Naif Arab University for Security Sciences
**Journal of Information Security and Cybercrimes Research**
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

# A Novel Hybrid Method for Effective Identification and Extraction of Digital Evidence Masked by Steganographic Techniques in WAV and MP3 Files

**Mohamed C. Ghanem*, Maider D. Uribarri, Ramzi Djemai, Dipo Dunsin, Istteffanny I. Araujo**
Cyber Security Research Centre, London Metropolitan University, London, United Kingdom.

*Received 17 Sep. 2023; Accepted 11 Nov. 2023; Available Online 30 Dec. 2023.*

## Abstract

Anti-forensics techniques, particularly steganography and cryptography, have become increasingly pressing issues affecting current digital forensics practices. This paper advances the automation of hidden evidence extraction in audio files by proposing a novel multi-approach method. This method facilitates the correlation between unprocessed artefacts, indexed and live forensics analysis, and traditional steganographic and cryptographic detection techniques. In this work, we opted for experimental research methodology in the form of a quantitative analysis of the efficiency of the proposed automation in detecting and extracting hidden artefacts in WAV and MP3 audio files. This comparison is made against standard industry systems. This work advances the current automation in extracting evidence hidden by cryptographic and steganographic techniques during forensic investigations. The proposed multi-approach demonstrates a clear enhancement in terms of coverage and accuracy, notably on large audio files (MP3 and WAV), where manual forensic analysis is complex, time-consuming and requires significant expertise. Nonetheless, the proposed multi-approach automation may occasionally produce false positives (detecting steganography where none exists) or false negatives (failing to detect steganography that is present). However, it strikes a good balance between efficiently and effectively detecting hidden evidence, minimising false negatives and validating its reliability.

## I. Introduction

In the current era, life is considered incomplete without the Internet, as everyone has some data to transmit and receive. Data secrecy and privacy play a vital role in transferring sensitive data over the Internet. In a world in dire need of technology, thousands of innovations take place everywhere and all the time, not just in protection, but in criminality. With the rapid advancement of technology in every field, people demanded high-performance communication platforms. Many individuals claim that technology has transformed the world into a global interconnected community. Various devices and platforms are required to communicate over the Internet and communication plays a crucial role in the modern era, where people want to reach one another rapidly independent of location [1]. Communication comes from

**Keywords:** Anti-Forensics, Steganography, Steganalysis, Cryptography, Data Hiding, Digital Forensics, Cybercrime Investigation, WAV; MP3, Exterro FTK, Magnet AXIOM.

Production and hosting by NAUSS

* Corresponding Author: Mohamed C. Ghanem
Email: ghanemm@staff.londonmet.ac.uk

doi: 10.26735/IZBK9372

the start of human life; one could even say it is one of the basic needs of people. People have introduced a variety of services based on basic mechanisms to communicate over the Internet. Individuals over 30 years old working and playing in this field can recognise the fast development and changes applied. With rapid adoption, where a sender and receiver are connected through a medium to exchange messages, communication becomes a target for attackers looking to disrupt communication patterns for various purposes. Different attacks and security breaches have been carried out by malicious users, but the communication medium has been less affected compared to direct information attacks, where information is either directly taken or manipulated by intruders. The information transmitted over the Internet from sender to receiver is taken by the attacker using various methods, such as phishing, spoofing, sniffing and man-in-the-middle attacks. Consequently, numerous security-based mechanisms were introduced and implemented to make secure communication possible. Firstly, the information hidden by using text shifting and substitution methods failed to provide a prominent level of security. Such techniques were easy to break because of the static key set by the sender. With the enhanced popularity and demand for security, an old but improved technique persists in the communication world, known as encryption, with various new forms and algorithms today [1]. Encryption is an important method for people and organisations to protect sensitive data from hackers. It is a technique where the text is transformed or converted into a code that is unintelligible to the attacker. The attacker may successfully get the message, but it is unreadable. The encoded information needs to be decoded first by using the key set by the sender. The sender and receiver use the same key to convert text into cypher text and then the cypher text back to plain text. Moreover, while these techniques help to scramble the data, they can still be breached by hackers based on the vulnerabilities of each method. Therefore, steganography is a valuable method to apply as it hides the data, rendering it invisible [3]-[5].

