# The Art of Piecewise Hashing: A Step Toward Better Evidence Provability

Aswin Gopalakrishnan[1], Emanuele Vineti[2],
Ashok Kumar Mohan[1] and M. Sethumadhavan[1]

[1] *TIFAC-CORE in Cyber Security, Amrita School of Engineering,*
*Amrita Vishwa Vidyapeetham, Coimbatore, India*
[2] *Vrije University, the Netherlands*
*E-mail: aswinkgopan@gmail.com; emanuele.vineti@gmail.com;*
*m_ashokkumar@cb.amrita.edu; m_sethu@cb.amrita.edu*

Received 03 January 2018; Accepted 21 March 2018;
Publication 26 April 2018

## Abstract

The integrity of digital evidence is believed to be the paramount trait in the world of cyber forensics. Cybercrime investigators face myriad challenges in the process similar to accommodating the call for bulk digital evidence. In due course extraction of useful information while maintaining the integrity and absolute protection against data degradation is mandatory. In this manuscript, we propose a novel approach by applying cryptographic hashing technique to only selected significant portions of the digital evidence, so even if the overall hash does not match, investigators could still verify the integrity of those critical sections of the evidence. We put forward two notions in this manuscript; former is heterogeneous piecewise hashing which is a flexible version of the piecewise hashing strategy, and latter is a novel evidence certification strategy which formalizes evidence provability process completely.

**Keywords:** Hashing, Piecewise, Acquisition, Certificate, admissibility, Litigation, Artifact, Corruption, Validation, Authenticity, Memory-block.

*Journal of Cyber Security and Mobility, Vol. 7_1,* 109–130. *River Publishers*
doi: 10.13052/jcsm2245-1439.719

## 1 Introduction

Forensics examiners work on dozens of evidence every day, and they have to follow strict procedures for each of them. They have to ensure the admissibility of the analyzed evidence to be presented to the court. Some digital evidence is very crucial in criminal investigations, and its corruption could assist dangerous malefactors to escape conviction by law.

One another issue is the lack of standardization in the process of evidence provability mainly due to the different legislation in each country, and often forensic investigator's best practices are questioned during court proceedings. Further to escape conviction from the law, the defendant often claims the evidence to be tampered by forensic examiner especially when the used forensic methods seem unorthodox to the court. This brings us to the question of the integrity of digital evidence because if an examiner inadvertently creates a single bit flip in the original evidence, it will be discarded by the court. Proving the integrity of parts of digital artifacts will be one of the primary goals in this paper.

Digital Forensic experts perform various hashing techniques to verify the integrity of any digital objects. They use hashing mainly for two reasons. If there is even a single bit change in the content, the original hash will also change. Secondly, it is collision resistance. Integrity is one of the critical aspects of digital evidence provability, especially with the exponential growth of the digital data and expanding cybercrimes which result in accumulation of digital evidence on a daily basis. The governments store these pieces of evidence while preserving integrity along with other fundamental information for their admissibility. It is apparent that at some point in time, the process of maintaining everything will become expensive and impractical. Also, one should consider the storage devices which preserve these artifacts will eventually get corrupted due to natural factors like aging. The only practical solution would be to create an exact backup copy of the original evidence. The admis-sibility of this copy is still a big problem because the present law doesn't apply to the volatile nature of the digital evidence and the court accepts only the original rather than the true copy of the evidence.

Our research tries to address and propose a solution to the problems mentioned above. We discuss the digital evidence admissibility and inadmissibility thoroughly along with the leading causes of evidence corruption. We prescribe (1.) a standard provability procedure for the digital artifacts, (2.) a novel technique which improves existing piecewise hashing by identifying corrupted and uncorrupted parts of digital objects, (3.) Digital Evidence

Integrity Certificate (DEIC), a compact representation of all the provability information.

We structure this proposal in the following way. In Section 2, we describe the existing forensics process, the various hashing functions and the notion of digital evidence admissibility. In Section 3 we discuss the probable causes for digital evidence corruption. In Section 4 we present our method which improves the existing evidence provability process. In this section, we first formalize the forensic workflow to ensure admissibility of evidence, and later we introduce a new sub-hashing strategy called *Heterogeneous Piecewise Hashing*. In Section 5, we present our new *Digital Evidence Integrity Certificate (DEIC)* which describes the application of our proposed provability process. In this section, we first formalize the provability process and then applying our proposal and then concluding with its verification. In the end we conclude with Sections 6, 7 and 8 with the related works, future works and conclusions.

