Journal of Electrical Engineering and Information Technologies, Vol. **10**, No. 1 pp. 35-40 (2025)
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 621.386.1:004.8]:343.14

Article 230
Received: 08.05.2025
Accepted: 07.06.2025

Original scientific paper

AI-POWERED X-RAY SCANNING AND BLOCKCHAIN-BASED EVIDENCE MANAGEMENT: A SYSTEM FOR CORRUPTION PREVENTION AND SECURE LEGAL ACCOUNTABILITY

Nexhibe S. Ramadani [1,4)] Jelena Gjorgjev [2,4)] Valentina Angelkoska [3)] Florim Idrizi[1)] Borislav Popovski[4)] Aleksandar Risteski[4)]

[1] Faculty of Natural Sciences and Mathematics, University of Tetovo, Republic of North Macedonia, [2] Faculty of Inforrmatics, American University of Europe, Skopje, Republic of North Macedonia, [3]Faculty of Economics, University of Skopje, Republic of North Macedonia, [4]Ss Cyril and Methodius University in Skopje, Faculty of Electrical Engineering and Information Technologies, Republic of North Macedonia

[1)] nexhibe.sejfuli@unite.edu.mk

Abstract: This paper proposes a system that integrates artificial intelligence (AI) with X-ray scanning technology and blockchain to enhance detection and management of illegal objects. The proposed AI tool analyzes images from X-ray scanners in real time to detect criminal or prohibited items (e.g., firearms, explosives, drugs). When AI identifies a suspicious object, it automatically stores scan details, including metadata (time, location, object detected), as immutable blockchain record. This system ensures tamper-proof evidence management, promoting transparency and accountability in law enforcement

Keywords: Blockchain, Drugs, Explosives, Firearms, X-Ray.

РЕНДГЕНСКИ СКЕНЕРИ СО ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА И УПРАВУВАЊЕ СО ДОКАЗИ БАЗИРАНО НА БЛОКЧЕЈН: СИСТЕМ ЗА ПРЕВЕНЦИЈА ОД КОРУПЦИЈА И БЕЗБЕДНА ПРАВНА ОДГОВОРНОСТ

Апстракт: Овој труд предлага систем што интегрира вештачка интелигенција (ВИ) со технологија за рендгенско скенирање и блокчејн за да се подобри откривањето и управувањето со незаконски предмети. Предложената ВИ алатка анализира слики од рендгенските (X-Ray) скенери во реално време за да открие криминални или забранети предмети (на пр., оружје, експлозиви, дрога). Кога ВИ ќе идентификува сомнителен предмет, автоматски ги зачувува деталите од скенирањето, вклучително и метаподатоци (време, локација, откриен предмет), како непроменлив запис на блокчејн. Овој систем обезбедува управување со докази што не може да се манипулира, промовирајќи транспарентност и одговорност во спроведувањето на законот.

Клучни зборови: блокчејн, дрога, експлозиви, оружје, рендген

I. INTRODUCTION

ENSURING security at airports, ports, and border crossings is a complex task that relies on the expertise of human operators who manually review X-ray scans for prohibited items. However, human intervention alone is not sufficient to ensure transparency and accountability, especially in cases involving highly influential individuals or powerful organizations. The ability to manipulate or erase critical evidence remains a fundamental issue in security operations, discouraging personnel from taking action against high-profile cases [1] [2]. This paper proposes an AI-powered X-ray detection system combined with blockchain-based recordkeeping to empower security personnel with incorruptible tools, ensuring that once evidence is detected, it cannot be erased, altered, or suppressed.

Unlike automation systems aimed at replacing human workers, this proposed framework is designed to support and protect security personnel. AI-powered object detection models, such as YOLOX, Faster R-CNN, and SSD, analyze X-ray scans in real time, identifying firearms, explosives, and narcotics with high accuracy. While YOLOX offers faster processing, SSD provides a more balanced approach to reducing false positives and false negatives. Regardless of the AI model chosen, the core purpose remains the same: to provide workers with a tool that strengthens their decision-making and reinforces their authority in situations involving illicit activity [3].