This research proposes a novel multi-approach steganography detection method in the context of audio files and considers the existing steganography and cryptography techniques. This work also elaborates on the current state of the art in terms of proposed hidden evidence detection and extraction approaches, the current challenges, and limitations in the field of audio forensics, as well as future research directions. This paper comprises five sections, in section 2 we introduce a comprehensive literature review with a deep critical analysis of related works. In section 3, we detail the proposed research methodology and reflect on the choices made. In Section 4 we discuss the proposed multi-approach steganographic content detection and extraction providing a detailed diagram. In section 5, we present the implementation and testing of the system we named StegoHound which embeds the proposed multi-approach method and present the obtained results with a comprehensive analysis. In section 6, we discuss the obtained results and provide a conclusion and further research directions.

## II. Literature Review and Related Works

The current advances in the use of cryptographic and steganographic techniques to conceal information within audio files, along with the methods and techniques employed to automate the process of extracting that information, serve as our starting point to develop an improved approach towards the efficient automation of steganography detection and extraction. Dhamija and Dhaka [4] introduced a steganography technique in which the actual information is hidden in another object, such as a sound, image, video, or watermark. However, as improved strategies emerged concurrently with this prominent level of attacking techniques, attackers also employed them. Steganography in the video was once considered one of the best ways to achieve high security, where the sender conceals data in the video's cover image or uses the LSB technique [6]. Before the development of video-based steganographic techniques, widely used audio-based steganographic approaches relied on spread spectrum encryption. These were later improved by incorporating the Direct Sequence Spread Spectrum (DSSS) phenomenon [8], as the Least Significant Bits became overused. Moreover, clustering is considered a popular and emerging

technology in the real world. Recently, an improved method for concealing information in an image was introduced through a K-means clustering algorithm. The pixel from the video-retrieved image is chosen to hide the information using the K-means clustering mechanism [1]. Despite these advanced techniques, hackers have discovered loopholes to attack and access information. Currently, several researchers are working on developing more useful and robust approaches that are challenging to break. For this reason, many implementations based on combined and hybrid mechanisms are already advancing, and encryption is performed with audio steganography using the DWT strategy [3]. Another attempt to secure the transmitted messages involved a combined strategy based on DES for DCT with image steganography, introduced in [7]. In addition, a steganography approach employing the Fibonacci sequence [5] conceals data using a traditional flow but employs the method to generate values for encoding pixels, utilising the Fibonacci innovative sequence concept, which provides a significant advance in the area. Furthermore, a recent multi-layered approach used information encryption based on genetic algorithms and residual numbers to achieve a secure environment for message transmission [2]. In total, we have enumerated eight families of detection and extraction approaches.

### *A. A Steganographic Approach Based on Clustering for Secure Data Communication*

Secure communication is challenging in contemporary times, and numerous researchers have proposed various solutions to overcome this security challenge, yet many of them still exhibit numerous flaws. SaiKrishna et al. [1] identified a trending issue and proposed a strategy to improve the security factor while transmitting messages, based on LSB substitution. Other researchers contributed to the research by combining steganography with K-means clustering techniques [9].

The clustering distinguishes this article from previous studies; the authors discovered that by employing the K-means clustering procedure, pixels can be divided to enhance secure communication. The proposed methodology has presented a novel approach to improving communication security, but the actual implementation of the methods was suggested for future work. Fig. 1 illustrates the basics of the approach, which also includes an encryption phase, as opposed to relying solely on steganography.

The work in [10] articulated clear and concise facts in the steganography detection domain. By understanding and conducting experiments, it provided a comprehensive comparative analysis based on the output of previous works, notably [11]-[17].

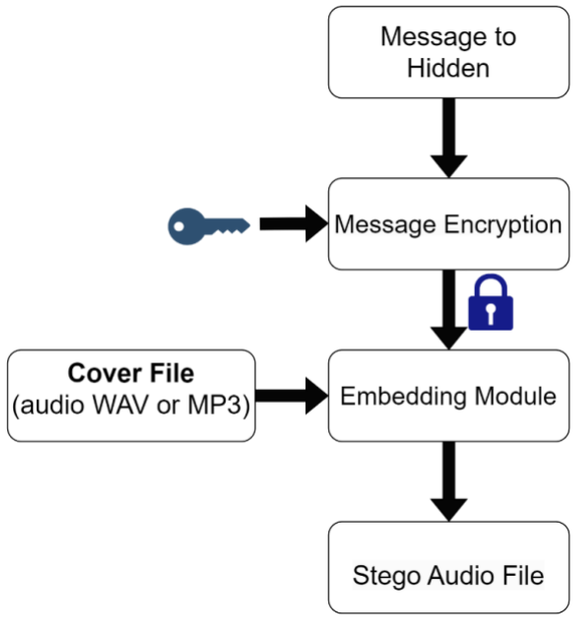


Fig. 1. Modern Steganography Information Hiding Phases in Audio Files..

