SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.04 NO. 1 2025
DOI: 10.51984/SUCP.V4I1.3934

المؤتمر العلمي الأول للتطبيقات الهندسية (ICEA'2024)
The First Scientific Conference on Engineering Applications (ICEA'2024)
Conference homepage: www.icea.ly

# Enhancing Security and Privacy of CCTV Data in Smart Cities through Digital Watermarks and Smart Contracts

*Kheraifia mohamed El Amine[a], Abdelatif Sahraoui[b], Derdour Makhlouf[c], Kouzou Abdellah[d]

[a]LAMIS Laboratory Echahid Cheikh Larbi Tebessi University, Tebessa, 12000 , Algeria
[b]LAMIS Laboratory Echahid Cheikh Larbi Tebessi University, Tebessa, 12000 , Algeria
[c] LIAOA Laboratory Oum el Bouaghi University, Oum el Bouaghi, 04000 , Algeria
[d]LAADI Laboratory Djelfa University, Djelfa, 17000 , Algeria

**Keywords:**
Blockchain
Video fingerprint
Smart contract
Hash
Watermark

**ABSTRACT**

Video surveillance plays a crucial role in smart cities, enhancing security, safety, monitoring, and analysis across various applications. These systems often collect data that includes sensitive information related to privacy, crime, and national security. Ensuring the authenticity and integrity of video footage is essential to confirm that the data comes from a legitimate and authorized source, which is critical for both security and legal purposes. An unverified video source in a surveillance system can present significant risks, as altered or manipulated footage may mislead investigations and result in wrongful accusations or convictions. Improving traceability within video surveillance systems is therefore vital for effectively tracking, verifying, and managing video data. This paper proposes a method that combines digital watermarking to prevent tampering or frame replacement with smart contracts to provide source verification and traceability for surveillance data.

# تعزيز أمن وخصوصية بيانات الدوائر التلفزيونية المغلقة في المدن الذكية من خلال العلامات المائية الرقمية والعقود الذكية

*خرايفية محمد الامين[a] و صحراوي عبد اللطيف[b] و دردور مخلوف[c] و قوزو عبد الله[d]

[a]مخبر لميس، جامعة الشيخ العربي تبسي ، تبسة 12000، الجزائر
[b]مخبر لميس، جامعة الشيخ العربي تبسي ، تبسة 12000، الجزائر
[c]مخبر ليوية، جامعة ام البواقي ، ام البواقي 04000، الجزائر
[d]مخبر ليدي، جامعة الجلفة ، الجلفة 17000، الجزائر

**الكلمات المفتاحية:**
التجزئة
العلامة المائية
العقد الذكي
بصمة الفيديو
سلسلة الكتل

**الملخص**

تلعب المراقبة بالفيديو دورًا حاسمًا في المدن الذكية، مما يعزز الأمن والسلامة والمراقبة والتحليل عبر التطبيقات المختلفة .غالبًا ما تجمع هذه الأنظمة بيانات تتضمن معلومات حساسة تتعلق بالخصوصية والجريمة والأمن القومي .يعد التأكد من صحة وسلامة لقطات الفيديو أمرًا ضروريًا للتأكد من أن البيانات تأتي من مصدر شرعي ومصرح به، وهو أمر بالغ الأهمية للأغراض الأمنية والقانونية .يمكن لمصدر فيديو لم يتم التحقق منه في نظام المراقبة أن يشكل مخاطر كبيرة، حيث أن اللقطات المعدلة أو التي تم التلاعب بها قد تضلل التحقيقات وتؤدي إلى اتهامات أو إدانات غير مشروعة .لذلك يعد تحسين إمكانية التتبع داخل أنظمة المراقبة بالفيديو أمرًا حيويًا لتتبع بيانات الفيديو والتحقق منها وإدارتها بشكل فعال .تقترح هذه الورقة طريقة تجمع بين العلامات المائية الرقمية لمنع التلاعب أو استبدال الإطار بالعقود الذكية لتوفير التحقق من المصدر وإمكانية تتبع بيانات المراقبة.

