 1, pp. 150–157, 2024, doi: 10.56472/25832646/JETA-V4I1P121.
[9] N. Kolli, J. W. Sajja, and A. Nerella, "Building Secure AI Agents for Autonomous Data Access in Compliance/Regulatory-Critical Environments," Comput. Fraud Secur., vol. 2024, no. 9, pp. 363–373, Sep. 2024, doi: 10.52710/cfs. 746.
[10] E. Nissan, "Legal evidence, police intelligence, crime analysis or detection, forensic testing, and argumentation: an overview of computer tools or techniques," Int. J. Law Inf. Technol., vol. 17, no. 1, pp. 1–82, 2009.
[11] S. Singamsetty, "AI-Based Data Governance: Empowering Trust and Compliance in Complex Data Ecosystems," Int. J. Comput. Math. Ideas, vol. 13, no. 03, pp. 1007–1017, 2021, doi: 10.70153/IJCMI/2021.13301.
[12] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), IEEE, 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.
[13] L. J. García Villalba, A. L. Sandoval Orozco, R. Ramos López, and J. Hernandez Castro, "Identification of smartphone brand and model via forensic video analysis," Expert Syst. Appl., vol. 55, pp. 59–69, Aug. 2016, doi: 10.1016/j.eswa.2016.01.025.
[14] Sandhya and A. Kashyap, "A statistical analysis for deepfake videos forgery traces recognition followed by a fine-tuned InceptionResNetV2 detection technique," J. Forensic Sci., vol. 70, no. 1, pp. 349–368, Jan. 2025, doi: 10.1111/1556-4029.15665.
[15] N. Jain, S. Borade, B. Patel, V. Kumar, and M. Godhrawala, "Detecting Deepfakes: Exploring Machine Learning Models for Audio, Video, and Image Analysis," Int. J. ofINTELLIGENT Syst. Appl. Eng., vol. 12, no. 4, pp. 481–487, 2024.
[16] I. Sudha, G. Kirubasri, M. Deivakani, V. P. Singh, T. R. Kumar, and M. Niranjanamurthy, "Detecting Objects in Surveillance Videos with Deep Neural Networks for Crime Scene Analysis," in 2023 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI), IEEE, Dec. 2023, pp. 1–4. doi: 10.1109/ICDSAAI59313.2023.10452608.
[17] N. T. J. and K. Thinakaran, "An Enhanced Forensic Analysis and Security Surveillance Using Deep Reinforcement Learning," in 2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon), IEEE, Aug. 2023, pp. 361–365. doi: 10.1109/SmartTechCon57526.2023.10391428.
[18] X. Jin, Z. He, J. Xu, Y. Wang, and Y. Su, "Video splicing detection and localization based on multi-level deep feature fusion and reinforcement learning," Multimed. Tools Appl., vol. 81, no. 28, pp. 40993–41011, Nov. 2022, doi: 10.1007/s11042-022-13001-z.
[19] S. Lee, S. Tariq, J. Kim, and S. S. Woo, "TAR: Generalized Forensic Framework to Detect Deepfakes using Weakly Supervised Learning," 2021. doi: 10.48550/arXiv.2105.06117.
[20] D. Ghimire, S. Jeong, J. Lee, and S. H. Park, "Facial expression recognition based on local region specific features and support vector machines," Multimed. Tools Appl., vol. 76, no. 6, pp. 7803–7821, Mar. 2017, doi: 10.1007/s11042-016-3418-y.
[21] A. Ismail, M. Elpeltagy, M. S. Zaki, and K. Eldahshan, "A New Deep Learning-Based Methodology for Video Deepfake Detection Using XGBoost," Sensors, vol. 21, no. 16, p. 5413, Aug. 2021, doi: 10.3390/s21165413.
[22] F. K. H. Mihna, M. A. Habeeb, Y. L. Khaleel, Y. H. Ali, and L. A. E. Al-saeedi, "Using Information Technology for Comprehensive Analysis and Prediction in Forensic Evidence," Mesopotamian J. CyberSecurity, vol. 4, no. 1, pp. 4–16, Mar. 2024, doi: 10.58496/MJCS/2024/002.
[23] S. Ferreira, M. Antunes, and M. E. Correia, "Exposing Manipulated Photos and Videos in Digital Forensics Analysis," J. Imaging, vol. 7, no. 7, p. 102, Jun. 2021, doi: 10.3390/jimaging7070102.