## 2 Digital Forensics Background

### 2.1 The Digital Forensics Process

According to the Digital Forensics Research Workshop, the digital forensics process can be divided into several stages [16] (see Figure 1).

- **Identification**: Assessment of the digital evidence that is useful to the case. This step includes the preliminary analysis of the technical instrumentation and procedures needed for the acquisition phase.
- **Preservation**: Main focus of this stage is to freeze the crime scene preventing the source from data corruption through physical or software means.
- **Collection**: Every device or digital evidence identified must be collected following a strict methodology to avoid any possible alteration of the original evidence.
- **Extraction**: An examination process has to be done on the collected evidence to identify the artifact for the analysis phase.
- **Analysis**: The recovered data need to be interpreted and organized in a logical and structured form and finally draw objectives and conclusion from it.
- **Presentation**: All the discoveries from the analysis need to be documented and summarized as a report [19].

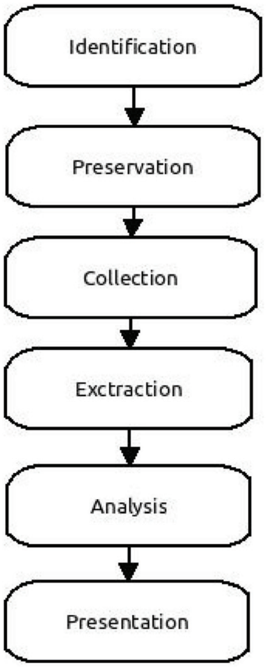

**Figure 1** Benchmarking digital forensic model.

## 2.2 The Acquisition Procedure

Data acquisition is the act or process of gathering information and evidence from a digital artifact [10]. During acquisition, the investigator should aim to preserve the integrity of the evidence as only the original evidence is admissible in court. Every analysis should be carried out on an exact copy of the original data which is verifiable through hashing digests. We classify data acquisition into two main categories. *Live Acquisition* which is a process of extracting live, real-time data before shutting down the system thereby preserving memory, network and process information. *Dead Acquisition* is when data retrieved is a nonvolatile source like a storage device where data remain part of the device after the device has been turned off. The latter has been the most common and safest form of acquisition in digital forensics. The Figure 2 demonstrates the steps needed to retrieve data from a storage device safely. First, the device needs to be connected to a forensics expert's machine through a hardware write-block device to avoid the risk of damaging the original data with unintended writes. Once the setup is ready, make an

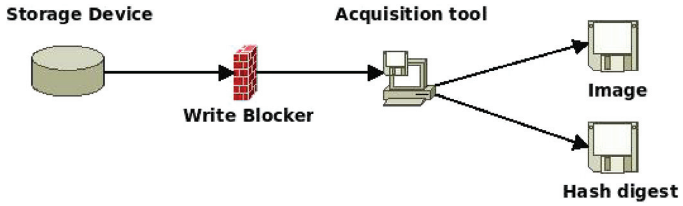

**Figure 2** Dead acquisition model.

exact copy of the disk content block by block using a data acquisition tool. The output of this procedure would be the true copy of the data and its hash digest.

### 2.3 Digital Evidence Admissibility

Hashing for integrity checking is one of the common methods to ensure admissibility in court, but there are other aspects to evidence admissibility further highlighted below.

#### 2.3.1 Relevance and admissibility

Relevance and admissibility are two crucial aspects considered when collecting and analyzing digital evidence. Both aspects need to be achieved to have strong evidence in front of the court [20].

- **Relevant**: If either proves or disprove facts in a case.
- **Admissible**: If it meets all regulatory and statutory requirements and its acquisition adheres to the best practices of digital forensics.

#### 2.3.2 Evidence in-admissibility

We summarize the main reasons to evidence inadmissible below.

1. The collection of the evidence has been conducted without the proper permissions or in general illegally
2. The evidence has been modified unintentionally or intentionally from the investigators
3. The digital forensics process applied to the evidence cannot be justified or transparently explained to the court
4. Not tracking the custody of the evidence or some parts of it have been missing.

### 2.3.3 Ensure admissibility

Now that we have pointed the potentials inadmissibility reasons, to avoid them we consider the following solutions:

1. **Legal Considerations**: The investigator needs to have granted the permission from the law enforcement to conduct an investigation.
2. **Integrity provability**: The investigator needs to follow some best practice procedure to avoid any modification of the original data 2.2. The integrity of the evidence can be proved to compute a mathematical hashing of the original evidence immediately after acquisition.
3. **Forensics process explainability**: The investigator needs to be able to justify and explain the forensic procedures. Most importantly, the results need to reproducible.
4. **Chain of custody**: This documentation includes every movement and procedure applied to evidence from the time its acquisition to submission courtroom.