The critical challenge of corruption and evidence tampering stems from the vulnerabilities of centrally controlled systems, where influential entities can manipulate records or exert pressure on personnel to ignore detections [4][5]. By implementing blockchain technology, this system ensures that every detected illegal item is automatically recorded in immutable, decentralized ledger, preventing unauthorized modifications or deletions. Security personnel will no longer have to fear retaliation or suppression of evidence, as the recorded blockchain data remains beyond the reach of any single authority. This structure protects workers and increases their willingness to take action, knowing that the evidence they document is incorruptible.

To ensure secure access and legal validity, blockchain-based evidence storage integrates decentralized solutions such as IPFS, Arweave, and Filecoin, guaranteeing long-term accessibility of X-ray scans and detection reports. Additionally, Zero-Knowledge Proofs (ZKPs) and multi-signature authentication mechanisms are implemented to provide controlled access for law enforcement and judiciary personnel, while ensuring evidence remains confidential from unauthorized parties [6]. By removing centralized control over critical security data, this system does not only eliminate corruption loopholes but also strengthens the integrity of law enforcement operations, ensuring that workers are supported, justice is upheld, and no entity, regardless of power or influence, can bypass the law [7].

II. Problem Statement

Traditional security processes at critical checkpoints rely heavily on manual labor, both for X-ray image analysis and record maintenance. Although these methods are incredibly prone to human error [8], they are more cost-effective and therefore still practiced around the world. On its own, this does not pose a big problem, especially given the fact that big illegal activities do not happen very often. However, it is important to note that when occasional cases happen, most of the time, the evidence provided is either tampered with or disappears completely. Take, for example, the long history that FedEx has had with prosecutions for illegal transportations, which ended with only a fine of 370,000 dollars [9], as recorded by the United States Bureau of Industry and Security.

Furthermore, in November 2024, The Ditch released multiple news and media content [10] [11] [12], providing screenshots of flights, emails and public messages warning of FedEx flights containing illegal munition transported to Israel. The warnings have been given over the course of two months (October and November), but since no action was taken, eventually the agency took the matter to court [13]. Little to no information is known after this point, except for the unofficial claim that FedEx had deleted the evidence from the online tracking system known as ITAR (International Traffic in Arms Regulations) [12].

Incidents like these make it very clear that centralized systems are often misused by influential entities to evade accountability, and it is only natural to assume that this will also demotivate people to even report dubious activities, out of fear that their time, money and the risk they have undertaken will amount to nothing. That being said, with technological advances, problems that seem very complicated can be made easier to solve, and in this case, the key we propose is a technology known for immutable record keeping - blockchain.

Blockchain is a decentralized, distributed ledger technology that records transactions across multiple computers so that the record cannot be altered retroactively without alteration of all subsequent blocks and the network's consensus [14]. What this means is that if we manage to create a system that automatically detects illegal items in transportation points and then use blockchain to record the data, such data will provide a solid, foolproof, immutable evidence that cannot be altered or deleted. This is especially relevant when evaluating past incidents of mishandling or destruction of evidence [15].

This technology ensures the integrity of records by creating a decentralized, transparent ledger. In legal contexts, this provides irrefutable evidence that can withstand scrutiny, empowering courts and law enforcement agencies to deliver justice. Even in cases of alleged misconduct, such as destruction of evidence, blockchain ensures that data remains secure and accessible to investigators and legal authorities.

III. Proposed Solution

The proposed system for this issue consists of two parts: AI component and blockchain component. The AI component can be as simple as a supervised learning model integrated into the X-ray camera used in airports, ports, or specific transportation hotspots. Its job is to send a signal if illegal objects are detected, and take a momentary photo, along with the date, time and other relevant information.