## 1. Introduction

Video transmission in vehicular networks is a pivotal technology enabling real-time multimedia data exchange between vehicles and surrounding infrastructure. With the rise of connected and autonomous vehicles, the demand for applications such as video conferencing, video streaming for navigation, and real-time surveillance has grown substantially. Innovative solutions, including network slicing [1] and advanced encoding techniques [2], show promise in enhancing the quality of experience and addressing application-specific challenges. However, secure video transmission in such networks faces unique obstacles, including high vehicle mobility, unstable connectivity, and the need to maintain low latency and high quality of service (QoS). Therefore, designing efficient routing protocols tailored to the

*Corresponding author:
E-mail addresses: mohammedelamine.kheraifia@univ-tebessa.dz , (A. Sahraoui) abdelatif.sahraoui@univ-tebessa.dz ,( D. Makhlouf) derdour.makhlouf@univ-oeb.dz ,( K. Abdellah) kouzouabdellah@ieee.org

*Article History : Received 21 March 2024 - Received in revised form 27 September 2024 - Accepted 15 October 2024*

constraints of vehicular environments is crucial for ensuring seamless and reliable video communication [3].Video surveillance systems play a vital role in smart cities, serving as essential tools for monitoring, managing, and enhancing various urban services and infrastructure. These systems are designed to improve safety, efficiency, and the quality of life for residents. Strategically placed cameras oversee public spaces, detect criminal activity, and ensure public safety. Advanced analytics integrated into these systems can identify unusual activities and promptly notify authorities. Additionally, they support real-time traffic monitoring to reduce congestion and enhance transportation efficiency, contribute to pollution control, and promote a healthier urban environment. Furthermore, video surveillance systems provide crucial real-time data, enabling swift responses to emergencies such as fires, medical incidents, and natural disasters.Although video surveillance systems provide significant advantages, they also pose notable risks, particularly concerning privacy. Constant monitoring can infringe on individual privacy, as movements and activities are continuously recorded [4]. Additionally, the vast amounts of data generated by these systems can become attractive targets for cyberattacks. Moreover, these technologies may be misused in specific attacks, such as video manipulation, which can mislead activists, industries, and security personnel. Such exploitation undermines the system's reliability and can result in serious consequences. Uncertainty about the origin of a video within a surveillance system can lead to several serious risks. Altered or manipulated videos may present false evidence, potentially misguiding investigations and resulting in wrongful accusations or convictions. Additionally, unauthorized entities could insert, delete, or modify frames, eroding trust in the system if the video's authenticity cannot be assured.

This research focuses on securing video surveillance data within an IoT environment by ensuring source verification to enhance credibility and integrity. We propose a lightweight system that integrates watermarks and QR codes, generated through smart contracts between an IoT video monitoring device and a data receiver, such as an edge or cloud system. The approach involves creating a recording timestamp file stored on the blockchain to authenticate and verify video recordings. To enable tracking during video review, a smart contract is established between the user and the cloud, utilizing watermarks and QR codes to document the review process. This method strengthens the detection and prevention of tampering or substitution of original footage with false data during video transmission. Additionally, it improves traceability within video surveillance systems, ensuring security and accountability through precise verification and tracking of video data.

The content of this paper is organized as follows: Section 2 introduces the related works. Section 3 introduces video surveillance system and Digital watermarking. Section 4 presents our watermark system for video surveillance. Section 5 presents the performance evaluation of the proposal. The section 6 concludes our work.