## 2.4 Digital Evidence Types

Digital evidence - Information and data of value to an investigation stored on, received or transmitted by an electronic device [6, 8]. This digital evidence is acquired when the law enforcement confiscates the digital equipment and performs forensic examination over it. There are four properties of any digital evidence [9]:

- The information is not openly available and hence needs to be extracted
- Its moves jurisdictional borders quickly
- It could be easily contaminated or destroyed
- It is time sensitive thus, evidence which is crucial to an investigation today, may not have any relevance later.

Although there are many sources [36] of digital evidence, for this proposal we wish to focus on digital evidence categories: memory/disk images and media types (audio, video, and pictures) are the types of digital artifacts acquired during forensic investigations.

# 3 Identifying Causes of Evidence Corruption

Data corruption refers to phenomenon of causing unintended changes to the original data when it undergoes operations like writing, reading, storage, transmission, and processing, i.e., when a corrupted file is fed into a system or to a related application for processing, it could result in unexpected outcomes like system crashing, application malfunction or file corruption. Aforementioned is the description of data corruption in a general sense, but our focus is on understanding, its relevance concerning a forensic investigation. Wikipedia defines digital forensics as the data stored or transmitted using a computer or related device or media that supports or refutes a legal element or a requirement. We discuss the principal causes of data corruption in digital forensics [7].

- **Negligent Spoliation**: This kind of corruption appears due to the negligence of the forensic officers-in-charge. Officers with good knowledge of computer and electronics sometimes don't attend the initial investigation at the scene of the crime. Moreover, the officers investigating the initial crime-scene are sometimes technically incompetent, and they might overlook or unwittingly contaminated the electronic evidence.
- **Intentional Spoliation**: During forensic investigations, the pieces of evidence are possibly altered by criminals to disprove its integrity in court. Although, if the defendant is found to be guilty of evidence destruction, he/she is subject to incarceration or fine. Such intentional spoliation is referred to court as ”spoliation inference” which is a negative evidential inference drawn by the judge when the party is found guilty of evidence spoliation relevant to the ongoing investigation.
- **Static Electricity**: This corruption is the result of improper storage of the evidence. ESD (electrostatic discharge) occurs when the charge from hand or metals finds a path of least resistance and affects the digital evidence. Therefore, practitioners usually preserve the integrity of an electronic artifact by storing them in anti-static bags. Each of these antistatic bags has a unique identification number, also recorded in the chain of custody document.
- **Data Degradation**: Data decay or data rot is due to the gradual corruption of digital evidence. Every digital storage device has a lifetime, and gradually due to the accumulation of hardware failures, data containing get corrupted eventually. Although most high-end disk drives [4] suffer only a few unrecoverable errors, however with growing disk capacity and larger file sizes, the chance of data decay and other forms of uncorrected and undetected data corruption could gradually increase.
- **In-different priorities of incident response and computer forensics teams**: In the event of cybercrime in organizations, two teams rush to the crime-scene, the incident-response team, and the cyber forensic team. The incident response focuses on getting the cyber-criminals out of their

network and bringing the system back online quickly whereas forensic investigators try to preserve the evidence and find the traces left by the attackers. Most often, incident response, in their haste to bring the system back online, destroy and compromise evidence which could have helped the forensic investigators to identify the attackers [34].

- **Booby-traps in Digital Evidence**: Booby-trap is a software, device, a configuration of the device or the combination of all of them intended to destroy the target which could be a file, device, hard-disk or only to make the forensic procedure difficult [23]. Criminals use various proximity sensors, and tags as anti-forensic measures for creating a booby-trap, e.g., a hard-disk seized for forensic investigation triggered a software booby-trap which encrypted the entire volume [24].

## 4 Proposed Evidence Provability Process

In this section we first introduce **heterogeneous piecewise hashing**, a new technique to improve the integrity checking in digital evidence. Secondly, we propose a **Digital Evidence Integrity Certificate (DEIC)**, a single document which summarizes all the information needed to prove the integrity of evidence and finally, we formalize the digital forensics process to ensure digital evidence provability.

Our proposed evidence provability process addresses the following aspects:

- The authenticity of the original evidence
- The validation of the analysis procedure
- The traceability of the original evidence from its retrieval
- The Integrity of the original evidence from its retrieval.

