Article

Not peer-reviewed version

A New Evidence Preservation Forensics Model Using Blockchain and Stenography Techniques

Mohammad AlKhanafseh and Ola Surakhi *

Posted Date: 17 March 2024

doi: 10.20944/preprints202403.0703.v1

Keywords: Blockchain; Evidence Preservation, Forensics; Stenography

Article

A New Evidence Preservation Forensics Model Using Blockchain and Stenography Techniques

Mohammad AlKhanafseh [1] **and Ola Surakhi** [2,*]

[1] Birzeit University; malkhanafseh@birzeit.edu
[2] American University of Madaba
* Correspondence: o.surakhi@aum.edu.jo

Abstract: The adoption of technology and digital tools across various user groups has brought about a heightened risk of cyber-attacks targeting devices and shared data. These elevated levels of cybercrime necessitate thorough investigations to address victims' inquiries about the nature, causes, affected data, and impacted resources of the attack. Digital forensics serves as a crucial means to answer these queries. Additionally, it enables the formulation of strategies and delineation of roles essential for fortifying future defenses against such attacks. Within digital forensics, digital evidence holds pivotal importance in the investigative process as it serves as a cornerstone in legal proceedings to identify perpetrators. Numerous research endeavors focus on devising solutions to safeguard evidence, including centralized storage centers or cloud computing. These efforts aim to create frameworks integrating diverse security levels for sharing and preserving evidence effectively. In this paper, a new framework is proposed that seeks to amalgamate novel technologies with forensic practices to address challenges in the preservation phase of digital forensics. Strategies include segmenting evidence into smaller components, leveraging steganography to support preservation, and employing blockchain technology to ensure the integrity of collected evidence.

Keywords: blockchain; evidence preservation; forensics; stenography

1. Introduction

With an increasing reliance on digital devices, the performance of smart technology like smartphones and tablets continues to advance. This progress in smart devices has sparked significant demand among users of varying technical expertise. These devices are used both by individuals well-versed in technology and by those with limited or no background in this realm. Consequently, the incidence of crimes committed using these devices has risen considerably, necessitating thorough investigation processes, making the role of digital forensics increasingly pivotal.

Digital forensics involves investigating digital crimes, focusing on recovering, preserving, and analyzing electronic evidence crucial for supporting criminal inquiries. In this context, preserving evidence stands as a cornerstone of the investigative process. Given the ongoing surge in digital data production, ensuring the integrity, authenticity, and admissibility of digital evidence is more crucial than ever before, demanding robust solutions to prevent tampering.

Preserving evidence presents various challenges beyond mere retention; it entails ensuring the credibility of evidence throughout the investigation's lifecycle, from seizure to its presentation in court. Blockchain technology offers a decentralized and immutable ledger solution, ensuring highly secure and transparent records, timestamps, and preservation of digital evidence and related media in forensic investigations [1]. Integrating blockchain technology can elevate the forensic process by enhancing evidence collection, preservation, and analysis in digital forensics, ultimately refining the entire investigative procedure.

This paper endeavors to introduce a novel framework for preserving evidence in digital forensics. The proposed solution aims to bolster the security, privacy, and authenticity of digital evidence throughout the investigative process. It leverages various advanced solutions in cybersecurity, including steganography, blockchain, and cryptography, to fortify the investigation's integrity and efficacy.

1.1. Concepts of Blockchain Technology

Satoshi Nakamoto [1] introduced blockchain technology in a white paper in 2008 for the first time. Blockchain represents a decentralized peer-to-peer (P2P) network with a distributed ledger that is both immutable and transparent [2]. In this blockchain system, the distributed ledger takes the form of interconnected blocks, where each block is connected to the previous one through its cryptographic hash [3]. Each block is assigned a unique block number and a timestamp. Within each block, multiple transactions are structured in a Merkle tree format, and each transaction is secured through cryptographic signatures using an asymmetric digital key. The rules for managing and maintaining the distributed ledger are determined by a governance mechanism known as the consensus algorithm [4].

Blockchain can be either public or private. Public blockchains are accessible to everyone, allowing anyone to view the ledger. In contrast, private blockchains restrict ledger access to specific members. Permissionless blockchains enable anyone to engage in transactions and join the consensus process, whereas permission-based blockchains restrict these activities to chosen members [5]. To efficiently and securely encode blockchain data, a Merkle Tree is employed. Additionally, consensus algorithms play a crucial role in achieving synchronization and establishing agreement among the numerous nodes within a blockchain network [5].

A Merkle tree aggregates all the transactions within a block and creates a digital fingerprint representing the entire set of operations. This fingerprint enables users to verify the presence or absence of specific transactions within the block. The Merkle tree is structured as a binary tree, where each leaf node represents the hash of an individual transaction, and each non-leaf node represents the hash of a combination of its child nodes. Moreover, the Merkle tree's root serves as a means to verify the data within it. The Merkle root employs a straightforward mathematical process to validate the data contained in the Merkle tree [6].

The consensus algorithm plays a critical role in establishing the rules for maintaining the distributed ledger [7]. The consensus algorithm is essential to achieving unanimous agreement across the entire blockchain network when determining the validity of each individual block because, in a blockchain, there is no central authority responsible for validating transactions or blocks. The literature showcases a variety of consensus algorithms, each with its unique characteristics and implementations [8].

Proof-of-Work (PoW) is a consensus algorithm that is used in Bitcoin as well as Ethereum and imposes a requirement on the peers in the blockchain network to solve a challenging mathematical problem [9]. In a PoW system, blockchain validators continuously run the data from a block's header through a cryptographic hash function. With each iteration, validators incorporate a random number known as a nonce. Determining the data added to the next block in a blockchain using PoW necessitates significant energy consumption and computational resources. The participants competing to solve the problem and validate blocks in the PoW are referred to as miners. They are rewarded based on the computational resources they expend [10].

Many consensus algorithms have been developed in the literature to overcome PoW cost issues such as Proof of Stack (PoS), Delegated-Proof-of-Stake, Byzantine consensus algorithm, and more [11].

