*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1249–1263
DOI : 10.47974/JDMSC-1733

# A blockchain based private framework for facilitating digital forensics using IoT

Bhawna Suri *
Shweta Taneja †
Siddharth Sharma §
Vishwajeet Verma ‡
Divyanshi Parashar @
Parth Sikka #
*Department of Computer Science & Engineering*
*Bhagwan Parshuram Institute of Technology*
*Delhi 110085*
*India*

Monika Arora $
*Department of Information Technology*
*Bhagwan Parshuram Institute of Technology*
*Delhi 110085*
*India*

Sayed Sayeed Ahmad ^
*Rochester Institute of Technology*
*Dubai Campus*
*Dubai*
*U.A.E.*

* *E-mail:* **bhawnasuri@bpitindia.com (Corresponding Author)**
† *E-mail:* **shwetataneja@bpitindia.com**
§ *E-mail:* **siddharth22sharma@gmail.com**
‡ *E-mail:* **vishwajeetverma.5@gmail.com**
@ *E-mail:* **divyanshi5120@gmail.com**
# *E-mail:* **parthsikkah704@gmail.com**
$ *E-mail:* **monikaarora@bpitindia.com**
^ *E-mail:* **saeed.ks@gmail.com**

**Abstract**

**Introduction:** Images play an essential role as evidence in any forensic analysis of a police investigation. They are a crucial part of the analysis and store important and nuanced information required to guide the analysis in the right direction and then finally lead the investigation to a just conclusion. However, these images are often subject to tampering. Malicious elements of society external or internal entities involved in conducting the investigation, try to tamper with, mend, and destroy pieces of evidence. This change can mislead the direction of the evidence and can benefit the accused.

**Research Problem:** Through the scope of this paper, we will try to tackle this problem and find a solution for it.

**Methods:** The approach proposed to tackle this problem is to implement a blockchain-based, distributed virtual private network (VPN) system. The network consists of devices spread across the internet, connected via a VPN. Only authorized devices are a part of the network and each device has a particular role and key. The image is captured from the IoT device at the crime scene, it is then encrypted using a Mixed Alphabet Cipher substitution algorithm that converts the RGB values to a string at the camera node and then transferred to the main server. It is further decrypted and again encrypted using the key of the main server. Upon encryption, the string is converted to a hash key which is then added to the blockchain.

**Results:** The performance of the proposed network is tested on two different parameters- operating system and image size. It was found that the encryption time of images varies linearly with image size, operating system and image size. The different operating systems are Ubuntu and two variants of MAC OS. The images being tested vary from 200x200 px to 3840x2160px. The encryption and decryption time of different images is recorded, and it was found that the encryption time of images varies linearly with image size.

**Conclusion:** The proposed solution was successfully developed and tested on different sets of images and operating systems. As our solution uses an in-house developed blockchain network, it has a better working cost than using an Ethereum-based blockchain.

---

***Subject Classification:*** *Primary 93A30, Secondary 49K15.*

***Keywords:*** *Digital forensics (DF), IoT, Blockchain, Virtual private network (VPN).*

## 1. Introduction

A crime is an illegal act that can be penalized. In any criminal case multiple entities and multiple evidence are involved for concluding the decision. Major chunk of important evidence of a criminal case are images which are often a target of malicious elements, who try to tamper with the evidence. In this paper we are dealing with DF in the form of digital evidence which is the image captured using the mobile phone's camera at the crime scene by the investigating officer or physical evidence which is the converted to image format (e.g. fingerprints scans converted to images). This electronic evidence is an indispensable component of DF and helps the investigation to move forward [1]. Nowadays, it is easy to

store and maintain the images digitally in comparison to the earlier days where the images were stored as physical copies and rolls of negatives and are more susceptible to damage. However, evidence tampering remains an issue and occurs frequently. This causes a lot of misinformed judgments, misdirected investigations, unnecessary usage of resources, and most importantly, often, it causes the guilty and malicious elements of society to go unpunished. With the help of our proposed model of evidence storage, we tackle this issue of evidence tampering, thus making the law enforcement system more resource-efficient and the judicial system juster. The distributed nature of blockchain is an appropriate solution for avoiding any intentional loss of evidence in digital forensics.