### 4.1 Flexible Piecewise Hashing

Piecewise Hashing was a hashing strategy first invented by Nick Harbour [12]. The definition of what piecewise hashing (PWH) is:

Given a message $m$, a bits string of length $n$, a robust cryptographic hashing algorithm $fh(m)$; piecewise hashing the technique breaks the message $m$ into block of length $n$ such that, $N = m/n$ where N is the number of blocks in message $m$.

$$i < m_i < N \tag{1}$$

$$d = fh(m_i) \tag{2}$$

Piecewise hashing can be approached in two different ways:

- **Homogeneous:** The message is divided into blocks of equal size i.e. $m_i = m_j$ and for each of them a hash digest is computed
- **Heterogeneous:** The message is divided into blocks of flexible size i.e $m_i! = m_j$ and for each of them a hash digest is computed.

The homogeneous PWH is the most straightforward approach where only the base block size is needed, and integrity of any block is verifiable easily. The only disadvantage is non-scalability as large messages have a more considerable number of the hash values which results in a storage problem. With the heterogeneous PWH, we need more information to reconstruct the hash values, namely the block interval pairs (*block_start, block_end*) but the benefit to this approach is to be able to identify and hash only the critical sections of a message which would save storage space.

## 5 Evidence Integrity Certificate (DEIC)

The Digital Evidence Integrity Certificate (DEIC) is our attempt to have a compact representation of all the integrity information related to any digital evidence in a single document, which proves its authenticity. The DEIC includes (1.) the context information related to the evidence and (2.) the digital signature of the certificate from the inspector.

A DIEC is structured as follows:

- **Evidence type**: Disk image, Audio, Video, Image file. Many more types may be added to this list
- **Context-information**:
  - When is the evidence found
  - How it is collected
  - Who is involved
  - Where it was found
  - External conditions
  - Internal conditions.
- **Hashing strategy**: Single hash, homogeneous or heterogeneous PWH
- **Hashing metadata**: This comprehends the hashing algorithm type, in case of homogeneous PWH, block size, number of blocks, in case of heterogeneous PWH blocks intervals

- **Hash values list**: Contains the complete hash value of the evidence (if this one is verified as correct there is no need to check the single blocks) and the list of the sub-blocks hash digests
- **Investigator Sign**: The certificate needs to be signed by the investigator responsible for the evidence for example with his PGP private key.

### 5.1 Formalizing the Provability Process

In this section, we formalize the steps that an investigator needs to follow to ensure the provability of evidence in court. It is important to keep track the information below:

- The context information during the evidence retrieval
- The evidence chain of custody
- The analysis process step by step
- The integrity of the original evidence.

The Figure 3 summarizes the necessary steps to follow to ensure complete evidence provability in front of the court. We inserted a flexible piecewise hashing approach to improve the reliability of the evidence integrity validation and the DEIC to have a compact document with all the integrity-related information.

We define a critical section of evidence which identifies the essential artifacts that support the cause of the investigation. For instance, in a disk image, a critical section consists of the sectors that contain the significant evidence files found during the analysis or in video evidence, the specific interval of frames that include crucial information.

While collecting digital evidence, the forensic investigator should document the context information described in the DEIC section. Since one cannot apply a hashing strategy before identifying the critical parts of the evidence, the first step is to ensure integrity is to compute the complete hash of the original evidence at the acquisition itself. Then evidence is then analyzed by the cyber-forensics expert where all the analysis step are documented, and forensic expert makes sure those steps are reproducible by a third party also. The investigator then identifies the critical sections of the evidence and finally create as an integrity proof, the **DEIC** which is digitally signed by him. The last step that we suggest is the refreshing of the evidence: as highlighted in the Section 3 because aging is a big issue for digital evidence and piecewise integrity check is not useful if data corruption is widespread. The only solution is to make a backup copy of the data in evidence storage device and apply DEIC on it to prove its admissibility.

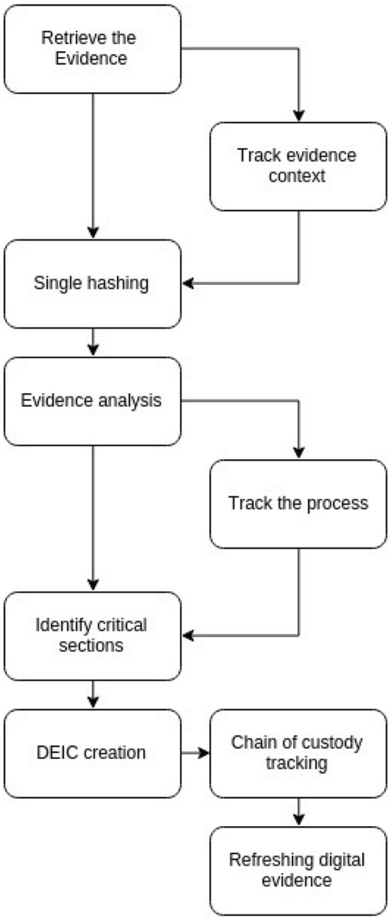

**Figure 3** Provability process.

## 5.2 Applying the Provability Process

The following section describes the evidence acquisition using our process in detail. For demonstrating our approach, we only analyzed the types of evidence most frequently acquired as evidence namely, Memory/Disk images, video, audio, and images. We use the keyword *BLOCK* to refer to a single piece of any evidence. Properties of this piece of evidence may differ with each evidence type as highlighted below.