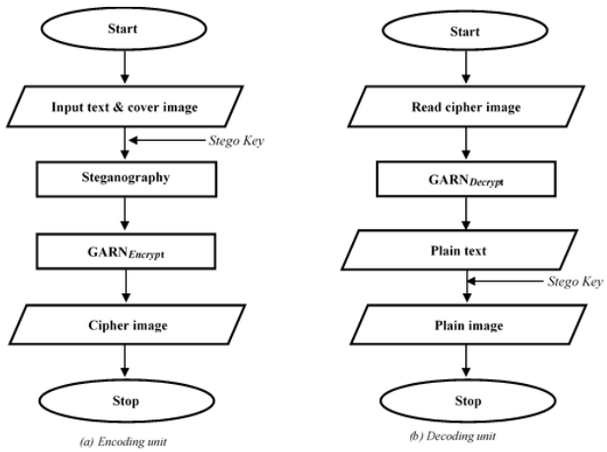


Fig. 2. GARN Algorithm Flowchart [2].

*B. Encryption and Decryption of Multi-Layer Data using Genetic Algorithms and Residual Numbers*

Baagyere work discusses new techniques unrelated to text encryption or traditional image, audio, and video steganography to enhance the reliability and security of digital data [2]. A multi-layered data encryption approach based on the genetic algorithm (GA), as depicted in Fig. 2, and residual numbers (RN) was employed for this purpose. According to the facts, GA belongs to the category of evolutionary algorithms, while RN is associated with traditional number systems. The researchers focused their efforts on the most effective methodology for the system and implemented it for experimental research to validate the discovery of secure data. The approach provided a secure and reliable steganographic mechanism at the expense of affecting the capabilities of embedded objects.

In [14], the researchers assessed the speed and compared the performance of their proposed scheme to that of existing schemes using key parameters. Complementary works [15] and [16] presented various debatable points on the proposed methodology, suggesting modifications to meet accuracy and effectiveness needs. They covered nearly every aspect of the targeted idea of image steganography. Still, it is noteworthy that utilising the same phenomena for audio and video is possible, and a practical implementation can be applied to test the method

*C. DWT-Based Secure Data Transfer*

Another recent method of security was described by Geethavani, Prasad, and Roopa [3]. Several researchers have recently conducted outstanding work in the field of security, aiming to improve the privacy and confidentiality of data through feature integration [19]. The researchers believe that combining the features of cryptography and audio steganography can result in a more advanced approach, as the strength of one algorithm increases when embedded with another popular technique. They referred to this as a double-lock approach, where the message or plain text is fed into a modified Blowfish algorithm, converting the text to ciphertext.

Following that, the second phase involves performing steganography on audio and encrypting

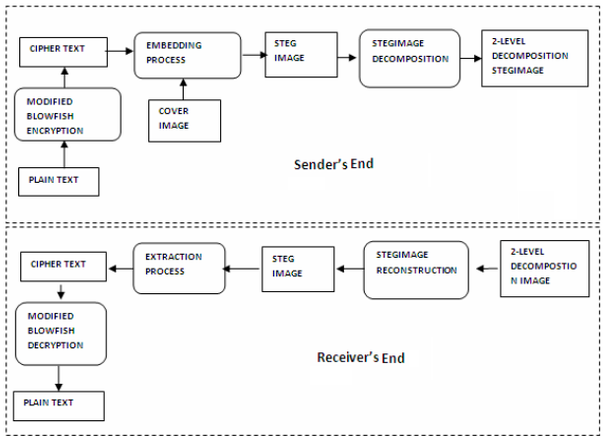


Fig. 3. DWT-Based Secure Data Transfer Framework [3].

it with Discrete Wavelet Transform (DWT). The orthogonal and biorthogonal DWT were employed for different purposes in the study. This approach is intricate because, in the DWT mechanism, the sender sends the ciphertext, which is then converted to the wavelength and reserved at the receiver's end [18], as depicted in Fig. 3.

The selection of these two demanding techniques resulted in distinct and positive societal outcomes, suggesting a better idea to improve information security and channel security [20]. With the help of experimental results, the articulated facts are well-defined, and the validity of the proposed system is evident. This technique can make hacking and other attacks more difficult to carry out. The uniqueness of the concept has left an open horizon for future research. However, there are some limitations to the type of steganographic approach used because one technique is ideal for a few scenarios, but it may not work in all other attacks using a different type of file, as opposed to the audio file used in their experiment.