## 2. Related Work

Blockchain-based watermarking surveillance systems use innovative techniques to effectively detect and prevent tampering or manipulation of surveillance data. By combining the immutable nature of blockchain technology with watermarking methods, these systems ensure data integrity and authenticity.This section discuss the research's that integrates the watermarking and blockchain for security of video surveillance systems. Li et al [5] proposed blockchain-watermarking scheme effectively detects and locates tampered areas in compressed sensed images, ensuring data integrity and preventing manipulation. By utilizing blockchain's decentralization and non-tamperability, it enhances the security of surveillance data against unauthorized alterations. Araghi et al [6] introduced a blockchain-based framework for detecting disinformation through semi-fragile watermarking, which accurately identifies tampered regions in images and videos. By providing evidence of manipulated content and limiting its spread, this approach strengthens the integrity of surveillance data. Meng et al [7] .,proposed a novel design scheme for a copyright management system that integrates digital watermarking, blockchain, a cognitive hash function (QR), and the Interplanetary File System (IPFS). Fang et al [8].,proposed a fragile block watermarking method using blockchain technology for localizing image tampering. This method demonstrates strong resistance to attacks and high accuracy in pinpointing tampered areas, indicating its potential for detecting and preventing manipulation in surveillance data . Zhaofeng et al. [9] proposed a digital rights management scheme for artwork images aimed at detecting misuse on the Internet. This scheme combines watermarking and blockchain technology to deliver robust protection and enhanced security. Zheng et al [10]., developed an innovative scheme for protecting video copyrights using blockchain and double watermarking technology. Padma Priya et al [11]., divided the video into frames based on its frame rate and duration. The first frame is merged with the selected watermark, and this watermarked frame is then used as the watermark for the second frame. Wang et al [12]., integrated blockchain technology with zero watermarking and employs the IPFS to address the issue of blockchain data scalability. Blake [13]., introduced an embedded blockchain scheme for detecting manipulated audio and video it combines blockchains, encrypted spread spectrum watermarks, perceptual hashing, and digital signatures. In our previous work [14]., we presented a method based on video fingerprinting that utilizes timestamps to prevent and detect image tampering or the replacement of original images during the transmission and reception of monitored data. This method employs blockchain for tracking, reviewing, and authentication procedures. Zhu et al [15]., employs Fully Homomorphic Encryption (FHE) to preserve user privacy while embedding watermarks. Simultaneously, it ensures the traceability of the watermark through blockchain smart contracts.

## 3. Background

This section discusses a Video Surveillance System and its components.

### a) Video Surveillance System

Video surveillance systems are integral to the development of smart cities, enhancing public safety and urban management through advanced technologies. These systems utilize artificial intelligence (AI), machine learning, and Internet of Things (IoT) devices to monitor urban environments in real time, providing critical data for law enforcement and city planners.In smart cities, the surveillance infrastructure is organized into four layers [16],.

**The foundational layer** consists of surveillance equipment, primarily Closed-Circuit Television (CCTV) systems. CCTV systems use video cameras to send signals to a limited set of devices, playing a crucial role in security across various sectors by providing real-time monitoring, recorded footage, and advanced features like motion detection and AI integration. This layer includes diverse camera types: IP cameras (Internet Protocol cameras), which send and receive data over the internet or a local network; PTZ cameras (Pan-Tilt-Zoom), which can pan, tilt, and zoom to cover extensive areas and focus on specific points of interest; and mobile devices such as car cameras, drones, and smartphones, all contributing to adaptable and multi-angle monitoring.

**The second layer**, Edge Computing, manages the processing and analysis of video data close to its source, enabling real-time processing [17]. This local analysis allows only relevant or summarized information to be transmitted, reducing the processing load on cloud servers.

**The third layer** incorporates cloud computing, offering a scalable, flexible, and cost-effective solution for storing video recordings, with easy access to footage from anywhere with an internet connection [18]. For instance, Sahraoui et al. [19]-[22], drvice for an intelligent traffic management system, which improves road safety by monitoring road segments and predicting potential accident risks

**The final layer**, Blockchain, serves as a decentralized, secure, and immutable ledger. It is used to prevent tampering and unauthorized access, making it an ideal choice for securing video surveillance systems in smart cities.