### 1.1 *Blockchain*

The blockchain technology is a decentralized ledger system, which can store linked records in the peer-peer network. The data is stored in the immutable unidirectional linked blocks. This is achieved with the help of hashes generated using cryptographic methods [2]. Storing digital evidence for criminal forensics just so happens to be one of those use-cases. The blockchain is implemented using VPN (Virtual Private Network).

### 1.2 *VPN*

A VPN is a way to create a private network in a public space [3]. The Wireguard protocol is used to set up a VPN between multiple machines. It creates an encrypted network that is high in speed and easier to configure [4]. and the management of the devices, via Tailscale.

### 1.3 *Major contributions of our work*

Through this research, we develop a system that:

- Removes the human element interaction while storing the images at the crime scene.
- VPN is used for blockchain implementation for storing and managing images is the novelty of our work.
- Takes optimal time for image encryption and decryption.
- Performance of the proposed system is tested on different sized images and as well as the machines with different configurations.
- Ensuring that no evidence can be tampered with, hence ensuring the smooth proceeding of cases.

The paper is organized as follows: Section 2 discusses the literature and usage of blockchain in DF. In section 3, system architecture and its detailed explanation is given. Section 4 introduces materials and methods for working of proposed model. Section 5 & 6 elaborates the working and performance of the proposed system. In the last section, conclusion is drawn with future aspects.

## 2. Related Work

In this section, the previous work related to DF, role of IoT and blockchain in DF is discussed.

### 2.1 *Digital forensics*

Digital Forensics is the branch of forensic science with four phases starting from data collection, examination, analysis, and reporting digitally. Collection, in this context, refers to the procedure by which a prosecutor gathers evidence from entities or IoT devices to obtain investigation-related data. The obtained data is then kept in a secure location. Examination performs a search and access of the retrieved data, as well as data verification. During analysis phase, the professional (physical or chemical) analysis can be done to get insights. The purpose of reporting is to deliver a final investigation report.

### 2.2 *IoT and Blockchain Technology in DF*

Blockchain is a secured and distributed P2P network. This technology is used by different researchers in different use-cases. In [5], the blockchain-based IoT forensics framework is built for the Identity privacy. They have incorporated a digital certificate method based on the Merkle signature to address identity privacy concerns. In another work[6], the massive data generated by IoT devices is prone to various types of cyber-crimes. The authors have used blockchain in forensics where the digital evidence is collected, preserved and reported using IoT. In [7], authors have used the concepts of Artificial Intelligence in Cloud Computing, IoT and blockchain to solve criminal forensics security issues. In [8] witness privacy and juror privacyare focused during evidence collection and court trials respectively. A local Ethereum-based test network was utilized with short signatures to authenticate witnesses' identities and ciphertext-policy attribute-based encryption for evidence access. In [9], a privacy-preserving and proof of existence approach (PPCF) was proposed to process records

based on blockchain and group signatures. Their approach is solely to convey forensics data, but lack in other critical digital forensics activities like minute data access. A digital forensics chain of custody based on blockchain was developed in [10] for the security of digital evidence. The creation, transfer, deletion, and display of evidence are all functions in their process model. Unfortunately, they failed to consider the prospect of malevolent lice investigators and failed to secure privacy. Another work is, blockchain-based digital evidence framework(Block-DEF), is built to support evidence gathering, storage, verification, and retrieval. Their solution keeps the information secure and traceable. Furthermore, repeated interactions among an evidence provider, a content provider, an evidence requester, and the trusted storage result in significant communication overhead [11].