*D. Steganographic and Cryptographic Method for Safe Cloud Data Migration*

Despite the numerous advantages of cloud computing, it has also faced several security and privacy concerns. Dhamija and Dhaka [4] highlighted the rapid adoption of cloud computing, commenting on its high availability and remarkable performance. In this article, the researchers address security issues and implement a composite strategy to provide high-level security to data transferred

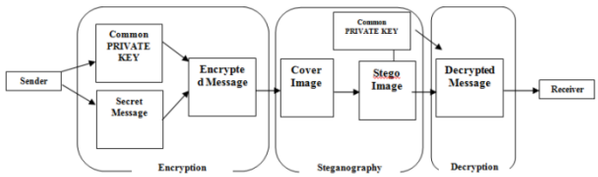


Fig. 4. Steganographic and Cryptographic Process [4].

over the cloud. They employed a two-way security mechanism based on a combined encryption algorithm and steganography technique [13]. While encryption was traditionally used to secure messages, this technique was sometimes replaced by improved approaches of steganography, each with its vulnerabilities. As a result, the authors proposed SCMACS: Secure Cloud Migration Architecture Using Cryptography and Steganography, a novel methodology to conceal data within images [17], as illustrated in Fig. 4.

This approach ensures secure data transmission to databases, later transferring the information to the receiver in encrypted form by using the proposed methodology to secure the information and reduce the likelihood of data loss. The dynamically generated values for the private key make the strategy more challenging to access, requiring further implementation work to conduct additional tests and reinforce the concept. Future work could explore current trends, such as video cryptography, as opposed to image steganography, considered more secure in terms of making steganalysis more difficult [5].

### *E. Steganography with Sub-Fibonacci Sequence*

Security breach attacks are carried out each year with the aim of obtaining valuable information from individuals for various purposes. According to Aroukatos et al. [6], securely concealing information poses a significant challenge. Their team worked on an approach where data is hidden using a traditional flow, with values to encode the pixels generated in a novel way, utilising the Fibonacci sequence concept. The Fibonacci sequence is employed to generate the key, improving upon their previous technique [20], which utilized the LSB of RGB technique. The article clearly explains the workings and limitations of the LSB approach, which were later addressed by using the Fibonacci sequence. This produces results using a base system other than binary, employing an approach not exhausted by previous researchers [5]. The Fibonacci sequence provides an improved mechanism for enhancing data security compared to the LSB approach. The complexity of this sequence makes the key difficult for criminals to gather, and a steganalysis approach cannot decode the sequence easily. Further research on this technology is recommended to determine the detailed criteria for selecting the encoding sequence.

### *F. DNA and KAMLA Approaches in Metamorphic Cryptography*

According to Singh et al. [6], life today would be deemed incomplete without the Internet, as everyone has something to send and something to receive online, hence, data secrecy and privacy are crucial. Previously, data transit over the internet was secure through encryption mechanisms. Several cryptographic schemes were proposed to enhance security, including the RSA method based on a singular cubic curve, JCE, a metamorphic cryptography method, an encryption method based on an indexing chaotic sequence ICSECV, a real-time video encryption method, and a metamorphic cryptography method using auditory information via a carrier wave. [21]. However, these cryptographic schemes quickly became outdated due to advancing cyberattacks and the availability of powerful resources for attackers. Consequently, attackers can launch a brute-force attack on encrypted data transmitted over the Internet.

The DNA and Kamla method address potential issues in securing internet-based information transmission. The technique employs a DNA approach to encrypt data transmitted over the Internet through a seven-step process. This process includes some special steps at the sender's end, such as applying a DNA process to the resulting keys and data after converting the data to ASCII bits. The KALMA technique is used in the final step to conceal the message in DNA bases [22]-[25]. To decrypt the received encrypted message at the receiver's end, the reverse approach is used to obtain the original message. This proposed scheme outperforms previously used techniques in terms of robustness, payload size, visual detection,

and steganography in this context. Combining cryptographic techniques, such as steganography methods and encryption, results in a highly secure environment. The DNA approach demonstrates satisfactory robustness, and the use of the KALMA approach results in a high payload. To expand on this work, different carrier mediums and DNA versions can be explored to improve the payload and security of digital data transmission [26].