### b) Digital watermarking

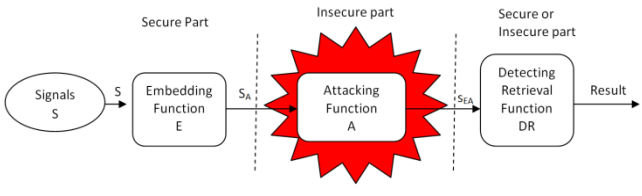

**Fig. 2: Digital watermarking life-cycle phases**

Watermarking is an essential method for safeguarding digital content, asserting ownership, and preserving data integrity across various fields. This technique embeds hidden information within digital media—such as images, audio, or video—to establish copyright and prevent unauthorized usage. Recent innovations have expanded watermarking applications and techniques, especially in multimedia content and recommender systems.

A digital watermark is a form of marker that is discreetly embedded within a signal that can tolerate noise, such as audio, video, or image data [23]. This technique embeds a message within multimedia works, classified into spatial, frequency, and wavelet domains[24].

Its primary purpose is to indicate ownership of the copyright for that signal. The figure 2 illustrates the general life-cycle phases of digital watermarking, encompassing embedding, attacking, and detection and retrieval functions. Digital watermarks can be categorized based on various criteria, including their application, visibility, and robustness, types of digital watermarks is:

**Visible Watermarks**: These are superimposed on the content, often for branding or attribution, and are easily noticeable to the viewer without any specialized tools.

**Invisible Watermarks**: Also called covert watermarks, these are embedded within the content and remain hidden from view, requiring specific software to detect and extract.

**Fragile Watermarks**: These are highly sensitive to any modifications, making them ideal for verifying the integrity of documents or images.

**Robust Watermarks**: Designed to endure standard signal processing operations and potential attacks, such as compression, cropping, or added noise, they are commonly used for copyright protection and content authentication.

**Spatial Domain Watermarks**: These are embedded directly into the pixel values of the content, making them straightforward to implement but generally less resistant to tampering or attacks.

**Frequency Domain Watermarks**: Embedded in the frequency components (such as the Fourier or wavelet domains), these watermarks offer more resilience but may require additional computational resources for embedding and detection.

**Digital Signature Watermarks**: Used to confirm the authenticity and origin of content, ensuring it hasn't been altered since signing.

**Dynamic Watermarks:** These are inserted with features that vary over time or based on specific conditions, often employed to track content distribution.

**4. Watermark In Video Surveillance:**

This section presents a model we developed to protect video data from tampering, specifically targeting visual layer attacks. Verifying the source is crucial to ensuring the authenticity and integrity of the footage, confirming that the video data originates from a legitimate and authorized source, which is essential for security and legal purposes. We achieve this by decentralizing access and integrating watermarking technology, all managed through smart contracts.

**a) Using a watermark in a video surveillance system**

The figure 3 shows the steps of our proposed model, where the smart contract creates and generates a list of random numbers. This contract takes place between two parties, namely the video surveillance IoT device and the edge device, which in turn performs several other operations.

The IoT video surveillance device generates an MD5 hash for each frame combined with its corresponding timestamp, creating a video timestamp file that is securely stored on the blockchain.

The IoT monitor utilizes the value *x*, along with the specified duration and the frame timestamps from the list generated by the smart contract, to create a QR code image based on the value $x$

