Automated Detection of Container-based Audio Forgery Using Mobile Crowdsourcing for Dataset Building

Homin Son[1], Sung Won Beak[2], Jae Wan Park[3]*
[1, 2, 3]Global School of Media, Soongsil University, South Korea
[1]ghals0921@soongsil.ac.kr, [2]bsw6399@soongsil.ac.kr, [3]jaewan.park@ssu.ac.kr
***Corresponding Author**

Article Info

Article history:

Submission Feb 12, 2024
Revised March 22, 2024
Accepted March 25, 2024
Published March 31, 2024

Keywords:

Digital Audio Forensics
Forgery Detection
Mobile Crowdsourcing
Audio Dataset
Container-Based Methods

ABSTRACT

This research paper introduces a new approach for detecting digital audio file forgeries, highlighting entrepreneurship spirit through innovation and market adaptability. It utilizes a cyclical system aided by mobile crowdsourcing to collect a comprehensive dataset of smartphone recordings, demonstrating an entrepreneurship approach to leveraging technology for scalable solutions. Digital forgery, an area ripe for entrepreneurship investment, is becoming increasingly accessible, making it challenging to detect manipulated audio files. This new method emphasizes the utility of metadata and file structure analysis and is scalable, reflecting an entrepreneurship mindset in creating adaptable and sustainable solutions. The researchers developed a mobile web-based prototype system to collect diverse audio data and automatically detect forgeries, showcasing their initiative and innovative thinking. They also conducted scenario-based testing to validate the effectiveness of their methodology, a step that underscores the entrepreneurship value of practical validation. This approach has the potential to significantly advance digital forensic practices by enabling broader detection of manipulated audio files, opening avenues for entrepreneurship ventures in digital security. The collected dataset will be made publicly available and serve as a valuable resource for future forensic investigations, encouraging entrepreneurship collaboration and knowledge sharing. The paper lays the groundwork for future research in expanding the scope of digital forensics, fostering technological innovation, and enhancing participatory models for data collection, all of which are essential elements in entrepreneurship ecosystems.

****Corresponding Author:***

Jae Wan Park (jaewan.park@ssu.ac.kr)
DOI: https://doi.org/10.34306/att.v6i1.383

1. INTRODUCTION

In today's society, the proliferation of smartphones has made it easier to create, edit, and utilize audio files, thereby increasing the risk of forgery [1, 2]. Furthermore, with advancements in digital audio editing software and artificial intelligence technologies such as Deep Voice software and deepfakes, it is now possible for laypeople to create forged voice files either by deleting specific parts of digital audio files or by inserting arbitrary content [3–5]. This study tackles the challenge of detecting digital audio file forgeries using a cyclical approach that requires continuous improvement throughout analyzing and modeling data. By leveraging mobile crowdsourcing, we minimize the resources required for extensive forensic analyses and engage a diverse range of participants in the forensic process. Such forged audio files can cause significant problems when used as critical data such as court evidence [6]. In such situations, experts expend significant time and effort to determine whether audio recording files have been tampered with [7]. Accordingly, there is a pressing need to develop a method to detect forgeries in digital audio files efficiently.

Methods for detecting forged audio files are broadly classified into container-based and content-based forgery detection methods [8]. Content-based forgery detection methods, a core task of audio forensics, detect the area forged by audio editing software within the audio content [9]. Owing to recent advances in deep learning, numerous studies have leveraged deep learning to detect forged audio files within audio content [4, 5], [10–12]. Deep-learning-based methods detect audio file forgery by training models on large-scale datasets, supporting multimodal inputs, including spectrogram images and text. This approach enables better learning of audio features and more accurate differentiation between original and forged audio. However, acquiring an authentically forged dataset edited by various audio editing software with their functions and encoded with the same encoder as the original recording device presents significant challenges [13]. For this reason, current deep learning-based and content-based forgery detection methods have limitations.

On the other hand, container-based forgery detection methods focus primarily on the file structure and metadata alterations occurring during audio file forgery [14]. As the factors for this technique can vary depending on smartphone models, operating systems, recording applications(apps), and file formats, various studies have been conducted to address these variables [15–20]. However, forging the structure and metadata of audio files to appear identical to the original file is possible because of the variety of audio recording apps available for smartphones and their re-encoding capabilities [21, 22]. Nevertheless, a technique for detecting forgery by comparing the metadata and structure of an audio file with those of an original test audio file is crucial for enhancing the efficiency of digital audio forensics. Based on the systematic characteristics with clear factors for detecting forged files, this approach has the potential to evolve into an automated forgery detection system. However, to the best of our knowledge, no audio dataset exists as original audio files for testing recorded across several smartphone models, various recording apps, and their options, considering that there are approximately 250 smartphone brands globally [23][24]. The absence of such datasets makes it difficult to detect tampering using a container-based method.

This study aims to develop a mobile web-based prototype system by collecting audio files recorded on smartphones, embodying an entrepreneurship approach in technological innovation and market responsiveness. To achieve this objective, we built a cyclical approach for detecting container-based forgery, illustrating entrepreneurship insight in problem-solving and market needs assessment[25][26]. This approach extracts elements to determine whether smartphone audio files have been tampered with, leveraging entrepreneurship skills in creating novel solutions[27]. Our methodology is based on various experiments conducted using Samsung Galaxy S23 Ultra (Android 14), guided by a comprehensive literature review, demonstrating an entrepreneurship spirit in pioneering research and development[28]. To prove the validity of this method, we developed a mobile web-based prototype system capable of collecting audio files recorded on smartphones and automatically detecting forged audio files created using container-based methods, showcasing an entrepreneurship venture in forensic technology[29]. Furthermore, this system was validated through scenario-based testing, demonstrating the practicality and robustness of our method for identifying forged audio files, reflecting the entrepreneurship value of product testing and market adaptation[4]. This system enables fast and accurate data collection through a simple and easy-to-use user interface, eliminating the need for user-generated annotations, an entrepreneurship achievement in user experience design. The system constructed in this study demonstrates cyclical and self-sustaining characteristics, epitomizing the entrepreneurship goal of creating scalable and adaptable solutions[30]. In other words, the detection range was automatically expanded by incorporating audio files from new smartphone models not included in the dataset, an entrepreneurship strategy in continuous improvement and market expansion.

This research is significant because it lays the foundation for an efficient method by building a dataset of audio files and developing an automatic audio forgery detection system based on the container-based method. Furthermore, making this dataset available to the public is expected to be a valuable resource for researchers and students seeking to explore the realms of audio forensics, fostering an entrepreneurship ecosystem in academic and research communities.

2. LITERATURE REVIEWS

2.1. Advancements in Container-based Forgery Detection

Metadata is essentially structured data that provides detailed descriptions of other data entities. In the context of voice recording files, metadata encompasses fundamental attributes, such as file name, type, size, creation date and time, and last modification date and time, alongside audio-specific characteristics, such as sample rate, bit rate, codec, number of channels, and audio length.

The analysis of metadata plays a pivotal role in identifying forgeries and alterations within voice recording files. This importance stems from the observation that the editing or manipulating of audio files invariably leads to modifications in their metadata and structure from the state of the original file. Grigoras and Smith [15] examined the metadata structures in MP3, WAV, and WMA audio files, revealing that metadata undergoes alterations during the editing process. They posited that analyzing the file format and metadata is a crucial step in digital audio authentication[31]. Similarly, Gangwar et al. [16] discovered that attributes, such as metadata, file signatures, and hex data, are instrumental in pinpointing the origin of a recording file, thereby making metadata a significant indicator for detecting file tampering across various formats.

Furthermore, metadata properties exhibit variability based on the smartphone model used for the recording. Distinctions exist between devices such as Apple iPhones and Samsung Galaxy smartphones and among models from the same manufacturer. Zeng et al. [17] demonstrated that voice recording files vary in their specific file structure, time information, and metadata depending on the iPhone model and operating system. Koenig and Lacey [18] also highlighted a discernible difference in metadata structure and properties when editing and re-encoding a voice recording file on an iPhone's Voice Memos compared to the original file. Park et al. [19] demonstrated that adding log records registered in the device during the creation of audio recordings under these foundational characteristics makes it possible to verify the authenticity of audio recordings generated using the Voice Memos application on the iPhone[32].