### *G. DES and DCT-Based Steganography*

The frequency of attacks on confidential data increased with technological advancements [29]. cryptographic methods of encryption and steganography are two widely used techniques for protecting digital information. However, several researchers have pointed out security concerns and suggested a reliable way to safeguard data [30]. According to Ramaiya [31]-[34], the best approach is to combine methodologies. They proposed two popular approaches, incorporating the DES algorithm and another via the discrete cosine transform (DCT) to overcome vulnerabilities in older approaches. Solichin and Ramadhan [35]-[38] proposed a method for securing Word, Excel, PDF, and PowerPoint documents into their secured versions [36]. Due to the high demand for DES, researchers prefer to use that algorithm for encryption and then employing the DCT approach to reveal the message hidden in the cover image. This combination of different techniques already in use enhances security [37]. The combination of DES and DCT steganographic methods has proven to improve data security, but achieving a high functional rate requires reducing computational time. Researchers conducted experiments to provide evidence for the proposed approach, and the results were as expected [38], expanding on previous research on the steganographic use of combining various cryptographic methods such as RSA, DES, AES, and Blowfish. however, they have not included a DWT comparison in this instance [39].

### *H. Encrypted Audio Steganographic System Based on Spread Spectrum*

According to Anjana et al. [8], communication always requires a smooth and secure path. Several algorithms have been introduced to provide a secure channel to transmit data, but some have failed due to their poor tackling power [40].

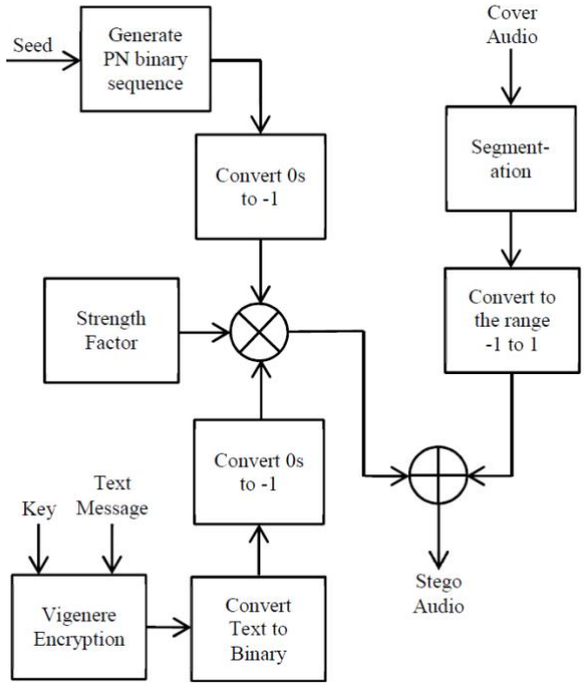


Fig. 5. The Standard Embedding Process [8].

Researchers have used audio steganography to enhance the security mechanism [41] based on the Direct Sequence Spread Spectrum (DSSS) scheme. By combining steganography and encryption, the algorithm provides additional security [42]. Performance measures such as BER, Ratio of Signal to Noise, Peak Signal to Noise, Vigour Feature, Chip Frequency, and others were employed to evaluate the proposed system's imperceptibility, security, detectability, distortion, capacity, and accuracy. This approach establishes a secure and reliable steganographic mechanism, albeit at the cost of affecting the entrenching volume [28]. Fig. 5 illustrates the embedding process of this technique. This DSSS mechanism represents a significant step toward improving traditional methods, providing a novel direction of work, as well as computational metrics that are useful for implementation and decision-making due to their measured values [24].

The system is developed to conceal messages, such as cyber intelligence text, where small messages must be communicated with elevated levels of required security. However, enhancing the capabilities to cover audio content could improve the

steganographic capacity limitation of the message. This limitation is influenced by a wide range of parameters used in the experimental designs and numerous other factors, all of which contribute to obtaining more improved results. A change in the chosen factors could have a broader impact on the contribution [8] of the research.

## III. Research Methodology

The methodology for this work blends conceptualisation, development, and experimentation which was explicitly designated to problem-solve the issue of automating the extraction of evidence hidden with cryptographic and steganographic techniques. The output of this work is a multi-approach system that ensures an efficient, effective, and accurate automated detection of steganographic and cryptographic artefacts in audio files. The chosen methodology for this research is as follows:

1. Attaining an in-depth domain understanding through a literature review and critical analysis of related works.
2. Shortlisting, selecting, and validating appropriate steganographic and cryptographic detection methods.
3. Determining the sequential order of the selected methods in the context of experimental conditions.
4. Introducing scheduled modifications to one or more variables.
5. Testing the proposed multi-approach detection in different-sized WAV and MP3 files, measuring, and controlling the used variables.