1.2. Digital Forensics

Digital forensics is the procedure of identifying, preserving, analyzing, and presenting digital evidence in a manner that meets the requirements for admissibility in a legal court, i.e. maintain the integrity of the collected evidence, ensuring its reliability and usability in a legal case [12]. The goal of a digital forensics' investigation is to preserve the evidence as it exists while also uncovering information that helps the investigator reconstruct past events and understand not just how, but also why, they occurred the way they did.

The digital forensic process entails five steps: identification, preservation, analysis, documentation, and presentation [13] as shown in Figure 1.

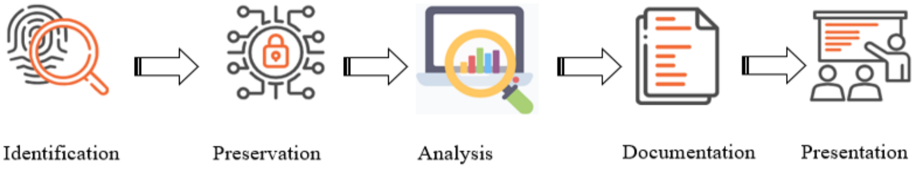


Figure 1. The digital forensics process.

Identification serves as the initial phase in any digital forensic investigation. During this stage, the investigator or investigative team is tasked with recognizing the scope of the evidence contained on the device, its storage locations, and the specific formats in which it is stored. Digital evidence can encompass a wide range of formats, such as text messages, emails, images, videos, web search histories, documents, transactions, and more. This evidence can be found on various devices, including computers, smartphones, tablets, fitness trackers, and numerous other digital platforms.

After identification, the next step in digital investigations is **preservation**. This phase involves the isolation and secure safeguarding of data, as well as the creation of a copy or image that can be subject to analysis and investigation. Preserving the original evidence in its unaltered state is crucial in digital investigations to ensure its admissibility as evidence in a court of law.

Analysis is the phase in a digital forensic investigation during which the forensic scientist or investigator pieces together fragmented data to construct a comprehensive narrative of the events that transpired during the crime or matter under investigation. Forensic experts primarily rely on the evidence, drawing from their experience and expertise. It often requires multiple attempts and examinations to formulate a well-substantiated theory about the unfolding of the crime.

Documentation involves the creation of a record that compiles the data to be presented in court or any other forum where the investigation is being resolved. It comprises a narrative reconstruction of the events in question, intertwined with the evidence that bolsters the theory. This documentation should be persuasive to an external party tasked with determining guilt or innocence.

Presentation marks the concluding phase of the digital forensic process. The investigator utilizes the documentation to articulate the conclusions they have drawn regarding the event in question. Whether the conclusion is conveyed in a courtroom or through a written report, the investigator's task is to translate their expert findings into a clear and comprehensible narrative that can be understood and assessed by individuals who are not experts in the field, relying on the details and evidence provided.

The investigative process commences immediately upon the incident being reported or a crime being detected [14]. Subsequently, the investigator proceeds through the steps depicted in Figure 1. Initially, the investigation commences with the identification of the machine or object associated with the alleged crime or violations. Once the crime is detected, the investigator begins gathering evidence from the objects identified as being involved in the offense. Following this, the investigator scrutinizes these objects and compiles a report detailing the findings. Ultimately, the last step involves reporting these findings and apprehending the suspect [15].

Computer Forensics Domains

The computer forensics domains can be divided into eight main eras as shown in Figure 2.

Operating System Forensics is the procedure of extracting valuable information from the operating system of a computer or mobile device under investigation [16].

The file system is of utmost importance in computing, as it ensures the organization and accessibility of data. Without it, files would become disorganized, making it impossible to determine their location, starting point, or endpoint. Each instance of a file system has a distinct size, but it can be processed by any computer supporting that particular file system type. Different file systems come with varying structures, logic, speed, flexibility, security, size, and other attributes [17]. File systems encompass key components such as filenames, directories, metadata, and space management. Analyzing a file system relies on the data contained within a partition or disk. This usually entails processing data to extract the contents of a file or retrieving the contents of a deleted file [18].

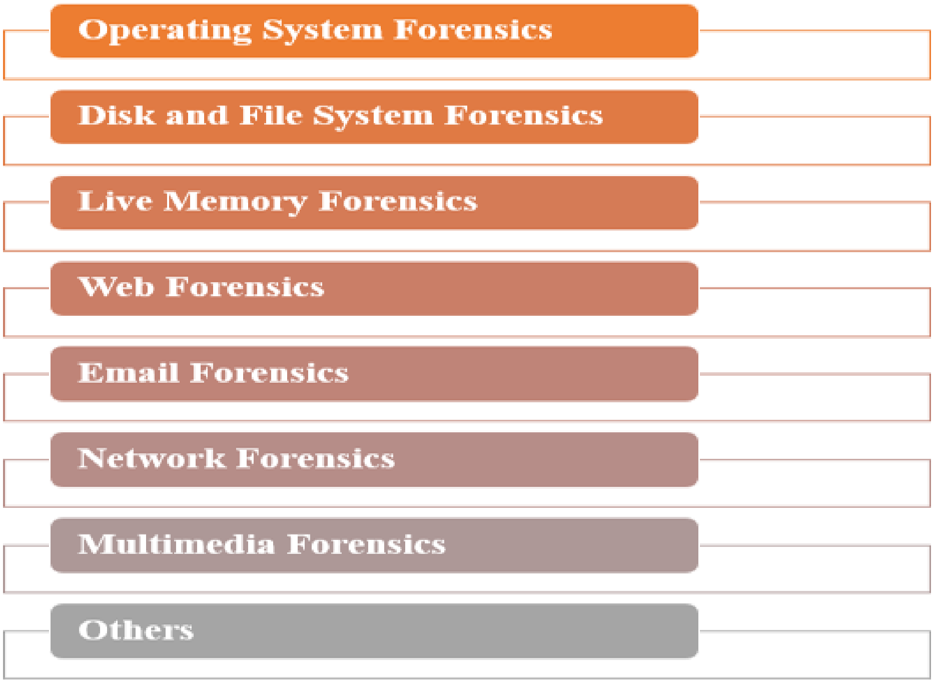


Figure 2. Computer Forensic Domains.

Live memory, RAM (Random Access Memory), facilitates the access and processing of various types of information, handles, open files, decrypted data, registry entries, user passwords, user activities, as well as connection and session details [19]. RAM permits data access in a manner that can unveil transparent information that might be otherwise concealed. This capability is instrumental in revealing hidden processes, detecting malware attempting to conceal information, and identifying the use of various toolkits [20].