### 2.3 *Image processing and Blockchain*

Blockchain technology is used in diversified areas of image processing in different domains like Automobile forensics [12], smart parking[13], medical data[14], data processing[15], software piracy[16] etc. In this paper, blockchain technology is used in digital forensics for examining criminal cases. The images captured from the crime scenes though IoT devices are compressed using DCT prior to be stored in database [17]. Other lossless image compression techniques like run length arithmetic encoding, Huffman coding and LZW are also popular[18].Once the images are stored in a database, to avoid any tampering with the important data, the security is a major concern. The authors in [19] have used digital signature-based authentication system. If anyone tries to play around with forensics evidence, can be traced using blockchain technology. The Ethereum based blockchain is implemented by authors in [20] for maintaining privacy and security. Another approach dealt with evidence security is storing evidence metadata in the information cryptography and the evidence in a secure storage medium [21]. In [22,23,24] IoT based blockchain for evidence collection, communication is devised for effective and secure evidence management using cross-border paradigm. Cryptocurrency usage is also seen in financing terrorist activities. In [25] the threat involved in cryptocurrency mining is discussed.

As seen above, the blockchain technology is explored in diverse use-cases and is implemented using Ethereum. We have also used the blockchain technology for ensuring the security of DF through a VPN over Wireguard protocol.

## 3. Materials & Methods

In this section, the entities involved and the proposed system architecture is discussed.

### 3.1 *Entities Involved*

The different entities involved in the criminal investigation process are shown in Table I

**Table I**
**Entities & their Roles**

| Entities Involved | Roles |
|---|---|
| Image Capturing Nodes | The IoT devices – image capturing nodes -police body cams capture and send the images to the blockchain. |
| Chief of Investigation | The chief officer has access to the data stored in the block chain and coordinates with the police, forensic investigator, and courthouse. |
| Police officers | The police officers working under Chief of Investigation carry body cams to the field. However, the policemen do not have access to the data they upload to the blockchain. |
| Courthouse | The Courthouse is the decision-making entity, interacts with the Chief of Investigation to receive details about the case. The Courthouse can access the blockchain network. |
| Judge | The Judge is the highest authority in the Courthouse and concludes the case by providing justice. The Judge has the access - to view the data stored in the blockchain. |
| Lawyers | The lawyers are part of the Courthouse and are given view access to the evidences stored the blockchain. |

### 3.2 *Proposed System*

We propose to create blockchain of IoT devices as shown in Figure 1, to safeguard the evidence storage for criminal forensics via a VPN (implemented using Wireguard protocol). The different entities in the network are image-capturing nodes, data servers, and access points to the servers. Each entity in the system is provided a numeric key (K) unique to the entity. The server stores a mapping of the keys to the machines, these keys are used to encrypt and decrypt the data items( images I). The workflow starts with the image-capturing node, once the image is captured, it is moved to the server, and verified at the server for its integrity

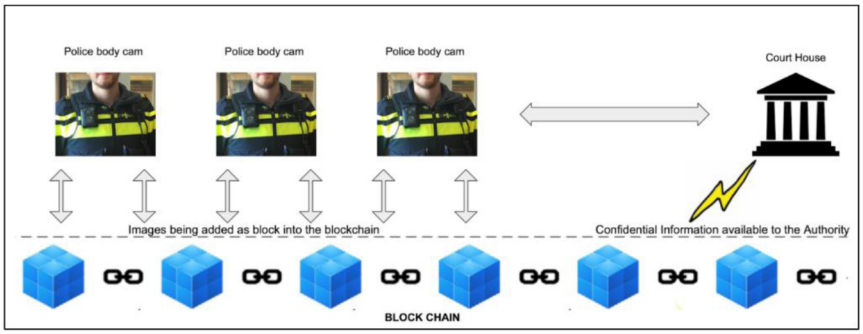


**Figure 1**

**Proposed Architecture**

and other distributed servers in the blockchain, the image is added to the blockchain, and all the other servers are updated. If an entity tries to access the chain, the server allows only certified entities.

## 4. Preliminaries

In this section different symbols used with their definitions are given in Table II. In Table III the functions devised for blockchain creation, hash key generation, encryption and decryption are mathematically explained.