M4A files, MPEG-4 Audio, are predominantly used as smartphone audio files. M4A files can encode audio using Advanced Audio Coding (AAC) or Apple Lossless Audio Codec (ALAC). By leveraging the unique file structure of M4A, Michalek [20] introduced a novel method for detecting forgeries and alterations in audio files. Michalek's analysis, conducted on recordings made with the default Samsung Galaxy smartphone app and nine Android recording apps, indicated that editing not only the metadata properties but also the structure of the MPEG multimedia container. Theoretically, upgrading the operating system (OS), even within the same model, could impact audio data encoding, potentially leading to modifications in the M4A file structure. Similarly, updates to recording apps might affect audio data encoding and result in structural changes to the M4A files. However, rapid updates to smartphone operating systems and recording apps limit the scope of these studies, as they may not fully account for the impact of such upgrades[33].

The deviation between the metadata and file structure of the original and altered audio files plays an important role as a clear indicator of forgery. However, the frequent introduction of new smartphone models and the swift release of updates for operating systems and recording applications makes it difficult to conduct a comprehensive and precise analysis of audio file forgery. Consequently, constructing an extensive database that categorizes metadata and file structure characteristics by operating system and recording application versions according to smartphone models is crucial for enhancing audio file authenticity verification[34].

2.2. Optimizing Mobile Crowdsourcing for Enhanced Data Collection

Crowdsourcing, a concept introduced by Jeff Howe in 2006, encapsulates the collective effort of soliciting contributions, ideas, skills, and information from a wide audience [35]. This methodology harnesses the ”wisdom of the crowd” for various purposes, aiding entities such as corporations, academic researchers, and governmental bodies to address specific challenges, foster innovation, and gather niche data[36]. Crowdsourcing is particularly beneficial for tasks that require human intellect to be superior to machine capability[37]. It is also advantageous for projects where leveraging a vast, heterogeneous crowd can improve efficiency in terms of both time and cost, compared to hiring specialized professionals [38].

The emergence of mobile technology has broadened the scope and effectiveness of crowdsourcing[39]. Mobile devices enable active participation without geographical or temporal limitations, enhancing accessibility. Moreover, the growing demand for data, propelled by advancements in artificial intelligence and the widespread availability of sensor-equipped smartphones, has facilitated the compilation of large-scale datasets through mobile crowdsourcing efforts [40–42][43].

Ensuring the efficacy of mobile crowdsourcing requires a thorough evaluation of several key factors, including task design, incentive mechanisms, quality control measures, and security and privacy concerns [44].

Incentives such as financial rewards, gamification elements, and social recognition are imperative for motivating extensive participation [45]. Implementing robust quality control protocols is vital for maintaining the accuracy and reliability of collected data[46]. In response to these challenges, research has shifted towards developing systems that automatically generate annotations from metadata harvested from various sensors within mobile devices, moving away from reliance on user-generated annotations [47][48].

Task architecture must be explicit and targeted to promote contributions through clear definitions, a refined user interface (UI), and appropriate granularity [49], [50]. UI has emerged as a pivotal component within mobile crowdsourcing initiatives. A UI that is straightforward and user-friendly and facilitates swift completion of tasks is deemed essential [51]. While traditional efforts have emphasized aesthetic design to achieve this, the advent of UI technologies that capitalize on data-related information can significantly diminish user effort and foster UI enhancements, culminating in expedited task processing[52]. Such advancements in UI design bolster participant engagement and improve data quality. They also highlight the need for a comprehensive strategy. This strategy should integrate incentives, privacy and security measures, quality assurance, and a focused emphasis on the UI to collect a wide array of smartphone recordings efficiently[53].

3. METHODS

3.1. Experiments for Container-based Forgery Detection

In this study, we adopted a three-step approach to detect container-based forgery in system design, involving: 1) observing changes in the audio file structure, 2) defining immutable metadata attributes, and 3) noting changes according to recording app settings. We utilized the latest Samsung Galaxy S23 Ultra with Android 14 as the operating system given the popularity of Samsung Galaxy smartphones in Korea. The original file was generated using a Voice Recorder and the default voice recording application on the Samsung Galaxy S23 Ultra[54]. Subsequently, leveraging the original file, we produced two forged versions: one re-recorded using the editing function of the built-in Voice Recorder app and the other using the audio editing software, DemoCreator [55][56].

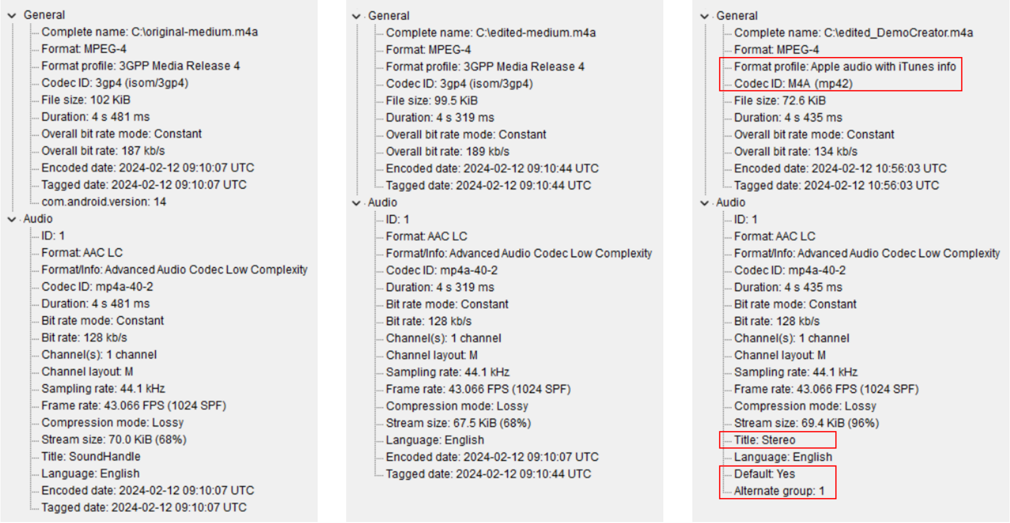
3.1.1. Immutable Attributes of Metadata

An experiment was conducted using the MediaInfo software [57] to identify immutable elements within the metadata of the recording files. Audio file metadata can be divided into two categories: general and audio metadata. General metadata includes file name, size, format, duration, tagged date, and encoded date. In contrast, audio metadata covers the bit rate, sampling rate, number of channels, recording length, and codec[58][59]. Certain metadata elements, including file name, size, duration, tagged date, and encoded date, may vary based on the recording environment. Conversely, audio files recorded using the same model, operating system, and recording application with identical settings exhibit immutable metadata attributes and display consistent properties and values. As shown in Table 1, the metadata of voice files can be segregated into immutable and mutable attributes, highlighting the distinction between changeable and unchangeable properties[60][61].

Table 1. Classification of immutable and mutable attributes in M4A file metadata

	Immutable Attributes	Mutable Attributes
General	format, format profile, codec ID, overall bit rate mode	complete name, file size, duration, overall bit rate, encoded date, tagged date
Audio	format, format/Info, bit rate mode, bit rate, channel(s), channel layout, sampling rate, ID, frame rate, compression mode, title	language, stream size

Figure 1 shows that edited files display significant differences, underscoring metadata modifications when files are re-encoded using various editing tools.



```
General
  Complete name: C:\original-medium.m4a
  Format: MPEG-4
  Format profile: 3GPP Media Release 4
  Codec ID: 3gp4 (isom/3gp4)
  File size: 102 KiB
  Duration: 4 s 481 ms
  Overall bit rate mode: Constant
  Overall bit rate: 187 kb/s
  Encoded date: 2024-02-12 09:10:07 UTC
  Tagged date: 2024-02-12 09:10:07 UTC
  com.android.version: 14
Audio
  ID: 1
  Format: AAC LC
  Format/Info: Advanced Audio Codec Low Complexity
  Codec ID: mp4a-40-2
  Duration: 4 s 481 ms
  Bit rate mode: Constant
  Bit rate: 128 kb/s
  Channel(s): 1 channel
  Channel layout: M
  Sampling rate: 44.1 kHz
  Frame rate: 43.066 FPS (1024 SPF)
  Compression mode: Lossy
  Stream size: 70.0 KiB (68%)
  Title: SoundHandle
  Language: English
  Encoded date: 2024-02-12 09:10:07 UTC
  Tagged date: 2024-02-12 09:10:07 UTC
```