In web forensics, forensic information can be obtained from various sources like web storage records, browsing sessions, search histories, and complete user activity logs. Each operating system (OS) and web browser has its unique method for retaining these records, which can be analyzed to trace and investigate criminal activities [21].

Email forensics is the process of gathering evidence from emails. Email serves as an electronic means of communication over the Internet, facilitating the exchange of messages, files, documents, and various transaction-related elements. This process involves the examination and analysis of email content to extract valuable information for investigative purposes [22].

Network forensic analysis centers on the monitoring of network traffic and the investigation of the sources of potential attacks. This process involves the collection and analysis of data related to network activities and events, intending to identify and mitigate security breaches or unauthorized access [23,24].

In contemporary times, digital visual media has become one of the primary modes of communication. Digital images are the subject of numerous digital investigations, as some of them may contain illicit content [25]. This type of analysis seeks to uncover details about the image's origin, including its location and the individuals depicted in it. Image analysis also involves scrutinizing images for potential evidence of steganography, which is the practice of concealing information within digital media.

There are various other domains within computer forensics. For example, cloud forensics is employed to investigate crimes committed using cloud platforms, focusing on digital evidence hosted in cloud environments. Database forensics, on the other hand, is used to examine data storage systems and address privacy-related crimes, involving the analysis of databases to uncover evidence of illicit activities.

The rising prevalence of cybercrimes worldwide, which vary in nature and complexity, including content forgery, financial data fraud, and even cyber terrorism involving large groups and government actors, has underscored the necessity for computer forensic algorithms, solutions, and tools. In response to these evolving and multifaceted threats, the development and advancement of forensic techniques and technologies have become imperative for effectively combating and investigating cybercrimes.

Blockchain technology has the potential to provide various applications for digital forensics investigations. These applications encompass evidence collection, preservation, validation, and analysis. Researchers and investigators can harness the capabilities of blockchain for digital forensics, as it allows for traceability and ensures the immutability of records. This can be particularly valuable in maintaining the integrity and reliability of digital evidence throughout the investigative process.

1.3. Stenography Technique

Steganography encompasses methods used to conceal confidential information within other digital media, essentially hiding it in plain sight. Some definitions characterize it as the practice of embedding one piece of information within another in a way that makes detection challenging, akin to a form of camouflage that remains unseen by unintended recipients or intruders [26]. Within the realm of information hiding techniques, steganography is regarded alongside methods like watermarks and cryptography [27]. The primary objective of these techniques is to ensure secure transmission and communication across insecure channels.

However, the goals of steganography differ from those of watermarks. Watermarks primarily aim to provide proof of ownership or identification, while steganography focuses on achieving confidentiality, integrity, and privacy through encryption. Notably, research indicates that steganography is utilized as an anti-forensics technique, enabling the hiding of evidence and complicating investigation processes [28]. Essentially, steganography operates differently from cryptography, which revolves around the art of rendering secret messages incomprehensible unless the specific key to decoding them is known.

Steganography, as a field, is broadly categorized into two primary divisions: linguistic steganography and technical steganography. Linguistic steganography involves concealing text within a text cover message, while technical steganography utilizes diverse types of media as cover messages.

The most common methods employed in steganography are Image steganography, text steganography, audio steganography, and video steganography. Each method uses a specific carrier or cover media. For instance, in text steganography [29], the carrier medium utilized is text. Within text steganography, the process of embedding a secret message into the carrier content can be executed through various techniques. These techniques might include altering spacing, selecting different fonts, or manipulating letter cases to conceal the hidden message within the text.

Indeed, the counterpart to steganography is steganalysis, which focuses on uncovering or detecting the embedded message within cover media. Steganalysis involves the investigation and detection of hidden data concealed using steganographic techniques. This field of study is generally divided into two primary categories.

Passive steganalysis aims to categorize a cover medium as either "stego" (having hidden data) or not and seeks to identify the steganographic embedding algorithm. On the other hand, active steganalysis goes a step further. In addition to determining whether a cover medium contains hidden data and identifying the embedding algorithm, active steganalysis endeavors to estimate the length of the embedded message and, ideally, extract it from the cover medium [30].

2. Related Works

The authors in [31] introduces an innovative framework known as the "Forensics Chain for Evidence Preservation System for IoT-based smart city security" to address the issues faced by forensic investigators, such as the risk of a single point of failure and potential evidence alterations. These issues arise when digital evidence is stored on cloud servers, it elevates the risk of evidence tampering and unauthorized sharing with malicious third parties.

In [32], the authors proposed a privacy-preserving digital forensics (P2DF) framework. The framework's objective is to safeguard the digital crime scene for subsequent validation through the synchronization and analysis of evidence. Following the confiscation of suspects' digital media, a thorough bit-by-bit imaging process is carried out on the original data contents. The integrity of the secure digital images is verified at each stage using MD5 or SHA-1 hash techniques to promptly detect any alterations in the copied image.

In [33], The authors have introduced a digital forensic framework that leverages case information, case profile data, and expert knowledge to automate the digital forensic analysis process. It also employs machine learning to identify the most pertinent evidence, all while safeguarding data privacy. This approach enhances the overall efficiency of digital forensic investigations without compromising the integrity and admissibility of the evidence.

In [34], the authors have put forth the "BEvPF-IoT" method, which is a framework for preserving multimedia evidence in the context of Internet-of-Things (IoT) devices. This method is based on blockchain technology. The framework includes the establishment of a secure and cost-effective environment through the utilization of IPFS and Ethereum blockchain. This implementation aims to improve network transparency and accountability during the forensic examination of digital multimedia evidence.

The authors in [35] introduced a blockchain-powered solution tailored for the smart home sector, addressing the tasks of gathering and safeguarding digital forensic evidence. The system employs a private forensic evidence repository to store collected evidence, alongside a permissioned blockchain framework that delivers security functionalities such as integrity, authentication, and non-repudiation.

The blockchain technology again used by the authors in [36] to provide a solution for evidence preservation of forensics technology. The proposed framework called IoTFC can deliver a guarantee of traceability and track provenance of evidence items. Details of evidence identification, preservation, analysis, and presentation will be recorded in chains of block. The IoTFC can increase trust of both evidence items and examiners by providing transparency of the audit train.