### *A. Decision on Sample Datasets*

The most serious perceived issue with steganography from a forensics point of view is never being 100% assured of the cleanness of the datasets, ensuring they are free from hidden artefacts and determining the compatibility of the file types that can host data. The most common form of steganography uses a file type that is not commonly employed. Image steganography can sometimes be seen as the first option and exhausted; thus, audio files will be the sample dataset. WAV files, in particular, containing encrypted data, such as a zip file, are preferred for this experiment. We designed and implemented a dataset generator which allowed us to generate 320 audio files of different lengths, ranging from 10 seconds to 1600 seconds, each with a proportionate amount of steganography contents hidden within. This dataset is divided equally between WAV and MP3 audio files.

### *B. Data Analysis Models*

This research uses two statistical models: inferential statistics, which enables the prediction of a hypothesis based on data obtained from testing that was tampered with to analyse it as a potential steganographic file. Many unprocessed artefacts result from the data-hiding technique used in this research. Moreover, the data obtained from the testing tools were analysed using empirical data analysis.

### *C. Result Analysis Metrics*

The results were analysed by comparing current tools with the project toolkit to determine which tools successfully identified steganography, which tools detected encryption, and which tools could identify and uncover the sample data. The tools were tested against a variety of sample datasets, including WAV and MP3 files, as well as encrypted text and graphic files. The hidden data used for testing included ZIP files, encrypted TXT, PNG or DOCX files. To eliminate discrepancies, each tool was tested multiple times with the same type of data. In summary, the metrics adopted for evaluating the efficiency and accuracy of the automation are the detection rate, indicating the number of hidden artefacts identified and extracted, as well as the number of false positives and false negatives.

## IV. Proposed Multi-Approach Steganographic Content Detection and Extraction

In this section, a detailed account of the proposed multi-approach detection mechanism is provided. Initially, the proposed method accounts for any captured data, whether stored or transmitted in digital format, and thus can be used as evidence in a legal case, referred to as digital evidence. This includes emails, text messages, media content,



social media posts, computer files, and other types of digital data. The following are the twelve phases constituting the multi-approach method proposed.

*A. Digital Evidence Acquisition*

The process of obtaining digital images for forensic analysis is referred to as image acquisition. Capturing images from a variety of sources, such as digital cameras, smartphones, tablets, and other digital devices, falls under this category. However, the image acquisition process is important in forensic analysis as it ensures the preservation of the original image in its unaltered state, thereby maintaining the integrity of the evidence.

*B. Live Forensics Analysis (Automated)*

The process of gathering and analysing digital evidence from an active, or live, computer system is known as a live forensics examination. This may entail performing tasks like scanning the RAM of a computer, analysing currently active processes, and logging network traffic. Contrary to conventional forensic examination, which frequently entails taking a snapshot of a computer's hard drive and analysing the data offline, this procedure eliminates such steps.

*C. Forensics Processing, Indexation, and Deleted File Reconstruction*

The process of analysing and deciphering digital evidence gathered during a forensic examination is known as forensic processing. However, this may also involve activities such as locating and extracting pertinent data, confirming the legitimacy of supporting documentation, and maintaining the accuracy of the data throughout the analysis process. Deleted file reconstruction is the process of recovering deleted files from a digital device, which can be done using specialised software to recover the deleted data and then attempting to reconstruct the original files.

Indexation, on the other hand, is the process of creating an index or catalogue of the digital evidence that has been gathered for additional forensics analysis.

*D. Indexed and Recovered WAV and MP3 Files*

Audio files that have been located and restored from a storage device or backup are referred to as indexed and recovered audio files. However, the files may be in the digital audio file formats WAV or MP3, respectively. Nevertheless, MP3 files are smaller in size and have lower audio quality, while WAV files are typically larger and have higher audio quality. These files can be recovered using specialised software even if they have been deleted, formatted, or lost due to other types of data loss.

*E. Tool-Automated Steganography Detection*

Software programs that can automatically scan digital files and detect the presence of hidden data are known as automated steganography detection tools. These tools operate by analysing digital files for patterns or anomalies that may indicate the presence of hidden data. However, statistical analysis of file headers, footers, and other metadata is a common method used by automated steganography detection tools in identifying hidden data.