(a)

```
General
  Complete name: C:\edited-medium.m4a
  Format: MPEG-4
  Format profile: 3GPP Media Release 4
  Codec ID: 3gp4 (isom/3gp4)
  File size: 99.5 KiB
  Duration: 4 s 319 ms
  Overall bit rate mode: Constant
  Overall bit rate: 189 kb/s
  Encoded date: 2024-02-12 09:10:44 UTC
  Tagged date: 2024-02-12 09:10:44 UTC
Audio
  ID: 1
  Format: AAC LC
  Format/Info: Advanced Audio Codec Low Complexity
  Codec ID: mp4a-40-2
  Duration: 4 s 319 ms
  Bit rate mode: Constant
  Bit rate: 128 kb/s
  Channel(s): 1 channel
  Channel layout: M
  Sampling rate: 44.1 kHz
  Frame rate: 43.066 FPS (1024 SPF)
  Compression mode: Lossy
  Stream size: 67.5 KiB (68%)
  Language: English
  Encoded date: 2024-02-12 09:10:07 UTC
  Tagged date: 2024-02-12 09:10:44 UTC
```

(b)

```
General
  Complete name: C:\edited_DemoCreator.m4a
  Format: MPEG-4
  Format profile: Apple audio with iTunes info
  Codec ID: M4A  (mp42)
  File size: 72.6 KiB
  Duration: 4 s 435 ms
  Overall bit rate mode: Constant
  Overall bit rate: 134 kb/s
  Encoded date: 2024-02-12 10:56:03 UTC
  Tagged date: 2024-02-12 10:56:03 UTC
Audio
  ID: 1
  Format: AAC LC
  Format/Info: Advanced Audio Codec Low Complexity
  Codec ID: mp4a-40-2
  Duration: 4 s 435 ms
  Bit rate mode: Constant
  Bit rate: 128 kb/s
  Channel(s): 1 channel
  Channel layout: M
  Sampling rate: 44.1 kHz
  Frame rate: 43.066 FPS (1024 SPF)
  Compression mode: Lossy
  Stream size: 69.4 KiB (96%)
  Title: Stereo
  Language: English
  Default: Yes
  Alternate group: 1
```

(c)

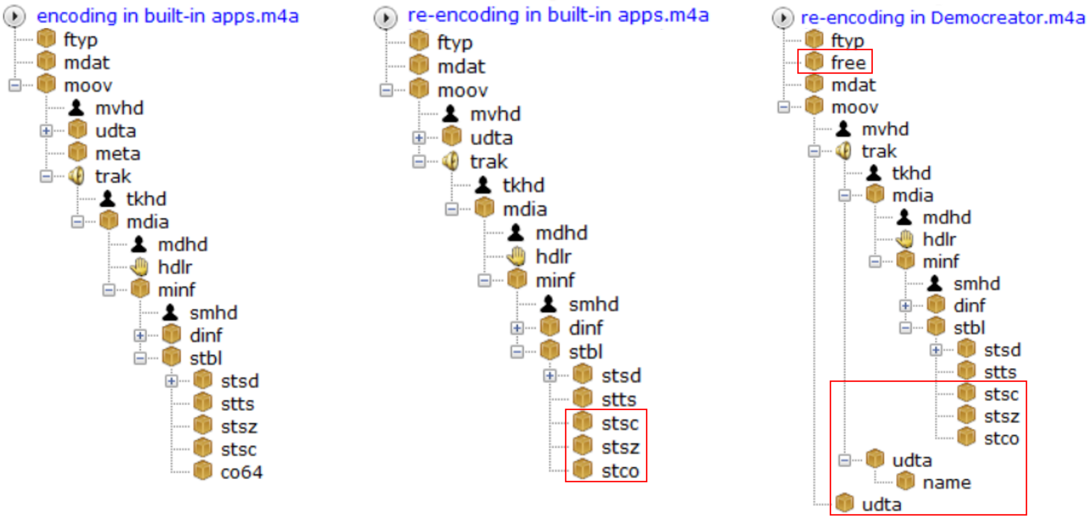
Figure 1. Metadata differences: (a) Original; (b) Edited by a built-in app; (c) Edited by DemoCreator

Files edited with the built-in voice recording app lacked metadata related to the operating system and file name of the model[62]. Conversely, files modified using the DemoCreator Software exhibited changes in the format profile, codec ID, and title values. Additionally, the encoded and tagged dates were eliminated and replaced with properties in the 'Default' and 'Alternate groups,' which previously did not exist. It is essential to verify the presence and sequence of attributes of the original data. Identifying immutable attributes and their consistent values is crucial for authentication purposes[63].

3.1.2. Changes in Audio File Structure

An M4A file features a hierarchical structure with various nested segments known as atoms or boxes [18][64]. Existing research has demonstrated that re-encoding an M4A file leads to structural changes that differ from the original file[65]. The purpose of this experiment is to identify changes in the file structure resulting from re-encoding and to verify whether these changes can be restored to the original file structure. To achieve this, we employed a specialized MP4 parser, MP4 Inspector [66], and a hex editor, HxD [67], for an in-depth analysis[68].

Figure 2 illustrates the M4A file structure comparison between the original and the forged files. The original M4A file encoded by a built-in app reveals the absence of the 'meta' box in the M4A file edited and re-encoded by the built-in recording app. Additionally, the re-encoding process changed sub-boxes within the 'stbl' box. Converting to M4A by DemoCreator generated a 'free' box, absent in the original file, and generated two 'udta' boxes, along with changes within the 'stbl' box.



```
encoding in built-in apps.m4a
  ftyp
  mdat
  moov
    mvhd
    udta
    meta
    trak
      tkhd
      mdia
        mdhd
        hdlr
        minf
          smhd
          dinf
          stbl
            stsd
            stts
            stsz
            stsc
            co64
```

(a)

```
re-encoding in built-in apps.m4a
  ftyp
  mdat
  moov
    mvhd
    udta
    trak
      tkhd
      mdia
        mdhd
        hdlr
        minf
          smhd
          dinf
          stbl
            stsd
            stts
            stsc
            stsz
            stco
```

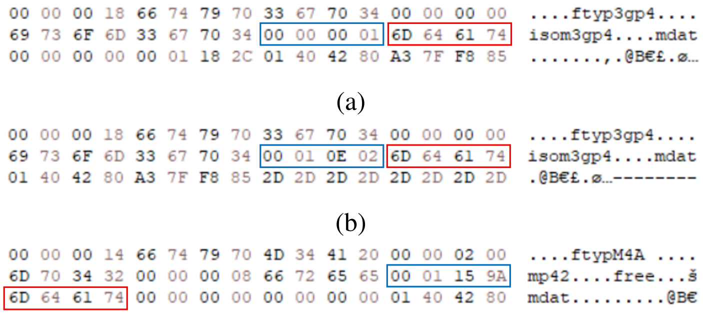
(b)

```
re-encoding in Democreator.m4a
  ftyp
  free
  mdat
  moov
    mvhd
    trak
      tkhd
      mdia
        mdhd
        hdlr
        minf
          smhd
          dinf
          stbl
            stsd
            stts
            stsc
            stsz
            stco
      udta
        name
    udta
```

(c)

Figure 2. Comparison of M4A file structure: (a) Original; (b) Edited by a built-in app; (c) Edited by DemoCreator

It is not easy to alter the structure within an M4A file. However, using a hex editor, the structure and name of the boxes in the original audio files can be modified[69]. Such changes can lead to errors that may cause the M4A file to become non-functional[70]. This issue arises because recordings made with Samsung Galaxy devices' built-in apps employ a 64-bit size in the media data box ('mdat'), in comparison to regular M4A files that use a 32-bit size. Consequently, the latest smartphones support a larger type of M4A file, allowing storage of up to 2 to the power of 64 bytes in the 'mdat' box. However, when re-encoded after editing in the built-in recording app or using DemoCreator, the file is treated as a regular M4A file. Figure 3 compares the media data box types of the original and the forged files. In the original file, the large type of a 'mdat' box is indicated when the 4 bytes immediately preceding the 'mdat' type identifier, represented in ASCII code as '6D 64 61 74, ' are '00 00 00 01'; a regular type of media data box represents any value other than '00 00 00 01. Typically, forged files feature a regular type in their media data boxes. When forged files of a regular type are converted into a large type, the same file structure can be created[71].



```
00 00 00 18 66 74 79 70 33 67 70 34 00 00 00 00  ....ftyp3gp4....
69 73 6F 6D 33 67 70 34 00 00 00 01 6D 64 61 74  isom3gp4....mdat
00 00 00 00 00 01 18 2C 01 40 42 80 A3 7F F8 85  .......,.@B€£.ø…
```