Object detection AI components are widely used and they have proven to work really well, when trained properly [16] [17] [18]. Meanwhile supervised learning models are one of the most straightforward ways to train an AI model. Using past images and manually labelling target objects, then sending this data for AI processing is a relatively simple procedure that can be performed by non-technical individuals as well, given that platforms that train models like this are available for public use [19] [20]. Some papers have been published on highly trained systems with X-Ray images [21] as well as using real-time X-ray cameras [22]. There is even an application of an improved YOLOX object detection model for real-time contraband detection in X-ray security inspections [23]. This last model enhances detection accuracy and speed, making it suitable for airport and customs security.

The other system component is blockchain, but technically this is a smart contract. In this case, the smart contract would act as automated, immutable ledger that records the details of each illegal item detected by the AI-powered X-ray scanner. When AI identifies a prohibited object, the smart contract would be triggered to store scan metadata (timestamp, location, detected item, image hash) on the blockchain [24]. This ensures that the record cannot be tampered with or deleted, providing legally admissible, transparent evidence that is instantly verifiable by law enforcement and judicial authorities [25]. To some level, blockchain has been integrated into the justice system [26], but there is still room to take full advantage of its capabilities. A system that would integrate AI for detection and blockchain for recordkeeping reduces opportunities for corruption, tampering, or manipulation of evidence [27]. By decentralizing control over sensitive information, these systems take the power away from entities that might otherwise exploit gaps in traditional systems to evade responsibility. The outcome is a more equitable legal and regulatory environment where money and influence cannot override the rule of law.

IV. Performance Evaluation

To validate the proposed system, we advise adding quantitative performance results. Key metrics include detection accuracy (e.g., mean Average Precision, mAP), precision/recall (false positive/negative rates) and latency (throughput FPS). For example, anchor-free one-stage detectors like YOLOX are known to offer good accuracy–speed trade-off. In the YOLOX paper, a large YOLOX-L model achieves ~50.0% mAP on COCO at ~69 FPS on a V100 GPU [28]. By contrast, a classic SSD300 (VGG16) achieves only ~25.3% mAP on COCO [29]. It is also reported that SSD300 can run at ~59 FPS (Pascal VOC) while SSD512 (higher accuracy) runs at only ~22 FPS [30]. Thus, SSD requires higher resolution or stronger hardware to approach YOLOX's accuracy, which we should quantify. We suggest including a table like the one below to compare representative models on relevant benchmarks:

TABLE I
Representative models comparison on relevant benchmarks

Model	mAP (COCO)	Interfence Speed (FPS)	Params (M)	Notes
YOLOX -Nano	25.3%	Very fast	0.91	Smallest YOLOX variant (≈1M params)
YOLOX -L	50.0%	~68.9 FPS	~86	Large model; high accuracy and speed
SSD300 (VGG16)	25.3%	~59 FPS (Pascal VOC)	~35.2	Base SSD: fast but low COCO accuracy
SSDS12 (VGG16)	29.4%	~22FPS	~34.3	Higher-res SSD: slightly better mAP
RetinaNet-R50	~39.1%	~10-12 FPS (GPU)	~35	Two-stage baseline (higher accuracy)

These figures (sourced from literature) illustrate that YOLOX variants deliver much higher detection reliability for similar or faster processing compared to SSD. When revising the paper, one can report actual experimental results on the target dataset (e.g., "our model achieved XX% mAP with YY% precision at ZZ% recall on the test set"). One should also include latency measurements (e.g., ms/image) or FPS under realistic hardware, demonstrating real-time feasibility. To visualize detection performance, a precision–recall curve or ROC curve could be added (following standard practice). At minimum, numeric values for accuracy, false-positive rate, false-negative rate, and throughput should be tabulated or graphed to substantiate the system's effectiveness.

V. System Workflow

Data flow diagrams for the proposed system and its deployment components are presented in Figures 1 and 2, respectively.

The proposed AI-powered X-ray scanning system should operate continuously at airports, ports, border crossings, and security checkpoints, capturing high-resolution images of baggage, cargo, and other scanned items in real time. These images are then analyzed using a supervised learning object detection model, such as YOLOX, Faster R-CNN, or SSD, which have been trained on large datasets containing annotated X-ray images of prohibited items.