- **Memory/Disk Image**: Memory or Disk Image is a container which consists of bit by bit copy of the physical or virtual memory and stored in forensic image format. For simplicity purpose, we call these contiguous block memory as *BLOCK* itself.

- **Audio File**: WAV format is most used format by the forensic experts mainly due to its uncompressed nature which makes analysis more manageable. The WAV format consists of Chunks. So, here we use *BLOCK* to refer to a single chunk.
- **Video File**: Digital video file are containers which consist of video data in video coding format and audio in audio coding format. Any video is a visual representation of moving images, and these images are called frames. We refer to the interval of frames as a *BLOCK*.
- **Image File**: Image is mainly composed of pixels which are the smallest element in them. We refer to the square matrix of these pixels as a *BLOCK*.

Earlier we established the unit for a slice for given evidence type; we further demonstrate the means to apply this strategy to evidence. Our approach is enumerated below and summarized in the Figure 4.

1. Identify the evidence type and format.
2. The blocks are identified from the evidence. E.g., if the image is the acquired evidence, the pixel matrix is considered as a BLOCK
3. The complete hash of the evidence is taken
4. User inputs the *BLOCK* size. Say for an image, input matrix size, i.e., p xq
5. The user chooses the hashing strategy [4]
   (a) If the user chooses homogeneous hashing, the artifact is split into pieces of same block size equally. These blocks are passed to the hashing function to generate the digest
   (b) If the user chooses heterogeneous hashing, the user further selects the intervals to be hashed. Here we defined an interval to refer to an aggregation of *BLOCKS* and aggregation of intervals is called as a set. The hashing function then receives the interval from the set.
6. The forensics investigator inserts the context evidence into the DEIC
7. The pieces are hashed and signed using DEIC by the forensic examiner
8. The DEIC is stored on a disk or image along with the original digital evidence.

The DEIC is unique to any digital evidence, and it acts as the key to proving its verifiability during litigations. We can also argue that, if DEIC verification is applied to a true copy of the digital evidence and return success, we can attempt to claim its admissibility during court proceeding especially, if the original gets corrupted.

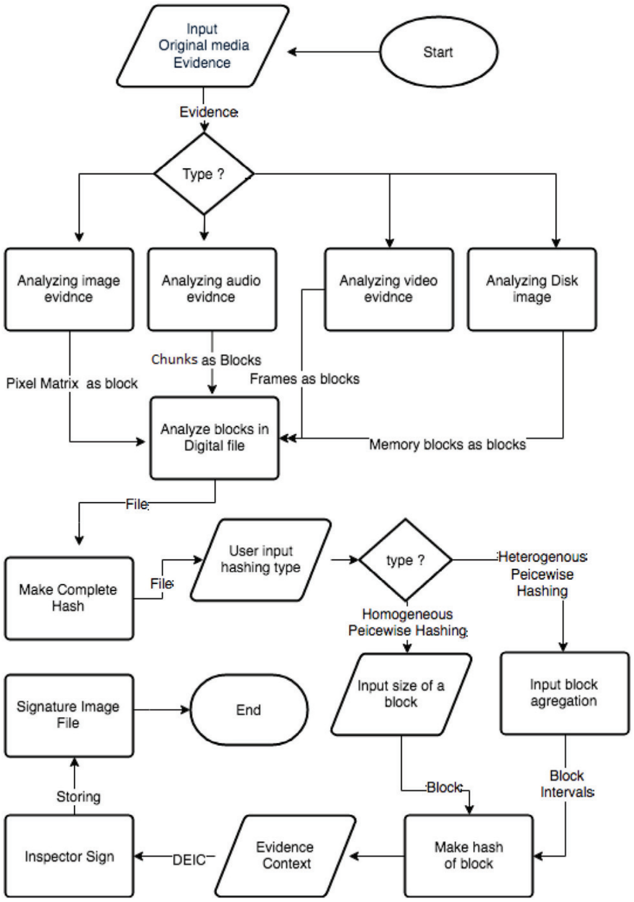

**Figure 4** Evidence acquisition strategy.

### 5.3 Verifying the Integrity Process

In the section, we describe the process used for verification of the evidence using the DEIC [5]. At this point, the examiner has the DEIC and the original evidence in place.