(a)

```
00 00 00 18 66 74 79 70 33 67 70 34 00 00 00 00  ....ftyp3gp4....
69 73 6F 6D 33 67 70 34 00 01 0E 02 6D 64 61 74  isom3gp4....mdat
01 40 42 80 A3 7F F8 85 2D 2D 2D 2D 2D 2D 2D 2D  .@B€£.ø…--------
```

(b)

```
00 00 00 14 66 74 79 70 4D 34 41 20 00 00 02 00  ....ftypM4A ....
6D 70 34 32 00 00 00 08 66 72 65 65 00 01 15 9A  mp42....free...š
6D 64 61 74 00 00 00 00 00 00 00 00 01 40 42 80  mdat........@B€
```

(c)

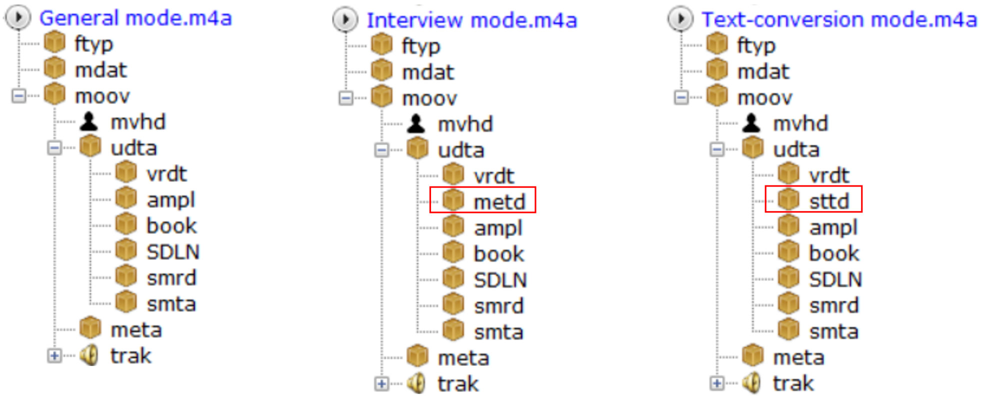
Figure 3. Comparison of M4A file structure: (a) Original; (b) Edited by a built-in app; (c) Edited by DemoCreator

Manipulating the file structure after editing the original file presents a challenge for the latest Samsung Galaxy smartphones. To achieve this level of forgery, it is necessary to utilize an encoder capable of supporting a large type of a 'mdat' box or manually converting it into a large type. Considering that most audio editing software and converters are designed for a regular type of M4A file and manual conversion requires a deep understanding of the MP4 file format, making direct changes is nearly impossible for the general public. In this context, container-based forgery detection methods are expected to be more effective in identifying audio file forgeries[72].

3.1.3. Changes According to Recording App Settings

The built-in recording apps of smartphones provide a range of configurable settings. The Voice Recorder app on the Samsung Galaxy S23 Ultra offers three quality settings for recording: High, Medium, and Low. The High setting uses a bit rate of 256kbps and a sampling rate of 48kHz, the Medium setting defaults to 128kbps and 44.1kHz, and the Low setting defaults to 64kbps and 44.1kHz. Despite these differences, all three options maintain a consistent file structure. The immutable attributes of bit rates, sampling rates, and potential frame rates in the metadata are key to distinguishing among recording quality options.

Moreover, the Voice Recorder app allows users to select from the three modes on the recording screen. The Standard mode was the default voice-recording mode. The Interview mode amplified the voices to record conversations more clearly. Finally, the speech-to-text mode converts speech into text in real-time and displays it on a screen. The metadata of these three modes are influenced by the quality settings; for example, when set to the Medium setting, they follow a 128kbps bit rate and a 44.1kHz sampling rate. However, the file structures of the three modes were not influenced by quality settings. As shown in Figure 4, the three modes have different file structures. Unlike the Standard mode, the Interview mode and the Speech-to-Text mode contain a ’metd’ box and an ’sttd’ box within the user data box (’udta’) respectively.



(a) (b) (c)

Figure 4. Comparison of M4A file structure: (a) Original; (b) Edited by a built-in app; (c) Edited by DemoCreator

While the Standard and Interview modes use the large type of a ’mdat’ box, the Speech-to-Text mode employs a regular type, indicating higher susceptibility to forgery. Based on the built-in recording app, a single smartphone model could generate nine different recording files. This file information can be used not only as a criterion for identifying tampering but also for automatic annotation when collecting data.

3.2. Our Strategies for Collecting Data Based on Mobile Crowdsourcing

In our data collection, we aim to collect audio files from diverse smartphone models, targeting audio files without individual voice recordings to comply with privacy norms. Our mobile crowdsourcing approach, reflecting an entrepreneurship mindset, is underpinned by three principal strategies:

(1) Leveraging the motivational power of social contribution as tangible incentives, encouraging participants by highlighting the societal benefits of their contributions, which aligns with entrepreneurship values of community impact and social entrepreneurship. (2) Developing a user interface that automatically generates data-related information through computing technology without requiring user-generated annotations, accommodating technical proficiencies and thereby lowering barriers to participation, demonstrating entrepreneurship acumen in creating accessible, market-driven solutions. And (3) supporting automated quality control to ensure the reliability and integrity of collected data, akin to entrepreneurship standards for product quality and consumer trust. This includes reducing participant errors by aiding automatic annotations using audio file metadata, a reflection of entrepreneurship innovation in process optimization. Furthermore, enhancing the quality

of data by allowing users to upload data that already are included in the database is an essential feature of our system, showcasing entrepreneurship foresight in data management and system sustainability.

In this research, our approach to collecting non-voice smartphone recording data through mobile crowdsourcing is comprehensive, integrating motivational incentives, user-centric design, and rigorous quality control, embodying entrepreneurship principles in operational efficiency, customer engagement, and ethical standards. These strategies collectively guarantee efficient data collection, strong participant engagement, and adherence to privacy standards, illustrating a holistic entrepreneurship strategy in research and development.

3.3. Building a Cyclical Process

Our system integrates two fundamental operations: the collection of audio file data and authentication. The core idea of this integration is to blur the lines between data collection participants and users. This approach enables users to examine audio files for potential manipulation that could be used against them as harmful evidence, as well as to verify the authenticity of their audio submissions as unaltered evidence. Consequently, it allows users to participate in crowdsourcing activities from both perspectives.

When users upload a file for inspection, the system initiates a verification process. It examines the file's internal metadata to identify specific details such as the model, OS, recording app, and app settings used. If the system does not find a matching original recording in the database, it notifies the user of the findings. Users can then secure their audio data and, in data collection mode, upload it for forgery detection. This approach fosters the development of a self-sustaining and cyclical system, contributing to its ongoing growth. Figure 5 illustrates this cyclical process through a flowchart within our system.