In [37], the authors proposed "ForensiBlock" which is a dedicated private blockchain solution. ForensiBlock guarantees thorough and transparent documentation throughout the investigative journey, encompassing stages such as data extraction, access control, and tracking of data versions.

The authors on [38] proposed a solution based on the theory of ontology to preserve the privacy in the area of digital forensics by abstracting the privacy attributes in digital forensics scenarios.

The authors in [39] proposed a practical and secure CustodyBlock (CB) model, which employs a private blockchain protocol and smart contracts. This model is designed to facilitate the management, transfer, analysis, and monitoring of evidence in a reliable manner. The integration of smart contracts within CB serves to automate and enhance the evidence preservation and handling processes, making them more efficient and secure.

By analyzing the previous works, it can be said that the advancement of blockchain technology, with its inherent qualities of integrity and immutability, has spurred the development of numerous solutions for the privacy preservation of forensic evidence. Many innovative solutions have emerged, harnessing blockchain's capabilities to safeguard sensitive data and transactions, ensuring their authenticity and preventing unauthorized alterations. This shift towards blockchain-based solutions reflects the growing recognition of the technology's potential to provide robust privacy preservation for forensics technology.

3. The Proposed Model

The proposed model consists of five main parts as shown in Figure 3:

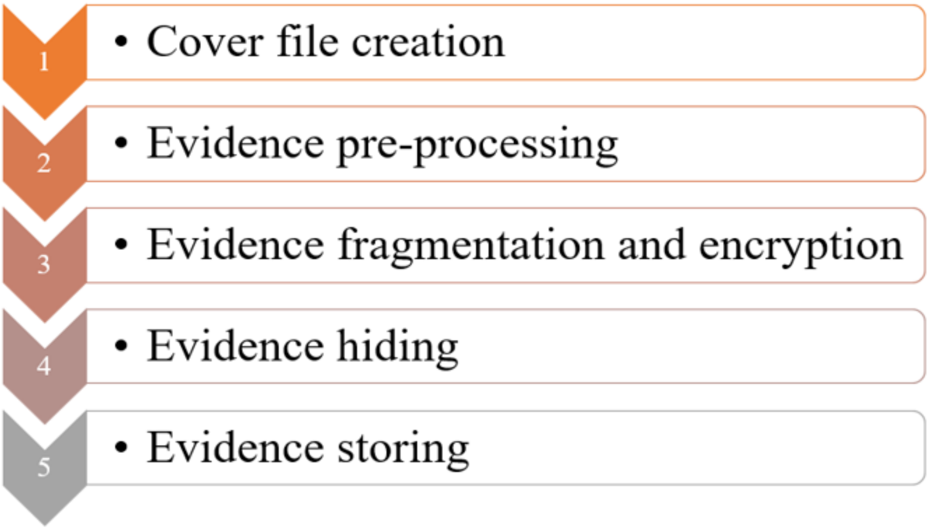

1
• Cover file creation
2
• Evidence pre-processing
3
• Evidence fragmentation and encryption
4
• Evidence hiding
5
• Evidence storing

Figure 3. The Proposed model.

The blockchain technology is used in the proposed model as a distributed database for evidence storing. Blockchain is a well-known technology to store data in a secure and decentralized manner. Decentralized blockchains are immutable, which means that the data entered is irreversible.

The data are stored in blocks linked together. When the block reaches its capacity, the data undergoes encryption through an algorithm, resulting in the generation of a hexadecimal number known as a hash. This hash is subsequently incorporated into the header of the next block and combined with the remaining data within that block. This process forms a sequence of interconnected blocks, creating a chain of information.

In the proposed model, the data extracted from the previous block in the blockchain is utilized to create the initial cover file. This is accomplished by employing an encryption algorithm to produce a cipher file with a predetermined size, which is determined by the block size in the blockchain. This process constitutes the initial phase.

The cipher file will be utilized in the third phase of our model to conceal forensic evidence within it and create the steganography file. Before that, the collected evidence is assembled for the preprocessing phase. During this phase, the evidence is organized into groups according to their data types, which could be image, text, video, PDF, etc. A machine learning method is used in this phase to achieve its goal; cleaning and transforming the evidence data. This step is important to correcting or eliminating inaccurate, compromised, improperly structured, redundant, or incomplete data. This may lead to correctly map different functions with the intended purpose of the data. And reduce the size of the data.

Subsequently, the third phase commences, during which each piece of evidence is divided into a set of chunks equal to 10. Then, each individual chunk of the same evidence undergoes the identical encryption algorithm employed for encrypting block data and producing cipher file encryption. This encryption process serves the dual purpose of concealing the original data and augmenting security measures.

The steganography phase initiates, where the set of encrypted chunks is embedded into the cipher file to conceal them, resulting in the creation of transaction data to be stored within the blockchain in the form of a steganography file. Lastly, the generated file is stored in the blockchain database following the execution of the blockchain mining process. The key features of the proposed model can be summarized as follows:

1. Ensure a heightened level of integrity, confidentiality, and privacy for digital evidence.
2. Employing a solution like blockchain offers an immutable safeguard, ensuring that any attempt to tamper with the content of a single piece of evidence would necessitate extensive effort.
3. Utilizing steganography techniques to conceal evidence in forensics is crucial due to its capacity to obscure sensitive information within seemingly innocuous data The details of each step are given below.

Cover File Creation

During this stage, the objective is to generate a cover file that will serve as a steganography container for concealing evidence within it. This is accomplished by obtaining the data from the preceding block within the blockchain and subsequently encrypting it using a designated encryption algorithm as shown in Figure 4. The size of the generated cipher file is calculated to be used later in the third phase of the model.