The process is enumerated below and also summarized using Figure 5.

1. Verification of the DEIC using the PGP key of the forensic examiner
   (a) If verification is successful, important information like block size, interval sets, hash list, the overall hash is retrieved
   (b) If failure; results in termination of the verification process

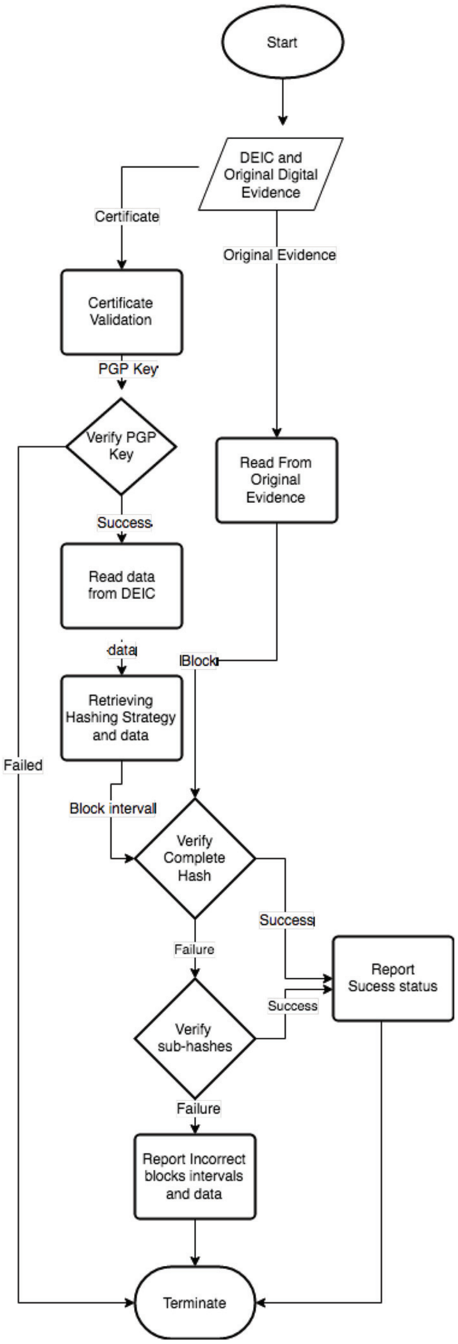

**Figure 5** Evidence verification strategy.

2. Verify the overall hash of the evidence
   (a) If the overall hash is a match which directly implies the validity of the evidence and hence success status is returned
   (b) If failure, then continue towards the verification of the sub-hash list
   (c) The sub-hash verification process returns all the hash and corresponding corrupted block.

## 6 Related Works

We believe this is the first of its kind proposal with attempts to formalize the digital evidence provability using a well-known method of Block based hashing. Che-Yen-Wen et al. [18], had proposed a method for digital image analysis and authentication using md5 hashing on a digital image which would further aid in its examination and analysis. Although Che-Yen work was aimed at providing authentication but did not use piecewise hashing strategy. One of the most popular work was done by Kornblum et al. [13], by proposing a context triggered piecewise hashing (CPTH) to identify identical files, which constructs hashing signatures by combining some traditional hashes whose boundaries are determined by the context of the input. Kornblum's method is modified form of our piecewise hashing methods, where our method aims at providing authentication and integrity and his method verified similarity in files, however, both used piecewise hashing. Later Chen et al. [2] proposed an improvement over Kornblum's context piecewise hashing wherein, he developed a *Store-Hash* and *Rehash* idea over the existing context triggered piecewise hashing technique. Their experimental results show that performance, speed and the ability of similarity detection of the new scheme are better than CTPH. Later, Nickel et al. [3] proposed another variation of Korn-blum's method for biometric recognition, where he introduced a new template protection method which works by applying cryptographic hash functions in a piecewise manner on biometric feature vector. Their experimental results indicate that the biometric performance of the method is close to the biometric performance obtained without template protection. Breitinger et al. [5] performed an analysis study on *sdhash*, a robust similarity preserving digest algorithm based on piecewise hashing. His research uncovered design errors within the fingerprint generation and other comparisons. They claim *sdhash* to have inconsistencies between the specification of *sdhash* and its implementation, which leads to unexpected results. Another research which used piecewise hashing was done by Winter et al. [1] where they proposed a solution to solve time-consuming nature of hashing techniques used by *ss-deep* and other fuzzy hashes. They base their strategy on n-grams contained in the piecewise hash signatures, and it allows for answering similarity queries very efficiently.