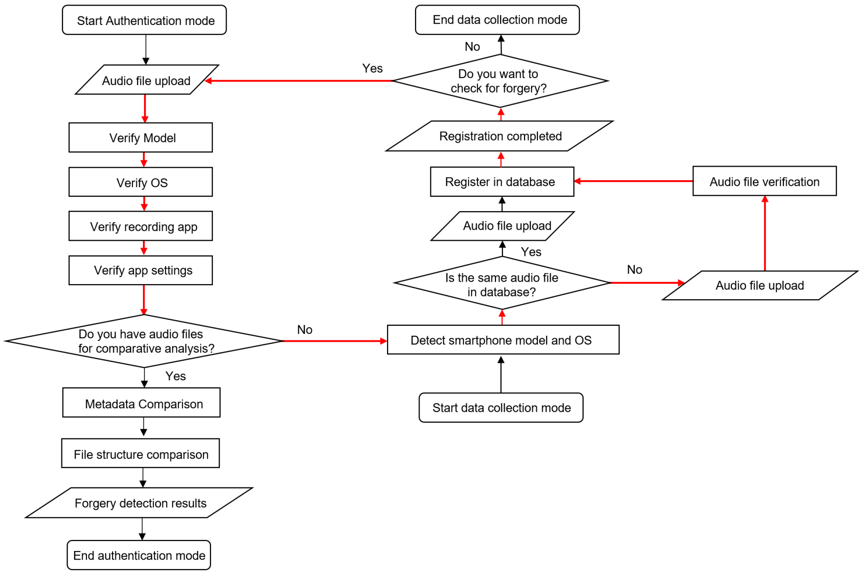


Figure 5. Cyclical procedure based on flowchart

4. INTEGRATED CONTAINER-BASED FORGERY DETECTION AND DATA COLLECTION SYSTEM

4.1. System Overview

The architecture of our system is intricately designed to simultaneously execute two main functions: data collection and forgery detection, through the analysis of metadata and the file structure of audio files. To achieve this, the system is organized into five distinct modules: the User Interface Module, Extraction Module, Analysis Module, Management Module, and Database Module. While not shown here, Figure 6 in the manuscript offers a visual representation of the system's architecture.

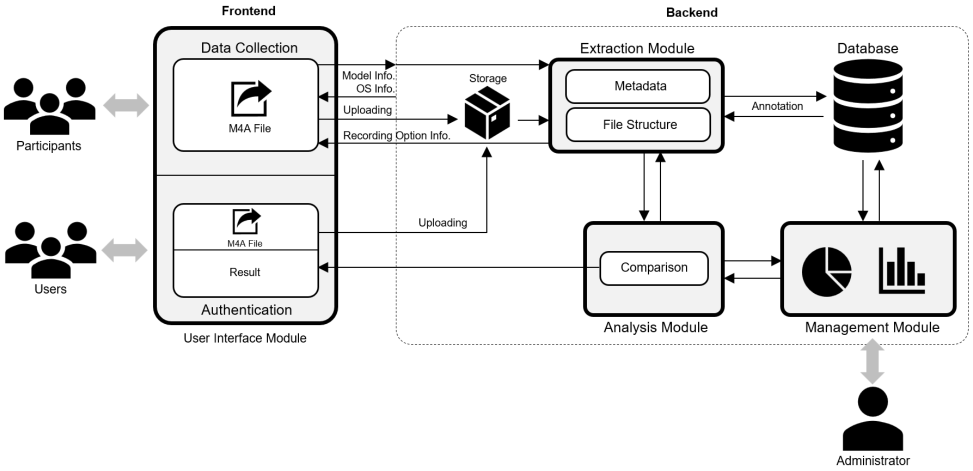


Figure 6. System architecture

In the User Interface Module, we have established two operational modes: Data Collection Mode and Authentication Mode. Data Collection Mode is geared towards crowdsourcing participants, streamlining the upload of audio files to minimize user input and reduce error likelihood, thereby speeding up the process. When users access our service, the server automatically detects the smartphone model and operating system, adjusting the user interface to fit the device specifications. In this mode, uploaded M4A audio files are stored in the repository, triggering the Extraction Module to annotate the files with metadata and file structure information before automatically forwarding them to the database. To further mitigate technical complexity for users, this module introduces a guided process for new users through tutorials, ensuring they can navigate the system effortlessly. Additionally, real-time support and FAQ sections will be incorporated, providing immediate assistance to users encountering difficulties.

Conversely, Authentication Mode is initiated when a file is uploaded for forgery detection. The Extraction Module retrieves metadata and file structure details from the data stored, searching the database for records that match the smartphone model, the closest operating system version, and identical settings. The Analysis Module then evaluates the extracted data against the information in the database to ascertain authenticity, with the findings presented via the Authentication Mode interface. To enhance user understanding and trust in the forgery detection process, detailed explanations of the analysis process and criteria used are made accessible. This transparency aims to demystify the system's operation for non-technical users.

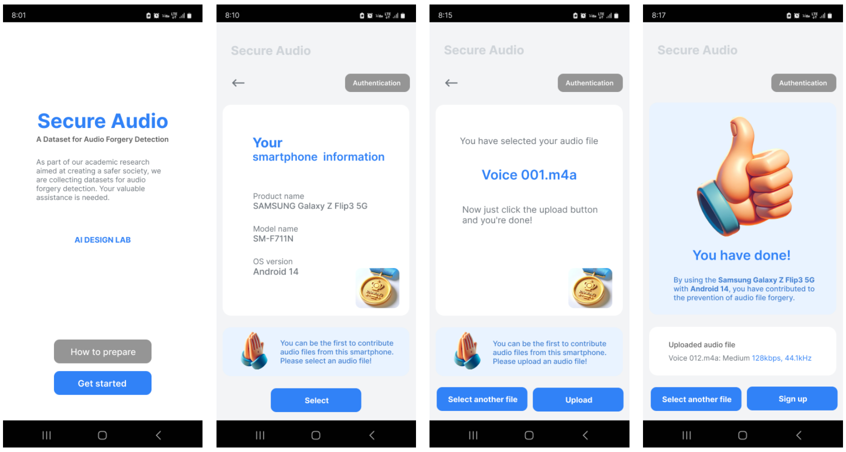
Additionally, our system features a Management Module, essentially a dashboard for administrators to monitor and manage collected data. This module offers tools for visualizing statistical data and generating graphs, facilitating effective data management and analytical insights.

4.2. Implementation

This prototype system has been developed as a mobile web-based system using the Flask framework, with the authors building the strategies for future scalability. Our web-based application is to be containerized because it can be horizontally scaled based on Kubernetes in the future. The choice to be created as a mobile web system was driven by the dataset's independence from smartphone sensor data, prioritizing user accessibility above all else. The primary objective during the data collection phase was to enable participants to upload data swiftly and with minimal errors, thereby enhancing the quality of the data collected.

When participants access the mobile web interface, as illustrated in Figure 7(b), they can immediately verify their smartphone model and operating system. This is achieved by parsing the User-Agent string in the HTTP request headers from the web browser to the server, which extracts details about the smartphone model and OS. As shown in Figure 7(d), information on the recording app settings is provided to participants through an automatic metadata check, ensuring the process is completed successfully. This approach eliminates the need for manual annotation by participants, as annotations are automatically generated, ensuring the verification and authentication of the audio files. For metadata extraction, we used a Python wrapper for the MediaInfo library, pymediainfo 6.1.0 [73], and for extracting file structure information of M4A files, we utilized construct 2.10.70

[74], a library aiding in binary parsing. The extracted data are then stored in a JSON database. Upon completing the upload, participants who wish to use the ranking feature are encouraged to sign up.



As part of our academic research aimed at creating a safer society, we are collecting datasets for audio forgery detection. Your valuable assistance is needed.

You can be the first to contribute audio files from this smartphone. Please select an audio file!

You have selected your audio file

Now just click the upload button and you're done!

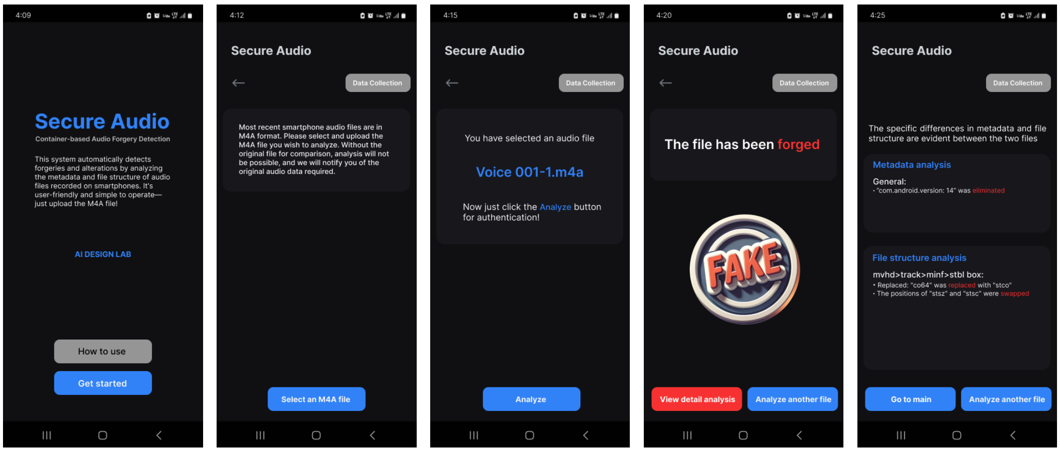
You can be the first to contribute audio files from this smartphone. Please upload an audio file!