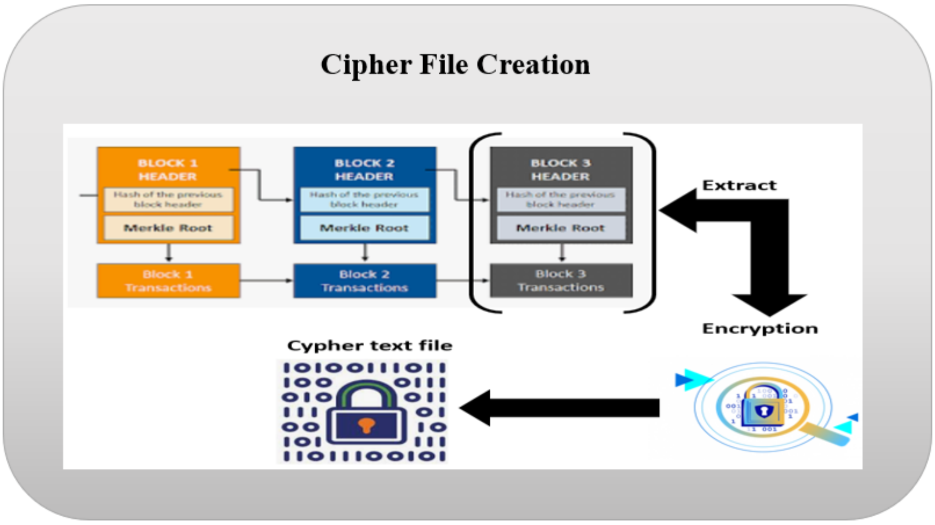


Figure 4. Cover File Creation Phase.

Evidence Pre-processing

From the pool of evidence available, a specific piece stands out as the starting point for initiating the preservation process. After receiving the evidence, it undergoes a series of preprocessing procedures to be categorized into the appropriate data set based on its type. Every set of evidence is regarded as a memory pool within the blockchain, housing a collection of unconfirmed transactions. The memory pool is a data structure that holds the evidence that has not yet been included in the mining process.

During this stage, each evidence undergoes a series of data preprocessing procedures. The evidence can exist in various formats, including text, images, audio, video, and more. To manage these diverse data types, protocols can be implemented for regulation. In our proposed model, we handled two main data types: text and image. First, we integrate and organize a set of evidence of the same data type into one group such that the text data in one group and the image data in another group. Then, each group goes through a sequence of cleaning and transformation operations to transfer the data into useful information. This can be done by using machine learning methods. In the case of image data, the image data undergoes an additional pre-processing phase wherein it is subjected to compression after the initial data cleaning. This compression step aims to reduce the image size by eliminating redundant data. In the end, the volume of the data will be reduced and the errors, outliers, and redundant data will be removed. Two sets of consistent data will be generated.

Evidence Fragmentation and Encryption

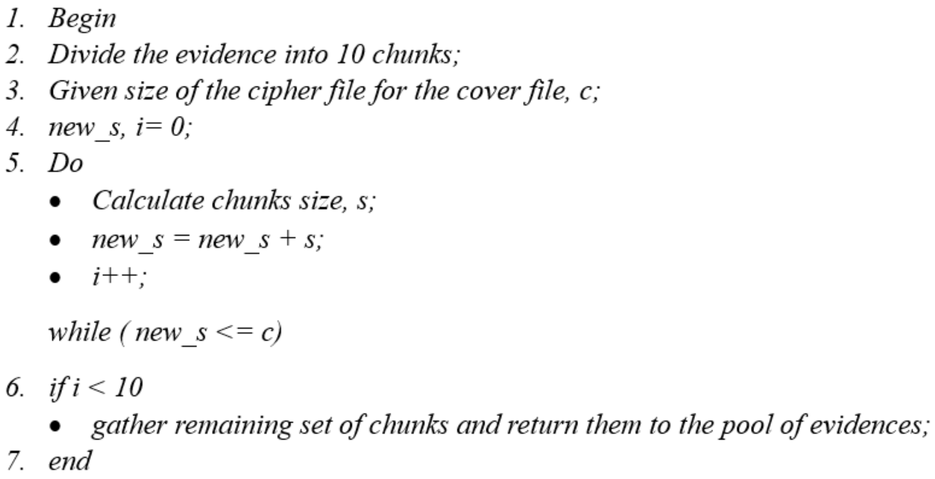
Upon completing the data preparation process, the evidence is fragmented and divided into smaller files known as chunks. This process is carried out by executing the algorithm outlined in Figure 5 for data fragmentation and encryption.

Initially, the data is partitioned into ten distinct chunks. Each of these chunks is then encrypted using the identical algorithm employed for encrypting the cover file in the initial phase of our model. Subsequently, the size of each encrypted chunk is determined, and these individual sizes are summed to yield the total size of the encrypted set of chunks. Next, a comparison is conducted between the size of the cipher file for the cover file and the total size of the encrypted set of chunks.

The ratio between the total size of the encrypted set of chunks and the size of the cipher file for the cover file is evaluated as follows:

$$r = \frac{\sum_{i=1}^{10} \text{chunk size}}{\text{cipher\_file}} \tag{1}$$

if r >1, then the total size of the encrypted set of chunks is greater than the size of the cipher file for the cover file. In this scenario, the number of chunks chosen to progress to the next phase is determined in a manner that ensures the total size of the selected chunks is less than the ciphertext file. If any remaining chunks are not selected, these chunks will be placed back into the memory pool, where they can be chosen again for inclusion in the subsequent block of the blockchain during a fresh iteration of the proposed model.



```
1.  Begin
2.  Divide the evidence into 10 chunks;
3.  Given size of the cipher file for the cover file, c;
4.  new_s, i= 0;
5.  Do
        •  Calculate chunks size, s;
        •  new_s = new_s + s;
        •  i++;
    while ( new_s <= c)
6.  if i < 10
        •  gather remaining set of chunks and return them to the pool of evidences;
7.  end
```

Figure 5. The chunks fragmentation and encryption algorithm.