**Table II**

**Symbols with their Definitions**

| Symbol | Definition | Symbol | Definition | Symbol | Definition |
|---|---|---|---|---|---|
| $\mathbf{B}^0$ | Blockchain | **K** | Key | **(x,x)** | Parameters |
| **H** | Hash | $\mathbf{m}_K$ | Mapping of digits according to the key K | $\rightarrow$ | Returns |
| $\mathbf{h}_p$ | Hash of the previous block | $\mathbf{m}_K^-$ | Reverse mapping in according to the key K | $\Gamma$ | Private network |
| $\mathbf{h}_c$ | Hash of the current block | **B** | Block class | **V** | Verified Blockchain |
| $\Delta_h$ | Database storing the hashes of every block | $\mathbf{b}_g$ | Genesis block | **V*** | Unverified Blockchain |

*Contd...*

| | | | | | |
|---|---|---|---|---|---|
| $\Delta_b$ | Database storing every block's data | $\mathbf{b_1}$, $\mathbf{b_2}$, $\mathbf{b_3}$ | Block instances | **C** | Authenticated Client |
| $\Delta_i$ | Database storing encrypted images | $\mathbf{b_d}$ | Block Data | **C*** | Unauthenticated Client |
| $\mathbf{I_p}$ | Path to the image file | $\mathbf{I_e}$ | Encrypted image | Γ | Client authentication key |
| **I** | Image | $\mathbf{I_d}$ | Decrypted image | $\mathbf{S_{ip}}$ | Server's IP Address |

**Table III**

**Brief Description of Functions**

| Function Name | Explanation | Mathematical Formulation |
|---|---|---|
| ***BlockClass - B ($h_p$, $I_e$)*** | The parameters are $h_p$ and $I_e$ and creates a new block. | $\mathbf{B\ (h_p, I_e) \rightarrow B(h)}$ |
| ***GenesisBlock - B ($h_p$, $I_e$)*** | The parameters are $h_p$ and $I_e$ returns the first block or the Genesis block $\mathbf{b_g}$ of the blockchain where $h_p$ is initially defined by the administrator and an empty string for $I_e$. A special parameter key (K) is assigned by the administrator while creating the block. | $B(h_p, I_e) \rightarrow b_g$ |
| ***BlockInstances - ($b_1$, $b_2$, $b_3$):*** | Instances added to the blockchain with every new image file. | $b_i\ V\ i = 1,2,3\ldots,n$ |
| GenerateKey - (K) | Parameters passed are $\mathbf{S_{ip}}$ and returns $\mathbf{m_K}$ as per the key $K$ (administrator defines $K$ while generating the genesis block) | $\mathbf{GenKey(S_{ip}) \rightarrow m_K}$ |
| EncryptImage- E(I, $m_K$) | Parameters passed are I and $m_K$ produced by the key K and returns $I_e$. This $I_e$ is then stored in blockchain in the form of a string. | $EnImg(I, m_K) \rightarrow I_e$ |
| DecryptImage- D($I_e$,$m_k$) | Parameters passed are $I_e$ and $m_k$ and returns $I_d$ in accordance with the mapping ($m_k$) produced by the key (K). | $DeImg(I_e, m_k) \rightarrow I_d$ |
| ReadImageData ($I_p$) | Input parameter - image path ($I_p$) Returns - an array of RGB pixel values of the file. This array is then converted into a "-" separated string form (denoted by I) for further processes. | $ReadImageData\ (I_p) \rightarrow \mathbf{I}$ |

*Contd...*

| | | |
|---|---|---|
| StoreBlockData ($h_c$, $b_d$) | Store the information of block data that is generated using $\Delta_b$ **($h_c$,$b_d$)**. It consists of $h_p$ and $h_c$ of the new block. | $SBD(h_c) \rightarrow \Delta_b(h_c,b_d)$ |
| StoreImageData ($I_e$, $h_c$) | Stores $I_e$ information with its hash ($h_c$) that is being sent over the secured network in encrypted form in JSON format. | $\Delta_h$ $(I_e, h_c)$ |
| Verification Authentication | Fetches ($\Delta_h$) stored in each of the clients over $\gamma$ into the main server. **Client authentication**: Checks the authentication key provided by the client while requesting access to the system. If the Client key ($\Gamma$) $\rightarrow$ 1, then { (C) } ,else { (C*) } | **Verify** the blockchain data ($\Delta_h$)1, ($\Delta_h$)1, ($\Delta_h$)1 …. With the main server data. If(($\Delta_h$)1==($\Delta_h$)1= =($\Delta_h$)1== ….) $\rightarrow$ 1 Then { blockchain is V } Else { blockchain is V*} |