By using the **Samsung Galaxy Z Flip3 5G** with **Android 14**, you have contributed to the prevention of audio file forgery.

(a) (b) (c) (d)

Figure 7. UI of data collection mode: (a) Introduction; (b) Selection; (c) Upload; (d) Results

Figure 8 illustrates the forgery detection workflow in our prototype system. The process for detecting container-based forgery is user-friendly: participants need only select and upload a recording file to initiate analysis and receive results. To ensure privacy, uploaded audio files are automatically deleted immediately following the analysis. By selecting the 'Check detail results' button, users can access in-depth comparisons with the original audio files. Should the comparison audio file be absent from the database, the system's analysis of the uploaded file's metadata will reveal crucial details about the original file, such as the smartphone model, operating system, and recording application utilized. Furthermore, users can transition to data collection mode by clicking the 'Go to Upload' button, facilitating seamless navigation within the system.



This system automatically detects forgeries and alterations by analyzing the metadata and file structure of audio files recorded on smartphones. It's user-friendly and simple to operate—just upload the M4A file!

Most recent smartphone audio files are in M4A format. Please select and upload the M4A file you wish to analyze. Without the original file for comparison, analysis will not be possible, and we will notify you of the original audio data required.

You have selected an audio file

Now just click the Analyze button for authentication!

The file has been forged

The specific differences in metadata and file structure are evident between the two files

General:
- "com.android.version: 14" was eliminated

mvhd>track>minf>stbl box:
- Replaced: "co64" was replaced with "stco"
- The positions of "stsz" and "stsc" were swapped

(a) (b) (c) (d) (e)

Figure 8. UI of authentication mode: (a) Introduction; (b) Selection; (c) Upload; (d) Results; (e) Detail Results

4.3. Scenario-based Testing and Validation

To validate the proposed system's capabilities effectively, we conducted scenario-based testing by simulating realistic conditions with various recording process variations. This approach not only demonstrated the system's efficacy but also provided valuable feedback for improving the user interface's quality. In light of the increasing use of voice recording files as evidence in Korean courts and the rising allegations of forgery, we designed a scenario to investigate the potential forgery of digital audio files in legal disputes.

The initial stage of developing the legal dispute scenario involved identifying two key personas: an individual committing the forgery and another responsible for detecting it. This foundational step was essential for the detailed elaboration of the scenario, which we systematically divided into two main phases: the forgery and its subsequent detection. We simulated the act of forgery using the Voice Recorder application on a Samsung Galaxy Z Flip3 with Android 14. Table 2 shows the forgery scenario procedure. The forgery scenario was composed of actions and software used according to the process of audio file forgery.

Table 2. Forgery scenario procedure

Steps	**Actions**	**Software Utilized**
Recording	Record the conversation for court submission	Voice Recorder
Editing & Re-encoding	Remove and save unfavorable statements from the recording file	Voice Recorder
Comparing	Identify discrepancies in the metadata between the original and edited M4A files	MediaInfo app
Editing & Re-encoding	Re-encode and save the edited M4A file	Easy Voice Recorder*
Verification	Verify that the metadata is identical in both original and edited recording files	MediaInfo app
Manipulation	Manipulate the edited recording file to have the same metadata as the original file	HxD
Submission	Submit the forged evidence to court	-

*Easy Voice Recorder is recognized as the most popular app in the Google Play store [36][75].

The detection phase outlines the challenges and necessary processes for identifying forgeries in audio files, that are notoriously time-consuming and costly. These limit the general public's access to specialized services for detecting voice file forgeries. Table 3 presents the workflow of forgery detection in our system within the framework of a legal dispute.

Table 3. Forgery detection procedure in our system

Steps	**Actions**	**System mode**
Recognition	Initially recognize discrepancies in the court-submitted evidence compared to the actual conversation	-
Upload	Upload the evidence to verify if it has been tampered with	Authentication
Results	Unable to analyze due to the lack of a comparative file	Authentication
Acquisition & Upload	Acquire and upload a comparative audio file through personal connections	Data Collection
Completion	Return to the detection page after upload confirmation	Data Collection
Re-Upload	Re-upload the evidence to verify if it has been tampered with	Authentication
Results	Conform the manipulation of the submitted evidence	Authentication
Detail results	Verify why the evidence has been manipulated	Authentication
Submission	Item 5	-

Even though the metadata of the original and forged voice files were identical, detection was possible due to differences in the M4A file structure. In legal contexts, the Korean judiciary relies on the Supreme Court precedent which states: "No signs of editing can be found in the copy of the recording file, and the file information and recording frequency band of this case's recording file copy are the same as those generated by the above digital recorder" [21]. Thus, analysis results from our system identifying such discrepancies will be accepted as evidence in court. The application of our system in these simulated scenarios reaffirmed its practicality and robustness. Scenario-based testing has demonstrated our system's capability to differentiate between original and forged files.

5. CONCLUSIONS

Our research introduces a novel and cyclical methodology for detecting digital audio file forgeries, emphasizing container-based forgery detection and complementing it with mobile crowdsourcing for data collection. This study highlights the critical need for developing practical and scalable solutions in digital forensics, demonstrating the effectiveness of analyzing metadata and file structures. Creating a crowdsourced, diverse audio dataset not only facilitates the identification of forgeries but also serves as a valuable resource for ongoing and future investigations.

The mobile web-based prototype system developed in this study is built on self-reliance, immediacy, and autonomy. Our findings underscore the significance of a self-sustaining, cyclical system in enhancing participant engagement and ensuring its continuous growth. Furthermore, the false positive rate, which refers to incorrectly identifying genuine files as forgeries, is zero. However, because the potential for metadata and file structure manipulation exists, this system has the limitation of false negatives that a manipulated file is incorrectly identified as authentic. Thus, some manipulated voice files may not be detected by this system.

Future works include (1) expanding the dataset to encompass a wider variety of smartphone models, recording applications, and recording settings, (2) integrating with content-based forgery detection techniques based on machine learning, (3) advocating for the public sharing of this dataset, (4) conducting real field testing and external validation with forensic institutions to enhance the credibility and reliability, (5) enhancing the UI/UX of the prototype system to expand participation and the quality of data collected, (6) investigating the interoperability of systems with various technologies to increase their applicability, and (7) exploring the social impact and implications of audio file counterfeiting, including ways to be protected from misuse of this audio file forgery detection technology, through collaboration with experts in linguistics, psychology, and law.

This research is expected to significantly contribute to digital forensics, especially by proposing a cyclical approach to collect diverse audio data and automatically detect forgeries using container-based methods. Additionally, the dataset collected will be made publicly available, serving as a valuable resource for future forensic investigations.

6. DECLARATIONS

6.1. Author Contributions

Conceptualization: J.W.P.; Methodology: J.W.P.; Software: H.S.; Validation: J.W.P. and S.W.P.; Formal Analysis: J.W.P. and H.S.; Investigation: J.W.P.; Resources: J.W.P.; Writing Original Draft Preparation: J.W.P. and S.W.B.; Writing Review and Editing: J.W.P.; Visualization: J.W.P.; All authors, H.S., S.W.B., Y.S., and J.W.P., have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6.3. Funding

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. NRF-2021R1F1A1063884).

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] Q. L. Huynh and V. K. NGUYEN, “Managerial accounting system between corporate governance and knowledge management,” *Access Journal*, vol. 5, no. 2, pp. 306–320, 2024.

[2] D. S. S. Wuisan, R. A. Sunardjo, Q. Aini, N. A. Yusuf, and U. Rahardja, “Integrating artificial intelligence in human resource management: A smartpls approach for entrepreneurial success,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 334–345, 2023.

[3] B. Ustubioglu, G. Tahaoglu, and G. Ulutas, “Detection of audio copy-move-forgery with novel feature matching on mel spectrogram,” *Expert Systems with Applications*, vol. 213, p. 118963, 2023.