*F. Flagged Files (Known Files Content)*

The process of identifying and marking specific files or pieces of data within a set of digital evidence for further forensic analysis is referred to as flagged files or indexed searches. This can be done manually by a human forensic expert or using specialised software. The human forensic expert, on the other hand, may use a keyword search to identify relevant files to the case and then flag or index those files for further review. However, performing such tasks requires considerable resources.

*G. Suspected Files Examination Using the Relevant Steganography Tool*

Examining suspect files with the appropriate steganography tool is the process of detecting and analysing hidden data within digital files suspected of containing steganography. A forensics human expert may use a variety of techniques to identify suspect files during a forensic examination, such as keyword searches, file hash comparison, or statistical analysis of file headers and footers. Once suspect files have been identified, the forensics

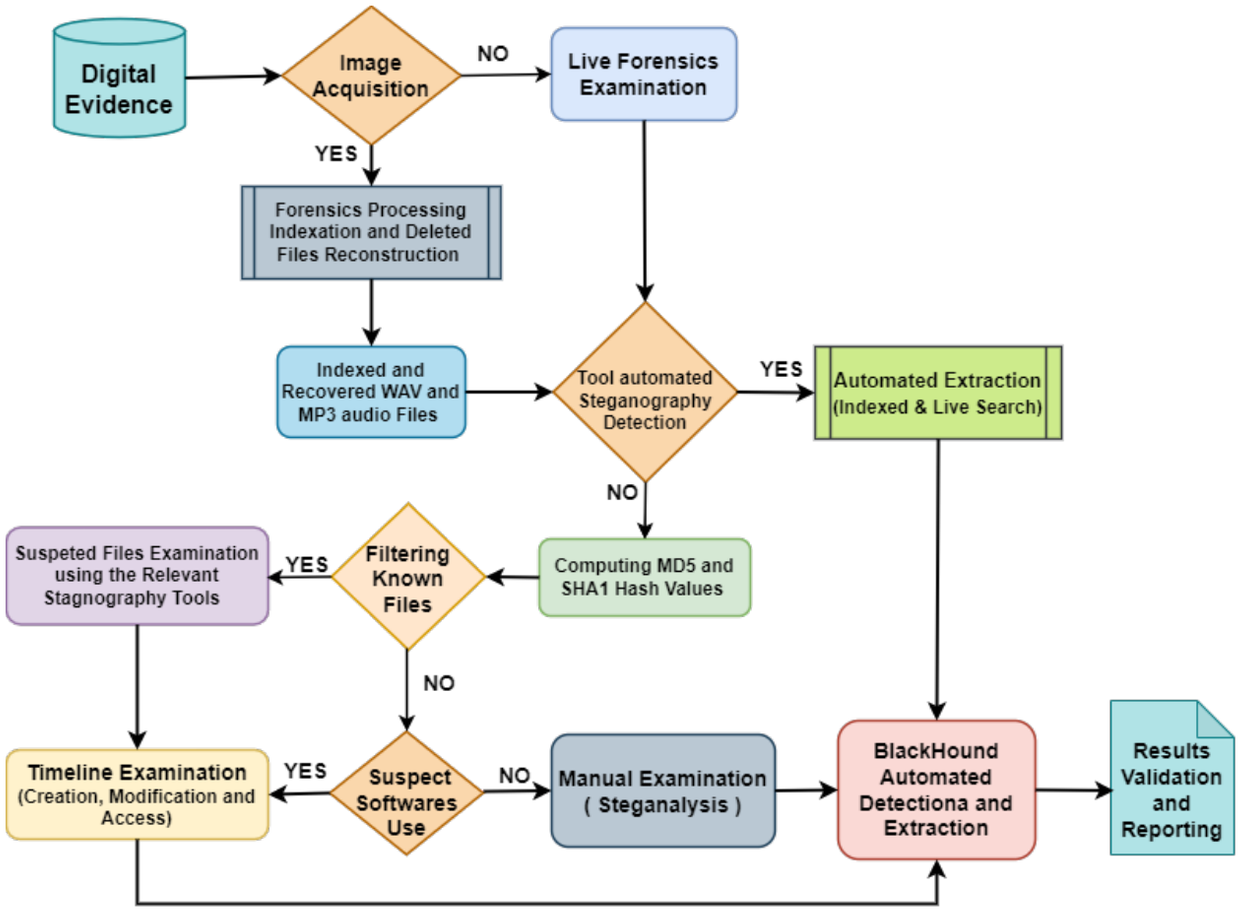


Fig. 6. Proposed Multi-Approach Steganography Detection and Validation Algorithm.

expert can analyse them with a steganography tool to detect the presence of hidden data.