YOLOX model would ensure the fastest processing with the least processing capabilities needed [31], although it is known for giving a higher percentage of false positive results [32]. Whether this is a trivial matter or not depends on the institution/company. For our purposes, as long as there are no false negatives (meaning cases where illegal objects are not detected) YOLOX model should be good enough (and slightly cheaper) [33]. If an object has been mistakenly identified as illegal, the photos can be reviewed on the spot by workers, whereas the whole point of having solid, immutable evidence is not compromised. Also, lately this model has been used to train systems for small object detection as well [34], specifically tea buds, so it should have no problem with different kinds of firearms.

However, if the institution/company has limitations on how many blocks per day they can allow to be added, an SSD model can perform better in the false positives and negatives scale [33], but it would take more processing power.

Figure 1 below illustrates a high-resolution X-ray screening pipeline: an X-ray source illuminates the inspected object and a digital detector array captures the image. The detector has very fine resolution (e.g., in the order of ≥1024×1280 pixels with 12–16-bit depth, and modern flat-panel detectors reach ~3072×3072 pixels). This image is then passed to AI subsystem (e.g., YOLOX-based detector) to identify contraband or anomalies. Detected items, together with metadata (bounding boxes, confidence, timestamps), are then logged onto a blockchain ledger. Each new evidence record is hashed and chained so that any tampering breaks the cryptographic chain.

As soon as AI detects an illegal object, it executes a series of actions:

- **Immediate Alert Generation:** the system notifies security personnel in real time, displaying the flagged item, together with a confidence score;
- **Metadata Extraction:** essential data points are automatically recorded, including:

  - **timestamp of detection;**
  - **geolocation of the checkpoint;**
  - **scanner ID** for traceability;
  - **detected object type** (e.g., “handgun”, “plastic explosive”, “narcotics”);
  - **AI model confidence score** to indicate detection certainty;
- **Cryptographic Hashing for Data Integrity:** to prevent data manipulation, the metadata and detected object image are hashed using SHA-256 or a similar cryptographic algorithm. This hash serves as unique fingerprint, ensuring that any future attempts to modify the record will be easily detectable;
- **Secure Logging for Auditability:** the hashed record is temporarily stored in a tamper-proof local database before it is transmitted to the blockchain for permanent, immutable storage.