[4] A. Ustubioglu, B. Ustubioglu, and G. Ulutas, “Mel spectrogram-based audio forgery detection using cnn,” *Signal, Image and Video Processing*, vol. 17, pp. 2211–2219, 2023.

[5] Y. Son and J. W. Park, “Detecting forged audio files using “mixed paste” command: A deep learning approach based on korean phonemic features,” *Sensors*, vol. 24, p. 1872, 3 2024.

[6] O. Candra, A. Chammam, U. Rahardja, A. A. Ramirez-Coronel, A. A. Al-Jaleel, I. H. Al-Kharsan, I. Muda, G. B. Derakhshani, and M. M. Rezai, “Optimal participation of the renewable energy in microgrids with load management strategy,” *Environmental and Climate Technologies*, vol. 27, no. 1, pp. 56–66, 2023.

[7] K.-W. Kim, “A study on the forensic application of smartphone recording database,” *Journal of Digital Forensics*, vol. 15, pp. 26–42, 2021. [Online]. Available: https://kdfs.jams.or.kr,

[8] P. R. Bevinamarad and M. S. Shirldonkar, “Audio forgery detection techniques: Present and past review,” in *Proceedings of the 4th International Conference on Trends in Electronics and Informatics, ICOEI 2020*, 2020, pp. 613–618.

[9] Q. Aini, U. Rahardja, D. Manongga, I. Sembiring, M. Hardini, and H. Agustian, “Iot-based indoor air quality using esp32,” in *2022 IEEE Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2022, pp. 1–5.

[10] M. A. Qamhan, H. Altaheri, A. H. Meftah, G. Muhammad, and Y. A. Alotaibi, “Digital audio forensics: Microphone and environment classification using deep learning,” *IEEE Access*, vol. 9, pp. 62 719–62 733, 2021.

[11] D. U. Leonzio, L. Cuccovillo, P. Bestagini, M. Marcon, P. Aichroth, and S. Tubaro, “Audio splicing detection and localization based on acquisition device traces,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4157–4172, 2023.

[12] C. Zeng, S. Kong, Z. Wang, K. Li, and Y. Zhao, “Digital audio tampering detection based on deep temporal–spatial features of electrical network frequency,” *Information (Switzerland)*, vol. 14, p. 253, 2023.

[13] D. Apriani, V. T. Devana, A. P. Sagala, P. A. Sunarya, U. Rahardja, and E. P. Harahap, “Security using blockchain-based otp with the concept of iot publish/subscribe,” in *AIP Conference Proceedings*, vol. 2808, no. 1. AIP Publishing, 2023.

[14] U. Rahardja, A. Sari, A. H. Alsalamy, S. Askar, A. H. R. Alawadi, and B. Abdullaeva, “Tribological properties assessment of metallic glasses through a genetic algorithm-optimized machine learning model,” *Metals and Materials International*, pp. 1–11, 2023.

[15] C. Grigoras and J. M. Smith, “Large scale test of digital audio file structure and format for forensic analysis,” in *Proceedings of the AES International Conference*, vol. 2017-June, 2017, pp. 1–6.

[16] D. P. Gangwar and A. Pathania, “Authentication of digital audio recording using file’s signature and metadata properties,” *International Journal of Engineering Applied Sciences and Technology*, vol. 5, pp. 162–165, 2020.

[17] J. Zeng, Q. Lian, and S. Shi, “Forensic originality identification of iphone’s voice memos,” in *Journal of Physics: Conference Series*, vol. 1345, 2019, pp. 52–53.

[18] B. E. Koenig and D. S. Lacey, “Forensic authenticity analyses of the metadata in re-encoded m4a iphone ios 12.1.2 voice memos files,” in *Proceedings of the AES International Conference*, vol. 2019-June, 2019, pp. 1–8.

[19] N. I. Park, J. W. Lee, K. S. Shim, J. S. Byun, and O. Y. Jeon, "A method of forensic authentication of audio recordings generated using the voice memos application in the iphone," *Forensic Science International*, vol. 320, p. 110702, 2021.

[20] M. Michałek, "The characteristics of popular audio recording applications installed on smartphones with an android operating system in relation to forensic audio analyses," *Z Zagadnien Nauk Sadowych*, vol. 120, pp. 335–361, 2019.

[21] J. W. Park, W. J. Kwak, and J. S. Lee, "A study on forgery techniques of smartphone voice recording file structure and metadata," *The Journal of the Convergence on Culture Technology (JCCT)*, vol. 8, pp. 807–812, 2022. [Online]. Available: http://dx.doi.org/10.17703/JCCT.2022.8.6.807

[22] S. W. Baek, H. Son, and J. W. Park, "Limitations of analyzing metadata and file structure of audio files for legal evidence: Focusing on samsung smartphones," *The Journal of the Convergence on Culture Technology (JCCT)*, vol. 9, pp. 1103–1109, 2023. [Online]. Available: http://dx.doi.org/10.17703/JCCT.2023.9.6.1103

[23] T. Hariguna, B. B. Madon, and U. Rahardja, "User'intention to adopt blockchain certificate authentication technology towards education," in *AIP Conference Proceedings*, vol. 2808, no. 1. AIP Publishing, 2023.

[24] T. Holwerda. (2023) Nearly 500 brands exited smartphone market during 2017-2023. https://www.osnews.com/story/137210/nearly-500-brands-exited-smartphone-market-during-2017-2023/. Accessed:(30 March 2024).

[25] S. I. Al-Hawary, J. R. N. Alvarez, A. Ali, A. K. Tripathi, U. Rahardja, I. H. Al-Kharsan, R. M. Romero-Parra, H. A. Marhoon, V. John, and W. Hussian, "Multiobjective optimization of a hybrid electricity generation system based on waste energy of internal combustion engine and solar system for sustainable environment," *Chemosphere*, vol. 336, p. 139269, 2023.

[26] Y. Son, W. J. Kwak, and J. W. Park, "Spectrogram dataset of korean smartphone audio files forged using the "mix paste" command," *Data*, vol. 8, p. 183, 12 2023.

[27] R. Widayanti, M. H. R. Chakim, C. Lukita, U. Rahardja, and N. Lutfiani, "Improving recommender systems using hybrid techniques of collaborative filtering and content-based filtering," *Journal of Applied Data Sciences*, vol. 4, no. 3, pp. 289–302, 2023.

[28] M. Zakariah, M. K. Khan, and H. Malik, "Digital multimedia audio forensics: past, present and future," *Multimedia Tools and Applications*, vol. 77, pp. 1009–1040, 2018.

[29] C. Lukita, N. Lutfiani, A. R. S. Panjaitan, U. Rahardja, M. L. Huzaifah *et al.*, "Harnessing the power of random forest in predicting startup partnership success," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*. IEEE, 2023, pp. 1–6.

[30] U. Rahardja, P. A. Sunarya, N. Lutfiani, M. Hardini, and H. R. Dananjaya, "Analysis of renewable energy utilization using solar power technology in eliminating microplastic emissions," in *2022 IEEE Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2022, pp. 1–6.

[31] E. P. Harahap, E. Sediyono, Z. A. Hasibuan, U. Rahardja, and I. N. Hikam, "Artificial intelligence in tourism environments: A systematic literature review," *2022 IEEE Creative Communication and Innovative Technology (ICCIT)*, pp. 1–7, 2022.

[32] H. Chen and J. Ren, "The effect of influencer persona on consumer decision-making towards short-form video ads—from the angle of narrative persuasion," in *International Conference on Human-Computer Interaction*. Springer, 2022, pp. 223–234.

[33] J. Feldkamp, "The rise of tiktok: The evolution of a social media platform during covid-19," *Digital responses to Covid-19: Digital innovation, transformation, and entrepreneurship during pandemic outbreaks*, pp. 73–85, 2021.

[34] R. Z. Rasyad, R. M. Mayasari, and M. N. Madani, “New era normal: Manajemen pemasaran hotel untuk penjagaan pelanggan dalam,” *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 4, no. 2, pp. 94–98, 2023.

[35] O. Bazaluk, M. A. Rahman, N. M. Zayed, M. Faisal-E-Alam, V. Nitsenko, and L. Kucher, “Crowdsourcing review: the crowd workers’ perspective,” *Journal of Industrial and Business Economics*, pp. 1–20, 2024.