## V. Workflow of Proposed System

The workflow of the proposed system is described in Figure 2. Also, the detailed description is as follows

**Step 1 Block creation**

Block creation, process require two parameters -$h_p$ and $I_e$, that was generated while the encryption of the string. These parameters are passed to create a new block instance (b) of Block class (B).

The block instance generates two parameters :-

block_data ($b_d$) = encrypted string ($I_e$) + "-" + previous block hash ($h_p$)

Block_hash ($h_c$) = SHA256Algorithm (block_data)

This data is stored in the files $\Delta_h$ ($h_c$), $\Delta_b$ ($h_c$,$b_d$), $\Delta_h$ ($I_e$, $h_c$) for the purpose of security and cross-checking of data.

**Step 2 Image transformation, Encryption and Storage**

For the transformation of the image, the image is first accessed through the image path ($I_p$) and then converted to an array of RGB pixel values. Going further, the elements of the array are changed to a string with "-" separating values. The generated string (I) is then encrypted according to the mapping ($m_k$) that is generated through a mapping algorithm and hence is unique. The W**atchdog** utility is used for creating and appending the new blocks containing data ($b_n$) and added in the blockchain ($B^0$). This is implemented using Python.

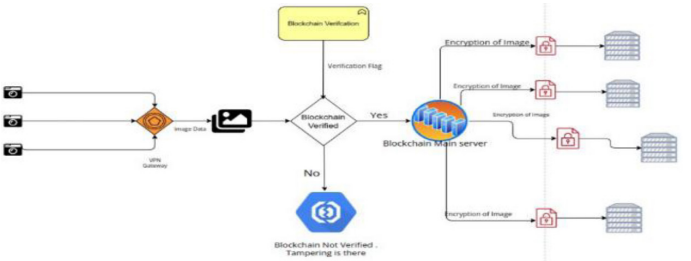


**Figure 2**

**Workflow of the Proposed System**

### Step 3 Decryption

Here, the hash (h) of a block is passed as a parameter, to obtain the encrypted data from the block by comparing the hash through the image data datafile ($\Delta_i$). Once this encrypted data is obtained, the key (K) is fetched from the block data datafile ($\Delta_b$) and the reverse key-value mapping ($m_K^-$) is obtained to decrypt the encrypted data. The encrypted data is first parsed and is split into an n-dimensional array of RGB pixel values. These pixel values are then decrypted using the reverse mapping ($m_K^-$) and user sees the decrypted image (I).

## 6. Results and Performance Analysis

The proposed system is implemented in python and SHA256 function is used to generate hashes in a one-directional fashion.

**Table IV**

**Images and their size**

| Image | Size |
|---|---|
| Image 1 | 259x194 px |
| Image 2 | 478x424 px |
| Image 3 | 1856x1880 px |
| Image 4 | 3840x2160 px |

**Table V**

**System Specifications**

| | |
|---|---|
| System 1 | OS: Ubuntu 20.04..3 LTS CPU11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40 GHz Quad Code |
| System 2 | OS: Mac OS 2 GHz Quad-Core Intel Core i5 Intel Iris Plus Graphics 1536 MB<br>16 GB 3733 MHz LPDDR4X |
| System 3 | OS: Mac OS Monterey 12.0.1<br>2.3 GHz 8-Core Intel Core i9<br>16 GB 2667 MHz DDR4<br>AMD Radeon Pro 5500M 4 GB |

6.1 *Performance Evaluation*

For the experimentation purpose, four samples of images of size varying from 200x200 px to 3840x2160px were taken as shown in Table IV. These images are sent to the network through the secure nodes. The testing of these images is done on three systems with different configuration (Table V).

Encryption, Appending & Decryption times of different images on different systems with different configurations shown in Table IV and V, are recorded & compared in Table VI.