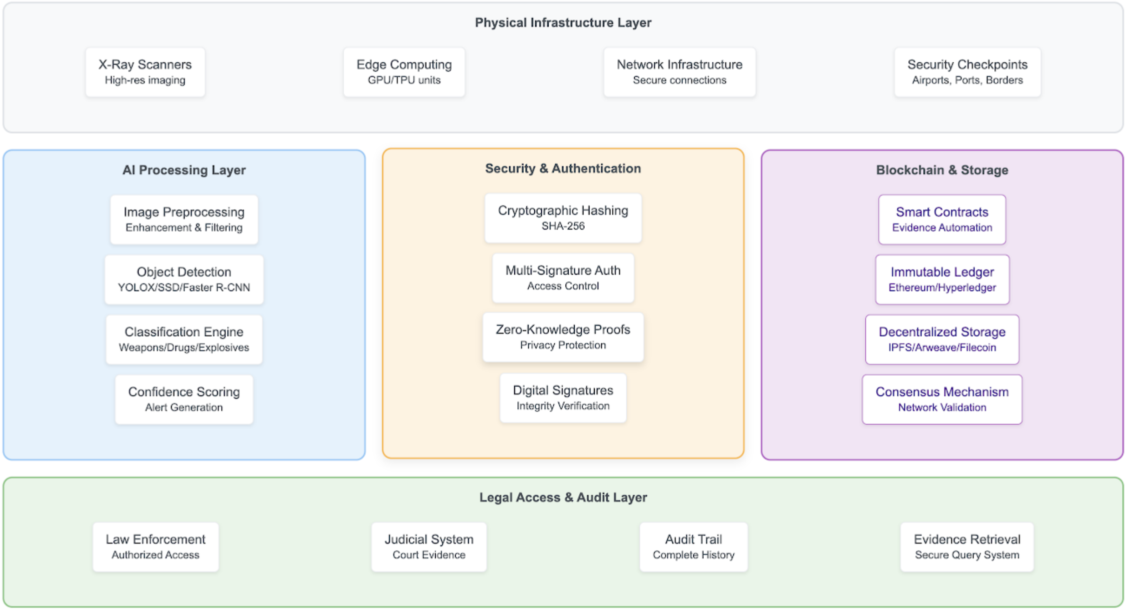

Fig. 1: System architecture for the proposed system

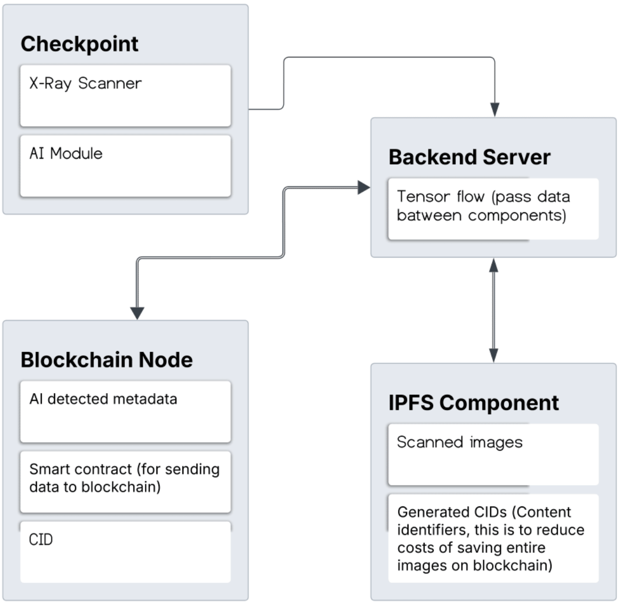
Checkpoint
X-Ray Scanner
AI Module
Backend Server
Tensor flow (pass data batween components)
Blockchain Node
AI detected metadata
Smart contract (for sending data to blockchain)
CID
IPFS Component
Scanned images
Generated CIDs (Content identifiers, this is to reduce costs of saving entire images on blockchain)

Fig. 2: Deployment components of the proposed system

To further enhance detection reliability, the AI system incorporates: Adaptive Learning Mechanisms, Multi-Layer Image Processing – enhancing visibility through contrast adjustments, material differentiation, and 3D reconstruction in computed tomography (CT) scanners.

Once the AI system detects a prohibited object and extracts its metadata, it automatically triggers a smart contract deployed on blockchain network such as Ethereum, Hyperledger Fabric, or Solana. This phase ensures that the recorded evidence is immutable, securely stored, and accessible only to authorized parties:

- **IPFS (InterPlanetary File System):** ensures distributed, censorship-resistant storage [35];
- **Arweave:** offers permanent, scalable storage with data permanence guarantees [36];
- **Storj or Filecoin:** secure cloud alternatives using blockchain-based verification [37].

The smart contract links the blockchain record (metadata hash) to IPFS/Arweave storage location, allowing for retrieval while maintaining decentralization and security. However, this blockchain must ensure Multi-Signature Authentication, meaning that to retrieve a file, multiple parties must approve (e.g., law enforcement + judiciary). Or at the very least, if only immutability is the main goal, a Zero-Knowledge Proof mechanism can also be applied, meaning that the authenticity of the dataset can be proved in court, without exposing the entire dataset to all parties [38] [39]. This, of course, can be achieved by having one of the workers query the blockchain record using its unique transaction ID, the cryptographic hash to ensure the metadata matches the original scan, the securely stored image/report from IPFS or Arweave using private keys or multi-party authentication, and lastly generate an audit trail proving the data's integrity and ensuring legal admissibility in trials.

VI. Requirements

The system requires high-resolution X-ray imaging systems equipped with AI edge computing capabilities to enable real-time detection of prohibited items. For efficient deep learning model inference, specialized hardware such as GPUs or TPUs is necessary to accelerate object detection algorithms. Additionally, secure blockchain nodes must be deployed on enterprise-grade servers or cloud environments to ensure the integrity, transparency, and scalability of blockchain-based evidence storage.