[36] U. Kustiawan *et al.*, “Pengaruh kepemimpinan autentik dan kepercayaan kepemimpinan terhadap perilaku kewarganegaraan organisasi (ocb) dan kinerja karyawan: Indonesia,” *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 4, no. 2, pp. 64–69, 2023.

[37] F. Serafini and S. F. Reid, “Multimodal content analysis: expanding analytical approaches to content analysis,” *Visual Communication*, vol. 22, no. 4, pp. 623–649, 2023.

[38] L. Nassar and F. Karray, “Overview of the crowdsourcing process,” *Knowledge and Information Systems*, vol. 60, pp. 1–24, 2019.

[39] I. Khong, “The circular economy’s performance and the impact of digitalization,” *International Transactions on Education Technology*, vol. 2, no. 1, pp. 18–23, 2023.

[40] R. Simpson, K. R. Page, and D. D. Roure, “Zooniverse: Observing the world’s largest citizen science platform,” in *WWW 2014 Companion - Proceedings of the 23rd International Conference on World Wide Web*, 2014, pp. 1049–1054.

[41] R. F. Sari, A. F. Rochim, E. Tangkudung, A. Tan, and T. Marciano, “Location-based mobile application software development: Review of waze and other apps,” *Advanced Science Letters*, vol. 23, pp. 2028–2032, 2017.

[42] J. Nugent. (2019) Migrate to mobile with ebird breadcrumb. https://www.nsta.org/science-teacher/science-teacher-novemberdecember-2019/migrate-mobile-ebird/. Accessed:(30 March 2024).

[43] R. Widayanti and L. Meria, “Business modeling innovation using artificial intelligence technology,” *International Transactions on Education Technology*, vol. 1, no. 2, pp. 95–104, 2023.

[44] A. Dudhat and V. Agarwal, “Indonesia’s digital economy’s development,” *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 4, no. 2, pp. 109–118, 2023.

[45] T. A. D. Lael and D. A. Pramudito, “Use of data mining for the analysis of consumer purchase patterns with the fpgrowth algorithm on motor spare part sales transactions data,” *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 4, no. 2, pp. 128–136, 2023.

[46] E. D. Safitri, S. R. P. Junaedi, and A. Priono, “Swot analysis is used in the startup business development strategy,” *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 2, pp. 136–142, 2023.

[47] Y. Wu and G. Cao, “Videomec: A metadata-enhanced crowdsourcing system for mobile videos,” in *Proceedings - 2017 16th ACM/IEEE International Conference on Information Processing in Sensor Networks, IPSN 2017*, 2017, pp. 143–154.

[48] Z. Cheng and Y. Li, “Like, comment, and share on tiktok: Exploring the effect of sentiment and second-person view on the user engagement with tiktok news videos,” *Social Science Computer Review*, vol. 42, no. 1, pp. 201–223, 2024.

[49] Y. Wang, X. Jia, Q. Jin, and J. Ma, “Mobile crowdsourcing: Architecture, applications, and challenges,” in *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*, 2015, pp. 1127–1132.

[50] M. Allahbakhsh, B. Benatallah, A. Ignjatovic, H. R. Motahari-Nezhad, E. Bertino, and S. Dustdar, “Quality control in crowdsourcing systems: Issues and directions,” *IEEE Internet Computing*, vol. 17, pp. 76–81, 2013.

[51] R. Nakatsu and E. Grossman, “Designing effective user interfaces for crowdsourcing: An exploratory study,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8016 LNCS, 2013, pp. 221–229.

[52] G. Ravi, M. F. Nur, and A. Kiswara, “Analyzing changes in traditional industries: Challenges and opportunities in the e-commerce era,” *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 1, pp. 39–49, 2023.

[53] E. Dollan, B. D. K. Ramadhan *et al.*, “Assessing the outcomes of circular economy and waste management partnerships between indonesia and denmark,” *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 1, pp. 76–83, 2023.

[54] U. Rusilowati, F. P. Oganda, R. Rahardja, T. Nurtino, and E. Aimee, “Innovation in smart marketing: The role of technopreneurs in driving educational improvement,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 305–318, 2023.

[55] Wondershare, “Democreator.” [Online]. Available: https://dc.wondershare.kr/

[56] N. Sutisna *et al.*, “Implementasikan sistem informasi dalam mendukung perilaku pembelian terhadap keputusan pembelian e-commerce,” *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 2, no. 1, pp. 20–30, 2023.

[57] Mediaarea, “Mediainfo.” [Online]. Available: https://mediaarea.net/en/MediaInfo

[58] A. E. Widjaja, S. Yumna, A. Ashar *et al.*, “Model manajemen pemasaran strategis baru untuk kekhususan e-commerce dalam rantai pasokan,” *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 2, no. 1, pp. 65–72, 2023.

[59] M. H. R. Chakim, P. A. Sunarya, V. Agarwal, I. N. Hikam *et al.*, “Village tourism empowerment against innovation, economy creative, and social environmental,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2sp, pp. 162–174, 2023.

[60] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and R. Efendy, “Innovation and key benefits of business models in blockchain companies,” *Blockchain Frontier Technology*, vol. 2, no. 2, pp. 24–35, 2023.

[61] D. Kundana *et al.*, “Data driven analysis of borobudur ticket sentiment using naïve bayes.” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2sp, pp. 221–233, 2023.

[62] M. Purno, F. Nurbaiti, S. Bakhri, and A. A. Yusuf, “Factors affecting stock prices in jakarta islamic index (jii) for the period 2018-2020,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 1Sp, pp. 84–96, 2023.

[63] I. C. Kawi and W. Pontjoharyo, “Integrating buddhist principles into management control systems: A cattari ariya saccani approach,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2sp, pp. 146–161, 2023.

[64] L. Aliyah, C. Lukita, G. Pangilinan, M. Chakim, and D. Saputra, “Examining the impact of artificial intelligence and internet of things on smart tourism destinations: A comprehensive study.” *Aptisi Transactions on Technopreneurship*, vol. 5, pp. 135–145, 2023.

[65] S. Pranata, K. Hadi, M. H. R. Chakim, Y. Shino, and I. N. Hikam, “Business relationship in business process management and management with the literature review method,” *ADI Journal on Recent Innovation*, vol. 5, no. 1Sp, pp. 45–53, 2023.

[66] Codeine Wong, “Mp4 inspector.” [Online]. Available: https://sourceforge.net/projects/mp4-inspector/

[67] Maël Hörz, “Hxd.” [Online]. Available: https://mh-nexus.de/en/downloads.php?product=HxD20

[68] M. Hardini, R. A. Sunarjo, M. Asfi, M. H. R. Chakim, and Y. P. A. Sanjaya, “Predicting air quality index using ensemble machine learning,” *ADI Journal on Recent Innovation*, vol. 5, no. 1Sp, pp. 78–86, 2023.

[69] K. Symons, I. Vanwesenbeeck, M. Walrave, J. Van Ouytsel, and K. Ponnet, “Parents’ concerns over internet use, their engagement in interaction restrictions, and adolescents’ behavior on social networking sites,” *Youth & Society*, vol. 52, no. 8, pp. 1569–1581, 2020.

[70] M. H. R. Chakim, A. Kho, N. P. L. Santoso, and H. Agustian, “Quality factors of intention to use in artificial intelligence-based aiku applications,” *ADI Journal on Recent Innovation*, vol. 5, no. 1, pp. 72–85, 2023.

[71] N. Lutfiani, S. Wijono, U. Rahardja, A. Iriani, Q. Aini, and R. A. D. Septian, “A bibliometric study: Recommendation based on artificial intelligence for ilearning education,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 2, pp. 109–117, 2023.

[72] M. A. A. Faruq, M. R. Bassalamah, D. Sudaryanti, and N. N. Azizah, “Hedonic values and utilitarian values to improve behavioral intentions and consumer satisfaction on product,” *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 319–333, 2023.

[73] Louis Sautier, “pymediainfo.” [Online]. Available: https://pypi.org/project/pymediainfo/

[74] Arkadiusz Bulski and Tomer Filiba and Corbin Simpson, “construct.” [Online]. Available: https://pypi.org/project/construct/

[75] Digipom, “Easy voice recorder.” [Online]. Available: https://www.digipom.com/portfolio-items/easy-voice-recorder/