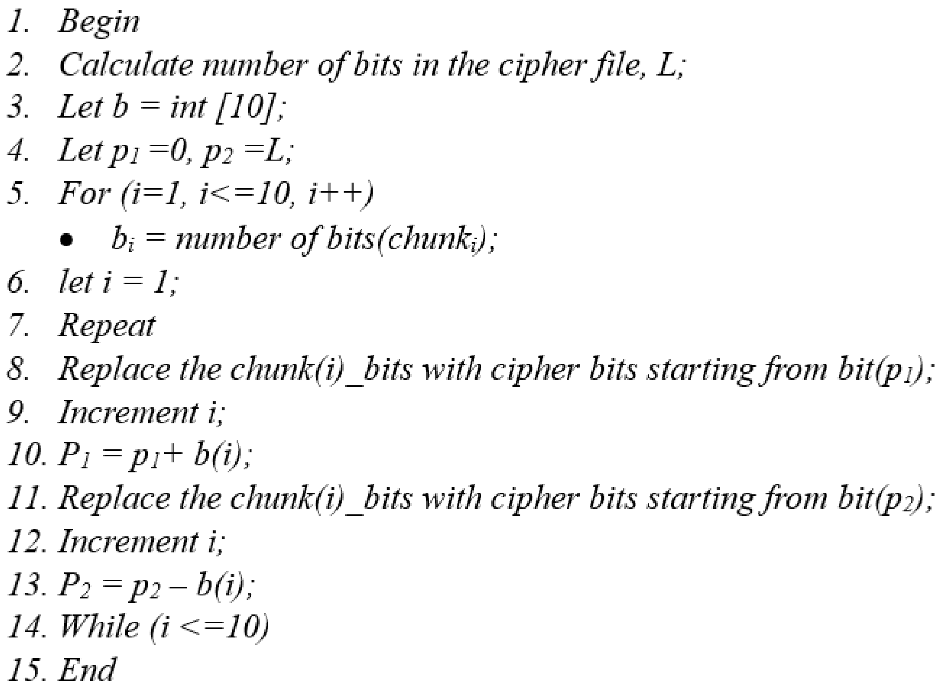
Evidence Hiding

In this phase, the cipher file prepared during the initial stage will be employed to conceal the encrypted set of evidences and create steganography file. The cipher file and the set of chunks share the same data type, as they are both encrypted using the same algorithm. Additionally, the size of the set of chunks is either less than or equal to the size of the cipher file. This implies that, after concealing the information within the cipher file, the resulting file should retain the same data type and size. Achieving this can be accomplished by substituting a set of bits in the cipher file with the bits from each chunk. This replacement operation is iterated for all 10 chunks. Here two parameters should be determined: the starting position of the bit to be replaced and the number of bits in the cipher file of covered file. To achieve that, we must determine the number of bits in the cipher file and the set of chunks.

The number of bits in a text can be determined by considering the character encoding used and the length of the text. To calculate it, we follow the following steps:

1. **Character Encoding:** First, we should determine the character encoding used for the text. Common character encodings include ASCII, UTF-8, UTF-16, and others. Each encoding uses a different number of bits to represent characters.
2. **Text Length:** Determine the length of the text in characters.
3. **Calculate Bits:** Once we determine the character encoding and the text length, we can calculate the number of bits as follows:
    - In ASCII, each character is represented using 7 or 8 bits.
    - In UTF-8, the number of bits per character can vary, with English letters typically using 8 bits.
    - In UTF-16, each character is typically represented using 16 bits.
4. So, to find the number of bits in a text, we multiply the number of characters by the number of bits required to represent each character in the chosen encoding. For example, for 100 characters in UTF-8 encoding, we will have 800 bits (100 characters * 8 bits per character).

The algorithm for generating the stenography file and hide the chunks is given in Figure 6.



```
Begin
Calculate number of bits in the cipher file, L;
Let b = int [10];
Let $p_1$ =0, $p_2$ =L;
For (i=1, i<=10, i++)
    • $b_i$ = number of bits($chunk_i$);
let i = 1;
Repeat
    Replace the chunk(i)_bits with cipher bits starting from bit($p_1$);
    Increment i;
    $P_1 = p_1 + b(i)$;
    Replace the chunk(i)_bits with cipher bits starting from bit($p_2$);
    Increment i;
    $P_2 = p_2 – b(i)$;
While (i <=10)
End
```

Figure 6. Hiding algorithm.

Where b is a one-dimensional array with length 10. $b[i]$ contains the length of the ith chunk. $P1$ and $P2$ are two pointers in the cipher file bits. Initially, $P1$ points to the first bit in the cipher file and $P2$ points to the last bit in the cipher file. Hiding the chunks within the cipher file is accomplished in both forward and reverse directions. The procedure involves replacing the bits of the first chunk with those from the cipher file, starting from the first bit and continuing until all the bits in the first chunk have been replaced. Following this, the pointer value $P1$ is incremented by the number of chunk bits, which is stored in the $b[i]$ location. Subsequently, the second chunk is substituted with bits from the cipher file. However, in this case, the replacement process commences from the end of the cipher file, proceeding backward until all the bits of the second chunk have been replaced. During this step, the value of $P2$ is decremented by the number of bits in the second chunk, which is also saved in the b array. This process is repeated until the hiding process for all chunks of evidence is completed. The output of this phase is the steganography file that contains the set of evidence chunks encrypted by the encryption algorithm and hidden in the ciphertext file.

Evidence Storing This phase involves the adding of the stenography file to the blockchain as a regular transaction. This includes the verification process which is the mining in the blockchain to add the data into a block. A unique cryptographic hash value is created for the new block to identify it. The blocks contain information such as transaction (stenography file), nonce, target bit, difficulty, timestamp, previous block hash, current block hash, and block ID, etc., and the blocks are cryptographically verified and chained up to form an immutable chain which is the blockchain.

The overall architecture of the proposed model is shown in Figure 7.