The implementation of smart contracts for blockchain-based evidence management necessitates the use of Solidity for Ethereum-based contracts and Hyperledger Composer for permissioned blockchain solutions. AI model development relies on Python-based frameworks such as TensorFlow, Keras or PyTorch, enabling creation and deployment of advanced object detection models. Seamless integration between AI processing and blockchain storage is essential for secure and automated evidence handling.

To ensure legal admissibility and compliance, the system must align with regulatory frameworks governing security and evidence management. Collaboration with law enforcement agencies is essential to facilitate integration of blockchain-stored evidence into judicial proceedings. Compliance with international security standards, such as ITAR (International Traffic in Arms Regulations), is critical for proper handling of sensitive evidence. Furthermore, legal frameworks must be adapted to recognize blockchain-based records as valid and tamper-proof evidence in legal investigations and court proceedings.

VII. Summary

This paper presents a novel approach to combating corruption in security screening by integrating AI-powered X-ray detection with blockchain-based evidence management. Unlike traditional systems that rely solely on manual image analysis and centralized databases, this framework equips security personnel with an incorruptible tool, ensuring that evidence of illicit activities remains untampered, even in cases involving powerful entities. AI-driven object detection models enhance real-time identification of prohibited items, providing immediate alerts and securely storing detection metadata on immutable blockchain ledger. The focus is not on replacing human workers, but rather on empowering them with a system that reinforces their role and protects their integrity.

Blockchain technology ensures transparent, decentralized, and tamper-proof evidence storage, preventing influential individuals or organizations from manipulating records. Use of smart contracts automates evidence handling, while decentralized storage solutions like IPFS, Arweave, and Filecoin ensure secure, long-term access to X-ray images and reports. Further security measures, such as Zero-Knowledge Proofs and multi-signature authentication, allow for controlled access by authorized legal and law enforcement personnel while maintaining confidentiality and data integrity. This system fundamentally reshapes security operations, ensuring that workers are no longer powerless in the face of corruption, and that justice is upheld through verifiable, tamper-proof digital records.

References

[1] Vukadinovic, D., & Anderson, D. (2022) "X-Ray Baggage Screening and Artificial Intelligence (AI)". JRC Science for Policy Report. Retrieved from: https://www.researchgate.net/publication/361305570

[2] Huegli, D. (2024) "Benefits and Pitfalls of Decision Support Systems in Airport Security X-Ray Baggage Screening". Retrieved from: https://www.researchgate.net/publication/380005776

[3] Mouton, A., & Breckon, T. P. (2015) "A Review of Automated Image Understanding within 3D Baggage Computed Tomography Security Screening." Journal of X-Ray Science and Technology, vol.23(3), pp.: 323–344. Retrieved from: https://core.ac.uk/download/pdf/578109329.pdf

[4] Khan, S. U., Khan, I. U., Ullah, I., & Saif, N. (2020) "A Review of Airport Dual Energy X-Ray Baggage Inspection Techniques: Image Enhancement and Noise Reduction". Journal of X-Ray Science and Technology, vol.28(5), pp.: 871–891. Retrieved from: https://www.researchgate.net/publication/341170754

[5] Huegli, D., Chavaillaz, A., Sauer, J., & Schwaninger, A. (2025) "Effects of False Alarms and Miscues of Decision Support Systems on Human–Machine System Performance: A Study with Airport Security Screeners." Ergonomics. Retrieved from: https://doi.org/10.1080/00140139.2025.2453546

[6] Cordova, A. (2022) "Technologies for Primary Screening in Aviation Security". Journal of Transportation Security, vol.15(2), pp.: 145–162. Retrieved from: https://doi.org/10.1007/s12198-022-00248-8

[7] Wachie, O. E. (2022) "Human Factor and X-Ray Baggage Screening on Provision of Security and Safety of Universities within Nairobi City County, Kenya." International Atomic Energy Agency. Retrieved from: https://inis.iaea.org/records/c1mxg-60952/files/53097336.pdf

[8] Hügli, D.M. (2022) "Benefits and Pitfalls of Decision Support Systems in Airport Security X-ray Baggage Screening".