**Table VI**

**Time Recorded for System 1, System 2 & System 3**

| Systems | Image Vs Encryption & Decryption Time | Encryption Time (S) | Encryption & Appending Time (S) | Decryption Time (S) |
|---|---|---|---|---|
| System 1 | Image 1 | 0.166 | 0.179 | 0.366 |
| | Image 2 | 0.615 | 0.627 | 0.699 |
| | Image 3 | 9.425 | 9.620 | 10.744 |
| | Image 4 | 21.421 | 22.054 | 25.638 |
| System 2 | Image 1 | 0.214 | 0.228 | 0.549 |
| | Image 2 | 1.014 | 1.032 | 1.235 |
| | Image 3 | 14.939 | 15.162 | 14.351 |
| | Image 4 | 34.183 | 34.862 | 34.443 |
| System 3 | Image 1 | 0.253 | 0.271 | 0.731 |
| | Image 2 | 0.958 | 0.981 | 1.376 |
| | Image 3 | 16.094 | 16.376 | 16.119 |
| | Image 4 | 36.141 | 37.175 | 38.112 |

6.2 *Performance Comparison*

The performance of our proposed system is compared with the existing systems on different parameters like encryption, integrity, authentication, access control etc. and shown in Table VII.

**Table VII**

**Performance Comparison**

| **Parameters** | **Zhang et al. (2017) [9]** | **M. Cebe et al. 2018[12]** | **Meng Li et al. 2021[ 8]** | **Proposed System (2022)** |
|---|---|---|---|---|
| Encryption | ✓ | x | ✓ | ✓ |
| Integrity | x | ✓ | ✓ | ✓ |
| VPN | x | x | x | ✓ |
| Access Control | x | x | ✓ | ✓ |
| Authentication | x | x | ✓ | ✓ |
| Immutability | x | x | x | ✓ |

## VII. Conclusion & Future Scope

To deal with the problem of tampering with evidence in criminal forensics, we have implemented a private blockchain network based on VPN. The network takes images as input, encrypts them, and adds them to the blockchain. The body cams which are the image capturing nodes capture images, encrypt them, and send them to the server which upon verification adds them into the chain as new blocks. SHA256 function is used for hash generation with parameters as hash of the previous block and the encrypted image. The entire network is built in python and is scalable with no added costs except that of the additional hardware required to scale. The performance of the system is tested on four different set of images and on three different operating systems. Our proposed system is better than the existing Ethereum and Solana-based models in terms of working cost. Our system also uses an in-house written encryption algorithm which makes the data stored hard to decrypt.

## References

[1] Selamat, Siti Rahayu, Robiah Yusof, Shahrin Sahib, Nor Hafeizah Hassan, Mohd Faizal Abdollah, and Zaheera Zainal Abidin. "Traceability in digital forensic investigation process." In *2011 IEEE Conference on Open Systems*, pp. 101-106. IEEE (2011).

[2] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." *International Journal of Web and Grid Services* 14, no. 4, 352-375 (2018).

[3] Ezra, Paul Joan, Sanjay Misra, Akshat Agrawal, Jonathan Oluranti, Rytis Maskeliunas, and Robertas Damasevicius. "Secured communication using virtual private network (VPN)." *Cyber Security and Digital Forensics*, 309-319 (2022).

[4] Lipp, Benjamin, Bruno Blanchet, and Karthikeyan Bhargavan. "A mechanised cryptographic proof of the WireGuard virtual private network protocol." In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 231-246. IEEE (2019).

[5] Le, Duc-Phong, Huasong Meng, Le Su, Sze Ling Yeo, and Vrizlynn Thing. "BIFF: A blockchain-based IoT forensics framework with identity privacy." In *TENCON 2018-2018 IEEE region 10 conference*, pp. 2372-2377. IEEE (2018).

[6] Kamal, Randa, Ezz El-Din Hemdan, and Nawal El-Fishway. "A review study on blockchain-based IoT security and forensics." *Multimedia Tools and Applications*, 1-32 (2021).