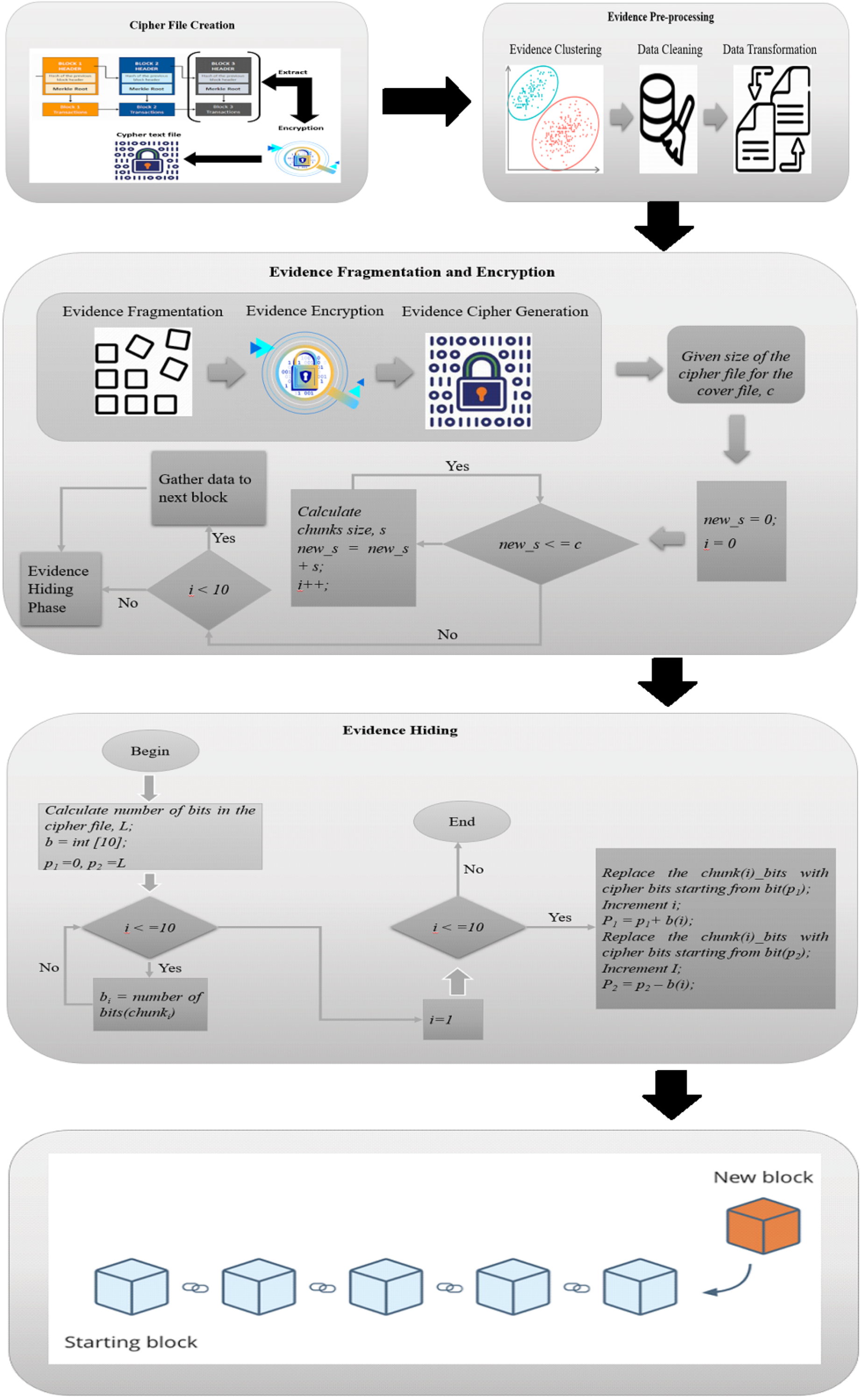


Figure 7. The overall architecture of the proposed model.

4. Conclusions and Future Works

This paper proposed a model with different levels of security for the preservation of evidence and secure sharing amongst various investigators and courts. The first level refers to using the idea of dividing the evidence over a set of chunks, which gives the solution level of complexity; the second level refers to distributing the chunks over a set of blocks, whereas the size of the blocks is identical, and the chunks will be embedding over the blocks using the idea of steganography, and based on the idea of blockchain since the chunks will be embedded over the ciphertext of the content of the preceding block. The proposed solution takes advantage of recent technology in the field of cybersecurity by using blockchain, steganography, and encryption to reach a situation where if the evidence is shared and distributed amongst different investigators and courts of law, it will be safe.

For future works, the authors will implement the proposed model on a forensic dataset. With the practical implementation of the proposed model to a diverse range of forensic scenarios and datasets, the authors aim to validate its robustness and efficacy in preserving evidence and facilitating secure sharing among investigators and legal entities. This hands-on approach will not only enhance the credibility of this research but also contribute valuable insights towards the development of more secure and efficient methods for handling digital evidence in forensic contexts.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized business review* (2008).
2. Sun, Ruo-Ting, Aravinda Garimella, Wencui Han, Hsin-Lu Chang, and Michael J Shaw. "Transformation of the transaction cost and the agency cost in an organization and the applicability of blockchain—A case study of Peer-to-Peer insurance." *Frontiers in Blockchain* 3 (2020): 24.
3. Hepp, Thomas, Patrick Wortner, Alexander Schönhaals, and Bela Gipp. "Securing physical assets on the blockchain: Linking a novel object identification concept with distributed ledgers." In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 60-65. 2018.
4. Surakhi, Ola M, and Mohammad Y AlKhanafseh. "Review on the Application of Blockchain Technology to Compact COVID-19 Pandemic." In *2021 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pp. 193–198. IEEE, 2021.
5. Tripathi, Ashish Kumar, K Akul Krishnan, and Avinash Chandra Pandey. "A Novel Blockchain and Internet of Things-Based Food Traceability System for Smart Cities." *Wireless Personal Communications* 129.3 (2023): 2157-2180.
6. Nguyen, Hai Nam, Hai Anh Tran, Scott Fowler, and Sami Souihi. "A survey of Blockchain technologies applied to software-defined networking: Research challenges and solutions." *IET Wireless Sensor Systems* 11.6 (2021): 233-247.
7. Viriyasitavat, Wattana, and Danupol Hoonsopon. "Blockchain characteristics and consensus in modern business processes." *Journal of Industrial Information Integration* 13 (2019): 32-39.
8. Bamakan, Seyed Mojtaba Hosseini, Amirhossein Motavali, and Alireza Babaei Bondarti. "A survey of blockchain consensus algorithms performance evaluation criteria." *Expert Systems with Applications* 154 (2020): 113385.
9. Sriman, B, S Ganesh Kumar, and P Shamili. "Blockchain technology: Consensus protocol proof of work and proof of stake." In *Intelligent Computing and Applications: Proceedings of ICICA 2019*, pp. 395-406. Springer, 2021.
10. Majeed, Umer, Latif U Khan, Ibrar Yaqoob, SM Ahsan Kazmi, Khaled Salah, and Choong Seon Hong. "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges." *Journal of Network and Computer Applications* 181 (2021): 103007.
11. Ge, Lina, Jie Wang, and Guifen Zhang. "Survey of consensus algorithms for proof of stake in blockchain." *Security and Communication Networks* 2022 (2022): 1-13.
12. Atlam, Hany F, Ahmed Alenezi, Madini O Alassafi, Abdulrahman A Alshdadi, and Gary B Wills. "Security, cybercrime and digital forensics for IoT." In *Principles of internet of things (IoT) ecosystem: Insight paradigm*, pp. 551-577. Springer, 2020.