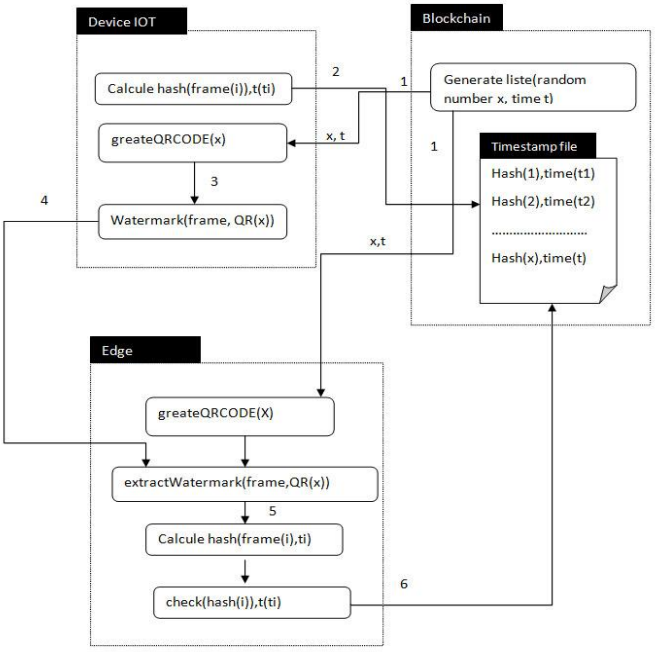


**Fig. 3: Watermarking between IoT Devices, Edge and Blockchain**

**Algorithm 1** Random_Numbers_List

**Data**: ID-Edge,ID-divice,Tmp
**Result**: List RandomNumberslist
$t \leftarrow 0$
**while** $t \leq Tmp$ **do**
  $x \leftarrow Random()$
  *RandomNumbersList.add(x, t)*
  $t \leftarrow t + 1$
**end**
**return**(RandomN umberslist)

Algorithm1 shows the smart contract for generating a list of random numbers . The IoT monitor generates a watermark using a QR code image and embeds it into the frame. The resulting result is sent to the edge. At the edge level, upon receiving the transmitted data, the system extracts the watermark using the $x$ value generated by the smart contract to recreate the QR code image and retrieve it from the frame. The extracted result is then cross-verified with the timestamp file stored on the blockchain

**b) Light watermark for the IoT**

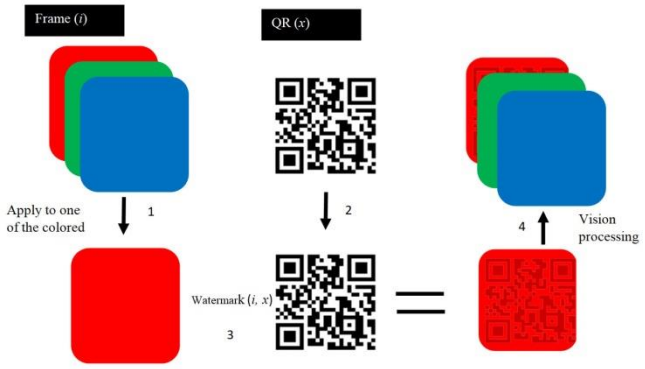


**Fig. 6. Light watermark steps**

In this section, we propose a lightweight watermarking algorithm (Figure 6) designed for IoT devices used in video surveillance. Algorithm 2 outlines the process of embedding a watermark into a video frame using QR code images. The QR codes are embedded into one of the color channels (RGB) of the video frame by reducing the value of a specific pixel in the chosen color channel whenever the corresponding pixel in the QR code is black. An MD5 hash is then calculated for the modified image. For the final display, all pixel

values of 255 in the layer containing the embedded QR code are converted to 0.

**Algorithm 2** watermark

**Data:** Image frame , QR
**Result:** Image Wframe
*i* ← *0*
*j* ← *0*
**while** *i* ⩽*QR*.Height - 1 **do**
**while** *j* ⩽*QR.Width - 1* **do**
*pixel* ← *QR(i, j);*
**if** *pixel == Color.black* **then**
*i* ← *i − 1*
**if** *frame(i, j).red == 0* **then**
*frame(i, j).red* ← *255*
**else**
*frame(i, j).red* ← *frame(i, j).red − 1*
**end**
**end**
j ← j + 1
**end**
i ← i + 1
**end**
*Wf rame* ← *f rame*
**return(***Wframe***)**

## 5. Evaluation And Results

This section presents the results obtained. For our experiment, we utilized the Ethereum blockchain, a decentralized platform that supports the development and deployment of security solutions for video surveillance. This was achieved through smart contracts involving blockchain users, IoT devices, edge nodes, and cloud storage services. The smart contracts were written in Solidity, a programming language specifically designed for creating blockchain-based smart contracts on platforms like Ethereum.