[9] Bureau of Industry and Security (2012, January 4). *FedEx agrees to pay $370,000 civil penalty for export violations.* U.S. Department of Commerce. Retrieved from: https://www.bis.doc.gov/index.php/licensing/embassy-faq/faq/232-when-is-a-license-required-for-export-of-non-mt-controlled-items-for-use-in-missile-activitie

[10] The Ditch. (2024, Month Day). [Tweet text excerpt] [Tweet]. X. https://x.com/wereontheditch/status/1849044880783270383

[11] The Ditch. (2024, Month Day). [Tweet text excerpt] [Tweet]. X. https://x.com/wereontheditch/status/1853478801998827557

[12] The Ditch. (2024, Month Day). *FedEx deletes evidence.* The Ditch. https://www.ontheditch.com/fedex-deletes-evidence/

[13] The Ditch. (2024, November 4). *The Ditch is going to court.* The Ditch. https://www.ontheditch.com/the-ditch-is-going-to-court/

[14] Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System". Retrieved from: https://bitcoin.org/bitcoin.pdf

[15] Alexopoulos, C., Ferro, E., & Lampoltshammer, T. J. (2025) "Blockchain and Tokenomics for Sustainable Development." Frontiers in Blockchain. Retrieved from: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1567925/full

[16] Zhang, H., Xiao, P., Yao, F., Zhang, Q., & Gong, Y. (2025) "Fusion of Multi-Scale Attention for Aerial Images Small-Target Detection Model Based on PARE-YOLO." Scientific Reports. Retrieved from: https://www.nature.com/articles/s41598-025-88857-w

[17] Matsuzaka, Y., & Yashiro, R. (2025) "The Diagnostic Classification of the Pathological Image Using Computer Vision". Algorithms. Retrieved from: https://www.mdpi.com/1999-4893/18/2/96

[18] Wang, Q., Zhu, X., Sun, Z., Zhang, B., Yu, J., & Qian, S. (2025) "Optimized Yolov8 Feature Fusion Algorithm for Dental Disease Detection". Computers in Biology and Medicine. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0010482525001283

[19] Labelbox. Available at: https://labelbox.com

[20] CVAT (Computer Vision Annotation Tool). Available at: https://cvat.org

[21] Varshney, T., & Sehrawat, R. (2025) “Object Detection Approach for Pneumonia Detection Using X-Ray Images”. Data-Driven Analytics for Healthcare. Taylor & Francis. Retrieved from: https://www.taylorfrancis.com/chapters/edit/10.1201/9781003558743-4/object-detection-approach-pneumonia-detection-using-ray-images-tanishq-varshney-ruchi-sehrawat

[22] Alabay, H. H., Le, T. A., & Ceylan, H. (2024) “X-Ray Fluoroscopy Guided Localization and Steering of Medical Microrobots Through Virtual Enhancement”. arXiv preprint. Retrieved from: https://arxiv.org/abs/2409.08337

[23] Liu, K., Ren, B., He, C., Wang, F., & Xu, Z. (2024) “X-Ray Security Contraband Detection Based on Improved YOLOX”. Proceedings of ACM Transactions on Computer Vision, Computing, and Machine Learning. Retrieved from: https://dl.acm.org/doi/abs/10.1145/3654823.3654863

[24] Mehta, R., Khabya, N., Patil, J., & Others. (2024) “Nivaran-Blockchain Based FIR System”. IEEE Conference on Intelligent Systems. Retrieved from: https://ieeexplore.ieee.org/abstract/document/10511219/

[25] Gutierrez, J., Klein, A., & Hung, P. C. K. (2024) “Introduction to the Special Issue on Thriving Amidst Disruptive Technologies”. ACM Distributed Ledger Technologies. Retrieved from: https://dl.acm.org/doi/abs/10.1145/3661804