13. Selamat, Siti Rahayu, Robiah Yusof, and Shahrin Sahib. "Mapping process of digital forensic investigation framework." *International Journal of Computer Science and Network Security* 8.10 (2008): 163-169.
14. Englbrecht, Ludwig, and Günther Pernul. "A privacy-aware digital forensics investigation in enterprises." In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1-10. 2020.
15. Javed, Abdul Rehman, and Zunera Jalil. "Byte-level object identification for forensic investigation of digital images." In *2020 International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1-4. IEEE, 2020.
16. Garfinkel, Simson L. "Digital forensics research: The next 10 years." *Digital Investigation* 7 (2010): S64–S73.
17. da Silveira, Claudinei Morin, Rafael T. de Sousa Jr, Robson de Oliveira Albuquerque, Georges D Amvame Nze, Gildásio Antonio de Oliveira Júnior, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba. "Methodology for forensics data reconstruction on mobile devices with Android operating system applying in-system programming and combination firmware." *Applied Sciences* 10.12 (2020): 4231.
18. Sudhakar, and Sushil Kumar. "An emerging threat Fileless malware: a survey and research challenges." *Cybersecurity* 3.1 (2020): 1.
19. Palutke, Ralph, Frank Block, Patrick Reichenberger, and Dominik Stripeika. "Hiding process memory via anti-forensic techniques." *Forensic Science International: Digital Investigation* 33 (2020): 301012.
20. Hausknecht, Kresimir, D Foit, and J Burić. "RAM data significance in digital forensics." In *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1372-1375. IEEE, 2015.
21. Nelson, Rebecca, Atul Shukla, and Cory Smith. "Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle." *Digital Forensic Education: An Experiential Learning Approach* (2020): 219–241.
22. Ghafarian, Ahmad. "An empirical analysis of email forensics tools." *Available at SSRN 3624617* (2020).
23. Javed, Abdul Rehman, Saif Ur Rehman, Mohib Ullah Khan, Mamoun Alazab, and Thippa Reddy. "CANintelliIDS: Detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU." *IEEE Transactions on Network Science and Engineering* 8.2 (2021): 1456–1466.
24. AlKhanafseh, Mohammad Y, and Ola M Surakhi. "VANET Intrusion Investigation Based Forensics Technology: A New Framework." In *2022 International Conference on Emerging Trends in Computing and Engineering Applications (ETCEA)*, pp. 1–7. IEEE, 2022.
25. Quan, Yijun, Chang-Tsun Li, Yujue Zhou, and Li Li. "Warwick image forensics dataset for device fingerprinting in multimedia forensics." In *2020 IEEE International Conference on Multimedia and Expo (ICME)*, pp. 1–6. IEEE, 2020.
26. Yari, Imrana Abdullahi, and Shahrzad Zargari. "An overview and computer forensic challenges in image steganography." In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 360–364. IEEE, 2017.
27. Barbier, Morgan, Jean-Marie Le Bars, and Christophe Rosenberger. "Image watermarking with biometric data for copyright protection." In *2015 10th International Conference on Availability, Reliability and Security*, pp. 618–625. IEEE, 2015.
28. Muh, Hajar Akbar, Imam Riadi, et al. "Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework." *International Journal of Advanced Computer Science and Applications* 11.11 (2020).
29. Majeed, Mohammed Abdul, Rossilawati Sulaiman, Zarina Shukur, and Mohammad Kamrul Hasan. "A review on text steganography techniques." *Mathematics* 9.21 (2021): 2829.
30. Karampidis, Konstantinos, Ergina Kavallieratou, and Giorgos Papadourakis. "A review of image steganalysis techniques for digital forensics." *Journal of Information Security and Applications* 40 (2018): 217–235.
31. Kamal, Randa, Ezz El-Din Hemdan, and Nawal El-Fishway. "Forensics chain for evidence preservation system: An evidence preservation forensics framework for internet of things-based smart city security using blockchain." *Concurrency and Computation: Practice and Experience* 34.21 (2022): e7062.
32. Abulaish, Muhammad, Nur Al Hasan Haldar, and Jahiruddin Jahiruddin. "P2DF: A Privacy-Preserving Digital Forensics Framework." *International Journal of Digital Crime and Forensics (IJDCF)* 13.6 (2021): 1-15.
33. Verma, Robin, Jayaprakash Govindaraj, and Gaurav Gupta. "DF 2.0: Designing an automated, privacy preserving, and efficient digital forensic framework." (2018).

34. Malik, Aruna, Ajay K Sharma, and others. "Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things." *Journal of Information Security and Applications* 77 (2023): 103579.
35. Brotsis, Sotirios, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Dimitris Kavallieros, Emanuele Bellini, and Clément Pavué. "Blockchain solutions for forensic evidence preservation in IoT environments." In *2019 IEEE conference on network softwarization (NetSoft)*, pp. 110-114. IEEE, 2019.
36. Li, Shancang, Tao Qin, and Geyong Min. "Blockchain-based digital forensics investigation framework in the internet of things and social systems." *IEEE Transactions on Computational Social Systems* 6.6 (2019): 1433-1441.
37. Akbarfam, Asma Jodeiri, Mahdieh Heidaripour, Hoda Maleki, Gokila Dorai, and Gagan Agrawal. "ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability." *arXiv preprint arXiv:2308.03927* (2023).
38. Wan, Xuejiao, Jingsha He, Na Huang, and Yonghao Mai. "Ontology-Based Privacy Preserving Digital Forensics Framework." *International Journal of Security and Its Applications* 9.4 (2015): 53-62.
39. Alruwaili, Fahad F. "Custodyblock: A distributed chain of custody evidence framework." *Information* 12.2 (2021): 88.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.