Additionally, we employed the C# programming language, a modern, flexible, and object-oriented language developed by Microsoft, to implement security policies tailored for surveillance applications, including mobile and cloud environments. Table 1 provides a comparison of resource usage for different computations, including RAM consumption, CPU usage percentage, and average execution time per iteration (based on 1000 iterations). The comparison covers the watermarking algorithm (Light-W), the MD5 hash calculation, and a combination of Light-W with MD5.

**Table1;Resource Usage Comparison**

| | MD5 | Light-W Light- | W+MD5 |
|---|---|---|---|
| CPU USAGE (%) | 9% | 12% | 14% |
| MEMORY USAGE(MB) | 7mb | 4mb | 8mb |
| AVERDGE TIME PER ITERATION | 29,169ms | 6139,83ms | 7113,51ms |

**Table2: Watermarking result**

| **Frame(i)** | **QR(x)** | **Watermark (frame(i),QR(x))** |
|---|---|---|
|  |  |  |
| **MD5:ae2684da01551e5 81c14a9cc1c039834** | **X=5021986** | **MD5:5e127c2905364 ffa606b004b7874aff9** |

Table 2 illustrates a specific frame captured by a computer camera, with its MD5 hash calculated and recorded in the timestamp file. A smart contract facilitates communication between the camera and the edge device to generate a random number. Column 2 presents the QR code image generated from this number, while Column 3 displays the output of the watermarking algorithm, including the corresponding MD5 hash. This output is transmitted to the edge device, where the watermark is extracted by retrieving the random number via the smart contract and reconstructing the QR code image. The MD5 hash of the extracted frame is then computed and compared with the value in the timestamp file for verification.

## 6. Conclusion

This study proposes a solution that integrates blockchain technology and watermarking to safeguard video authenticity and prevent tampering, ensuring that recordings remain admissible as forensic evidence for law enforcement and judicial purposes. Looking ahead, our objective is to enhance this framework by combining watermarks with blockchain technology, encryption methods, and centralized management systems. This will establish a comprehensive traceability framework that bolsters security and privacy for video recordings in smart cities.

## 7. References

[1]- Arbaoui, A., Abdelatif, S., & Derdour, M. (2024, April). Network Slicing solutions for Internet of Vehicles (IoV) Networks: A Review. In 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)(pp. 1-7). IEEE.

[2]- Abdelghani, G., Abdelatif, S., & Derdour, M. (2024, April). Improving QoE in IoV: a review of solutions and challenges for MPEG-DASH. In 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS) (pp. 1-8). IEEE.

[3]- Abdelatif, S., Derdour, M., Ghoualmi-Zine, N., & Marzak, B. (2020).VANET: A novel service for predicting and disseminating vehicle traffic information. International Journal of Communication Systems, 33(6), e4288

[4]- Ruchaud, N., & Dugelay, J. L. (2017, July). ASePPI: Robust Privacy Protection against De-Anonymization Attacks. In CVPR Workshops (pp. 1352-1359).

[5]- Li, M., Zeng, L., Zhao, L., Yang, R., An, D., & Fan, H. (2021). Blockchain-watermarking for compressive sensed images. IEEE Access, 9, 56457-56467:

[6]- Araghi, T. K., Megías, D., Garcia-Font, V., Kuribayashi, M., & Mazurczyk, W. (2024, June). Disinformation detection and source tracking using semi-fragile watermarking and blockchain. In European Interdisciplinary Cybersecurity Conference (pp. 136-143).