[26] Sachan, A., Pandey, S., & Saxena, R. (2024) “Blockchain-Enabled Vault for Evidence Management System”. IEEE 13th International Conference on Blockchain Security. Retrieved from: https://ieeexplore.ieee.org/abstract/document/10545764/

[27] Chang, T. K., Yang, C. N., & Tseng, C. Y. (2024) “BT-DEF: A Secure Digital Evidence Framework Using Blockchain and TP-Merkle Tree”. IEEE Conference on Control and Robotics. Retrieved from: https://ieeexplore.ieee.org/abstract/document/10585397/

[28] Ge, Z., Liu, S., Wang, F., Li, Z., Sun, J. (2021) “YOLOX: Exceeding YOLO Series in 2021”. Retrieved from: https://arxiv.org/abs/2107.08430#:~:text=For%20YOLO,practical%20scenes%2C%20and%20we%20also

[29] PyTorch-SSD – GitHub. Retrieved from: https://github.com/biyoml/PyTorch-SSD

[30] Hui, J. (2018) “SSD Object Detection: Single Shot MultiBox Detector for Real-Time Processing”. Retrieved from: https://jonathan-hui.medium.com/ssd-object-detection-single-shot-multibox-detector-for-real-time-processing-9bd8deac0e06

[31] Luan, T., Zhou, S., Zhang, G., Song, Z., Wu, J., & Pan, W. (2024) “Enhanced Lightweight YOLOX for Small Object Wildfire Detection in UAV Imagery”. Sensors. Retrieved from: https://www.mdpi.com/1424-8220/24/9/2710

[32] Patel, K., & Peters, D. (2025) “Object Detection for City and Highway Driving Scenario with YOLOX and Mask RCNN”. SAE Technical Papers. Retrieved from: https://www.sae.org/publications/technical-papers/content/2025-01-8015/

[33] Kunhoth, S., & Alfadhli, M. (2024) “Optimizing High-Altitude UAV Object Detection with Deep Learning”. IEEE Conference on AI for Quality of Life. Retrieved from: https://ieeexplore.ieee.org/abstract/document/10822964

[34] Balaram, A., Suneel, S., & Kavitha, P. M. (2024) “A Secured Multiple Party Key Agreement Protocol Design Over Cloud Computing Platform by Using Statistical Data Analysis Logic”. IEEE Conference on Blockchain and Smart Systems. Retrieved from: https://ieeexplore.ieee.org/abstract/document/10624739/

[35] Jadhav, R., Gonepuri, A., & Deshpande, P. (2024) “Blockchain-Based Government Fund Disbursal System using Blockchain and IPFS”. IEEE Conference on Intelligent Systems. Retrieved from: https://ieeexplore.ieee.org/abstract/document/10581236/

[36] Honnungar, R. V., Prasad, S. B., & AR, A. K. (2024) “An Extensive Study of Decentralized Storage Networks Driven by Blockchain”. SCRS Publications. Retrieved from: https://www.publications.scrs.in/uploads/final_menuscript/d5bf28178cde441c4039ca1bcc5d0fc6.pdf

[37] Giacomelli, I. (2024) “Filecoin: From Proof-of-Space Blockchain to Decentralized Storage”. CrypTorino Conference. Retrieved from: https://iris.unito.it/retrieve/b3fb13c7-a30c-43cc-8109-918d9078066d/Cryptorino.pdf#page=28

[38] Coskun, V., Ajlouni, N., & Busra, O. (2024) “Secure Mobile Authentication With Blockchain Utilizing ECC, ZKPs, and Post-Quantum Cryptography”. Research Square. Retrieved from: https://www.researchsquare.com/article/rs-5310431/latest

[39] Vinoth, P. I., Kumar, D. N., & Guhan, M. P. S. (2024) “A Secure Authentication Mechanism for IoT Devices Using Hyperledger Fabric”. Advances in Distributed Systems. Retrieved from: https://books.google.com/books?hl=en&id=qQIPEQAAQBAJ