## 7 Future Works

In this proposal, we discussed only four evidence types, which include disk image and media types (video, image, and audio). In the future works, the scope of the DEIC and the proposed integrity provability process could be extended to other digital artifacts collected through live or remote acquisition. Another issue is storage and preservation of the digital evidence or its backup which is considered by many, a costly practice. A solution could be that, instead of storing all the digital artifact, if one could identify and store only the critical sections, we could save a lot of storage space. Moreover digital evidence like in disk images often does not contain any relevant information for the case, consequentially resulting in a waste of space for governmental digital storages. We suggest that more study need to be done on the ad-missibility of critical sections of digital evidence and we also believe that a standardized approach to evidence provability such as our proposed, can be a good starting point for a formal admissibility proof.

## 8 Conclusions

Forensic experts carry out a very complicated task when it comes to analyzing digital artifact by making sure not to compromise the data contained in them. This arrangement is often a challenging task which always required expert care and handling. With our work, we have formalized the provability process, we have tried to propose a new and efficient method for ensuring the integrity of critical artifacts and its copies thereby guaranteeing their admissibility in court. We also have introduced a certification process, DEIC which is the condensed representation of all information which ensures integrity and authenticity of the evidence. Given its advantages and effectiveness, we believe our approach would mark a step towards strengthening evidence integrity and its admissibility during litigation.

## References

[1] Winter, C., Schneider, M., and Yannikos, Y. (2013). F2S2: Fast forensic similarity search through indexing piecewise hash signatures. *Digital Investigation,* 10(4), 361–371.

[2] Chen, L., and Wang, G. (2008). An efficient piecewise hashing method for computer forensics. In *First International Workshop on Knowledge Discovery and Data Mining, WKDD*, 635–638.

[3] Nickel, C., Zhou, X., and Busch, C. (2009). Template protection via piecewise hashing. In *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP'09, 1056–1060.

[4] Jose, J., Pande, K. S., and Murty, N. S. (2015). A memory architecture using linear and nonlinear feedback shift registers for data security. In *IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 1–5.

[5] Breitinger, F., Baier, H., and Beckingham, J. (2012). Security and implementation analysis of the similarity digest sdhash. In *First international baltic conference on network security & forensics (nesefo).*

[6] Mohan, A. K., and Kumar, T. G. (2015). Secure Seed-Based Sturdy OTP via Convenient Carry-on Device. In *Artificial Intelligence and Evolutionary Algorithms in Engineering System,* 447–455. Springer, New Delhi.

[7] Jason Jordaan, Digital Forensics and Corruption (2013).

[8] Electronic CSI, A Guide for First Responders, 2nd edition, National Institute of Justice (2008).

[9] Electronic CSI, A Guide for First Responders, 2nd edition, National Institute of Justice (2008).

[10] Reys, A., and Wiles, J. (2007). Cyber Crime and Digital Forensics, 401.

[11] Kumar, K., Sofat, S., Jain, S. K., and Aggarwal, N. (2012). SIGNIFICANCE of hash value generation in digital forensic: A case study. *International Journal of Engineering Research and Development.* Available at: http://www. ijerd. com/paper/vol2-issue5 I, 2056470

[12] Harbour, and Dcfidd. (2002). Defense Computer Forensics Lab.

[13] Kornblum, J. (2006). Identifying almost identical files using context triggered piecewise hashing. *Digital investigation,* 3, 91–97.

[14] Martínez, V. G., Álvarez, F. H., and Encinas, L. H. (2014). State of the art in similarity preserving hashing functions. In *Proceedings of the International Conference on Security and Management (SAM)* 1.

The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[15] Andreeva, E., Mennink, B., and Preneel, B. (2015). Open problems in hash function security. *Designs, Codes and Cryptography,* 77(2–3), 611–631.

[16] DFRWS 2001 USA, A Road Map for Digital Forensic Research (2004).

[17] George Reis, Digital Image Integrity (2004).

[18] Che-Yen Wen, Kun-Ta Yang, (2006). Image authentication for digital image evidence.

[19] Shanmugam, K. (2011). *Validating digital forensic evidence* (Doctoral dissertation, Brunel University School of Engineering and Design PhD Theses).

[20] Solomon, M. G., Rudolph, K., Tittel, E., Broom, N., and Barrett, D. (2011). *Computer forensics jumpstart.* John Wiley & Sons.