[7]- Meng, Zhaoxiong, et al."Design scheme of copyright management system based on digital watermarking and blockchain." 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). Vol. 2.IEEE, 2018.

[8]- Fang, W., Wang, Y., & Wang, X. (2020). Image tampering location and restoration watermarking based on blockchain technology. In Big Data Analytics for Cyber-Physical System in Smart City: BDCPS 2019, 28-29 December 2019, Shenyang, China (pp. 420-428). Springer Singapore.

[9]- Zhaofeng, M., Weihua, H., & Hongmin, G. (2018). A new blockchain based trusted DRM scheme for built-in content protection. EURASIP Journal on Image and Video Processing, 2018(1), 91

[10]- Zheng, J., Teng, S., Li, P., Ou, W., Zhou, D., & Ye, J. (2021). A novel video copyright protection scheme based on blockchain and double watermarking. Security and communication networks, 2021, 1-16.

[11]- Padma Priya, R., Tiwari, A., Pandey, A., & Krishna, S. (2021). Identifying video tampering using watermarked blockchain. International Journal of Performability Engineering, 17(8), 722.

[12]- Wang, B., Jiawei, S., Wang, W., & Zhao, P. (2020, December). A blockchain-based system for secure image protection using zero-watermark. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 62-70). IEEE.

[13]- Blake, S. (2020). Embedded Blockchains: A Synthesis of Blockchains, Spread Spectrum Watermarking, Perceptual Hashing & Digital Signatures. arXiv preprint arXiv:2009.00951.
[1] Girija, S. S., Zelalem, Y. D., (2012), IsatinsAs Privileged Molecules in Design and Synthesis of Spiro-Fused Cyclic Frameworks., Chem. Rev., **112**, 6104-6155. DOI:

[14]- Kheraifia, M. E. A., Sahraoui, A., & Derdour, M. (2024, April). Blockchain-Driven Adaptive Streaming for IoT: Redefining

Security in Video Delivery. In 2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS) (pp. 1-7). IEEE.

[15]- Zhu, D., Zheng, J., Zhou, H., Wu, J., Li, N., & Song, L. (2022). A hybrid encryption scheme for quantum secure video conferencing combined with blockchain. Mathematics, 10(17), 3037.

[16]- Ghimire, S., Choi, J. Y., & Lee, B. (2019). Using blockchain for improved video integrity verification. IEEE Transactions on Multimedia, 22(1), 108- 121

[17]- Cao, K., Liu, Y., Meng, G., & Sun, Q. (2020). An overview on edge computing research. IEEE access, 8, 85714-85728.

[18]- Myagmar-Ochir, Y., & Kim, W. (2023). A survey of video surveillance systems in smart city. Electronics, 12(17), 3567.

[19]- Sahraoui, A., Makhlouf, D., & Roose, P. (2018). Smart Traffic Management System for Anticipating Unexpected Road Incidents in Intelligent Transportation Systems. International Journal of Grid and High Performance Computing (IJGHPC), 10(4), 67-82.

[20]- Benzerogue, S., Abdelatif, S., Merniz, S., Harous, S., & Khamer, L. (2024).Multi-Path Transmission Protocol for Video Streaming over Vehicular Fog Computing environments. IEEE Access.

[21]- Abdelatif, S., Ghozlane, A., & Roose, P. (2022, October). A Virtual Clustering for Data Dissemination in Vehicular Fog Computing. In 2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS) (pp. 1-6). IEEE.

[22]- Abdelatif, S., Makhlouf, D., & Roose, P. (2017). Extended iCanCloud simulation framework for VANET-Cloud architectures. In 3rd International Conference on Networking and Advanced Systems.

[23]- Sencar, H. T., Ramkumar, M., & Akansu, A. N. (2004). Data hiding fundamentals and applications: content security in digital multimedia. Elsevier.

[24]- Tabassum, A. (2023). Digital Watermarking. International research journal of computer science, 10(05):124-129. doi: 10.26562/irjcs.2023.v1005.04