[7] Ganesh, N. S., N. G. Venkatesh, and D. Prasad. "A Systematic Literature Review on Forensics in Cloud, IoT, AI & Blockchain." *Illumination of Artificial Intelligence in Cybersecurity and Forensics*, 197-229 (2022).

[8] Li, Meng, Chhagan Lal, Mauro Conti, and Donghui Hu. "LEChain: A blockchain-based lawful evidence management scheme for digital forensics." *Future Generation Computer Systems* 115, 406-420 (2021).

[9] Zhang, Yong, Songyang Wu, Bo Jin, and Jiaying Du. "A blockchain-based process provenance for cloud forensics." In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 2470-2473. IEEE 92017).

[10] Lone, Auqib Hamid, and Roohie Naaz Mir. "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer." *Digital Investigation* 28, 44-55 (2019).

[11] Tian, Zhihong, Mohan Li, Meikang Qiu, Yanbin Sun, and Shen Su. "Block-DEF: A secure digital evidence framework using blockchain." *Information Sciences* 491, 151-165 (2019).

[12] Cebe, Mumin, Enes Erdin, Kemal Akkaya, Hidayet Aksu, and Selcuk Uluagac. "Block4forensic: An integrated lightweight blockchain

framework for forensics applications of connected vehicles." *IEEE Communications Magazine* 56, no. 10, 50-57 (2018).

[13] Zinonos, Zinon, Panayiotis Christodoulou, Andreas Andreou, and Savvas Chatzichristofis. "Parkchain: An iot parking service based on blockchain." In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 687-693. IEEE (2019).

[14] Shen, Meng, Yawen Deng, Liehuang Zhu, Xiaojiang Du, and Nadra Guizani. "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach." *IEEE Network* 33, no. 5, 27-33 (2019).

[15] Xu, Ronghua, Sherry Chen, Lixin Yang, Yu Chen, and Genshe Chen. "Decentralized autonomous imaging data processing using blockchain." In *Multimodal Biomedical Imaging XIV*, vol. 10871, pp. 72-82. SPIE (2019).

[16] Suri, Bhawna, Shweta Taneja, Hemankur Bhardwaj, Edwin John, Ayushi Jain, and Akansha Pal. "Ameliorating software piracy-a block chain based approach." *JIMS8I-International Journal of Information Communication and Computing Technology* 6, no. 1, 338-342 (2018).

[17] Strang, Gilbert. "The discrete cosine transform." *SIAM review* 41, no. 1, 135-147 (1999).

[18] Raghavendra, C., S. Sivasubramanian, and A. Kumaravel. "Improved image compression using effective lossless compression technique." *Cluster Computing* 22, no. 2, 3911-3916 (2019).

[19] Alam, Shahzad, Amir Jamil, Ankur Saldhi, and Musheer Ahmad. "Digital image authentication and encryption using digital signature." In *2015 International Conference on Advances in Computer Engineering and Applications*, pp. 332-336. IEEE (2015).

[20] Patil, Sonali, Sarika Kadam, and Jayashree Katti. "Security enhancement of forensic evidences using blockchain." In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pp. 263-268. IEEE (2021).

[21] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography,* 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437.

[22] Arvind Panwar & Vishal Bhatnagar. Analyzing the performance of data processing in private blockchain based distributed ledger, *Journal*

*of Information and Optimization Sciences*, 41: 6, 1407-1418 (2020), DOI: 10.1080 /02522667.2020.1809095.

[23] Pawan Kumar, Reshma, Kamal Kant Sharma & Abhishek Gandhar. A block-chain excellency in the mining of crypto currency, *Journal of Information and Optimization Sciences*, 43:1, 123-130 (2022), DOI: 10.1080/02522667.2022.2037281.

[24] Liang, Wenbing, and Nan Ji. "Privacy challenges of IoT-based blockchain: a systematic review." *Cluster Computing* 25, no. 3, 2203-2221 (2022).

[25] Kumar, Gulshan, Rahul Saha, Chhagan Lal, and Mauro Conti. "Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications." *Future Generation Computer Systems* 120, 13-25 (2021).