[21] Ernesto Dal, Martin A. Rossi, Electronic Forensics Education Needs of Law Enforcement (2004).

[22] Armstrong, H., and Russo, P. (2006). Corruption and Inefficiency, Theory and Evidence from Electrical Utilities.

[23] Gordon E. Pelton, Computer Evidence Destroyed (2004).

[24] Imsand, E. S., and Hamilton, J. A. (2004). Auburn University, Digital Battlefield Forensics.

[25] Lázaro, P. G. C. (2004). Forensic computing from a computer security perspective.

[26] Edmond, G. (2014). Contextual bias and cross-contamination in the forensic sciences the corrosive implications for investigations.

[27] Khanna, H. (2017). Digital spectrographic cross-correlation: tests of sensitivity.

[28] Hua, G., Bi, G., and Thing, V. L. (2017). On Practical Issues of ENF Based Audio Forensics.

[29] Rasmussen, J. O. (2015). Ensuring end-to-end protection of video integrity.

[30] Courtesy of serre-lab.clps.brown.edu Available at: http://serre-lab.clps.brown.edu/wp-contentuploads/2012/08/example-medium-quali.jpg

[31] Timothy, A., Dunton, An Introduction to Time Waveform Analysis, Available at: http://reliabilityweb.com/articles/entry/anintroduction totimewaveformanalysis

[32] Zeltser, L. Hex-Editors, Available at: https://digital-forensics.sans.org/blog/2010/09/29/hex-editors-for-malware-analysis

[33] Phil Manchester, Authenticity and Integrity of Audio Evidences, Available at: http://www.soundonsound.com/techniques/introduction-forensic-audiotop

[34] Deloitte, Preserving Evidence of Cyber Crime, Available at: http://deloitte.wsj.com/cio/2014/12/03/computer-forensics-preserving-evidence-of-cyber-crime/

[35] ASG Group, Computer Forensics and Spoliation of Evidence, Available at: https://asginvestigations.com/attorney-services/spoliation-of-evidence/

[36] Gubanov, Y.Digital Evidence Types, Available at: https://www.forensicmag.com/article/2012/05/retrieving-digital-evidence-methods-techniques-and-issues-part-1

[37] Edward John Primeau, Wav Components, Available at: http://www.audioforensicexpert.com/tag/audio-evidence/

[38] Dawate, Sound Wave Components, Available at: hhttps://blogs.msdn.microsoft.com/dawate/2009/06/23/intro-to-audio-programming-part-2-demystifying-the-wav-format/

## Biographies

**Aswin Gopalakrishnan** received M.Sc. Computer System Security from Vrije University, the Netherlands, and M.Tech in Cyber Security from Amrita Vishwa Vidyapeetham, India. He is currently functioning as a security analyst in Secura, a cyber security organization based out of the Netherlands. He aspires to practice, acquire and improve his skills as a security information analyst. His specialty lies in safeguarding computers and networks by establishing and enforcing system access controls, maintaining disaster preparedness, developing a framework for checks and levels of access while recommending improvements. He is also familiar with the full spectrum of project management skills backed by complete Software Development Life Cycle (SDLC) and IT service delivery expertise.

**Emanuele Vineti** from 2012 was following his Bachelor degree in Computer Science at the University of Modena, Italy. In 2015 he moved to the Netherlands in the University of Groningen for a research project on a power grid optimization. Later that year he achieved his Bachelor degree with a distinction. In 2016, he began his M.Sc studies in Computer Science with the core track in computer system security. From January 2018 he is working on his Master Thesis research at the Vrije University of Amsterdam.

**Ashok Kumar Mohan**, M.Tech specialized in Cyber Security, is a Research Associate at TIFAC-CORE in Cyber Security, Amrita Vishwa Vidyapeetham, Coimbatore, Tamil Nadu, India. He is currently a PhD scholar doing his research in the area of Cyber Forensics funded by Ministry of Electronics & Information Technology (Government of India) under Visvesvaraya PhD scheme for Electronics and IT. He is currently pursuing his research over the cyber security core vicinity in Metadata Forensics, Wireless Security Auditing, Rumor Prediction in Social Media Networks and Slack Space Analysis of NTFS File Systems. He is also the Certified EC-Council Instructor (CEI) for ethical hacking and penetration testing certification courses at the research centre.

**M. Sethumadhavan** received his PhD from Calicut Regional Engineering College. Currently, he is a Professor of Mathematics and Computer Science, Amrita Vishwa Vidyapeetham, Coimbatore. His research interest include Cryptography and other solutions for Cyber Security