*H. Filtering Using Known File Format KFF*

Filtering known files refers to the technique used by a forensic human expert to identify and remove files from the collected set of digital evidence that are known to be irrelevant. This can be accomplished by comparing the files in the evidence to a database of known files, such as operating system files, common software files, and other types of files that are unlikely to be relevant to the case. However, this file filtering technique can help reduce the amount of data that must be manually reviewed by a human forensic expert.

*I. Computing MD5 and SHA-1 Hash Values*

The MD5 algorithm generates a hash value of 128 bits, while the SHA-1 algorithm generates a hash value of 160 bits. Both algorithms are considered one-way functions. However, in digital forensics, hash values are used to identify and track specific files, verify the integrity of files collected as evidence, and detect if a file has been tampered with. A human forensics expert can manually compute the hash or rely on specialised software such as FTK, AXIOM or UFED to determine if two files are identical by comparing their hash values.

*J. Timeline Analysis (Creation, Modification, and Access)*

The process of creating a chronological representation of events that occurred on a computer or digital device is known as timeline analysis. This may include file creation, modification, and access times, as well as other system events like logon and logoff times and network connections that may be stored in RAM. Timeline analysis, on the other

hand, is a significant practice in digital forensics for identifying patterns of activity or reconstructing events.

*K. Suspect Software Use*

The identification and analysis of software suspected of being used in cybercrime or other legal issues are referred to as suspected software use [36]. Forensic human experts may examine the contents of a computer's hard drive to identify specific software programs that have been installed, or network traffic may be examined to identify the use of specific software tools or protocols to collect traffic data without the administrator's knowledge.

*L. Manual Indexed Forensics Search*

A manual indexed forensic search is a process in which a human forensics expert examines a computer or other digital device in real-time while looking for specific files or information. This method can be used for a variety of purposes, including conducting forensic investigations, locating evidence for a legal case, and recovering lost or deleted data. During a digital forensic investigation, the human forensics expert searching will typically use specialised software and techniques to search the device. Nonetheless, this manual indexed forensic search is performed in real-time, allowing the human forensic expert to quickly retrieve information and make informed decisions. The proposed solution's functioning is graphically summarised in Fig. 6.

## V. Design, Implementation, and Testing

The proposed multi-approaches concatenate in a precise order common detection and analysis techniques to address steganographically hidden content. Therefore, detecting steganography in MP3 and WAV files may require a combination of different techniques and tools to increase the likelihood of detection.

In the first stage, the StegoHound algorithm uses the Statistical Analysis Function (SAF) to identify any subtle changes in the statistical properties of the audio files and seeks to identify deviations from normal patterns. The output of the first stage is crucial in deciding the next stage. If the SAF output is negative, meaning no statistical abnormalities were detected, StegoHound will proceed with Spectrogram Analysis to detect any steganography track through the observation of modified frequency components of an audio signal. Analysing the spectrogram may reveal hidden patterns or anomalies, and StegoHound uses Spek to generate and analyse spectrograms.

In the second stage, StegoHound operates a comprehensive File Signature Analysis (FSA) by comparing the file signatures of suspected files against known steganography tools. It employs the least significant bit (LSB) examination to reveal hidden data within the audio files and detects modifications.

Finally, the fourth stage involves a Forensics Content Analysis (FCA) looking for any alteration of the audio perceptual quality. This toolkit's goal is to provide code and materials for automating the detection of hidden data as well as the retrieval of any discovered data items. It serves as a framework to help forensics professionals find hidden data that might otherwise be missed.

StegoHound is a modular framework that houses several interchangeable Python scripts for detecting encrypted and steganographically hidden data. The toolkit is written in Python 3 and consists of three Python scripts and two test files. The full code and dependencies are provided for free on the GitHub platform.

*A. System Architecture*

The system architecture of StegoHound is based on a standard module structure. Modules are used to integrate all the toolkit's functionality into separate scripts and units, as shown in Fig. 7. To verify file integrity, the source files must be loaded into the extra/music folder to create a comparable hash database.

The 'create_DH_of_audioc.py' script allows for manual digital hash computation; it is the shortest of the three scripts, consisting of 11 lines of code, and serves only to create a hash dictionary of the audio source files. The StegoHound Toolkit maintains a database hash digest of other file types, and this

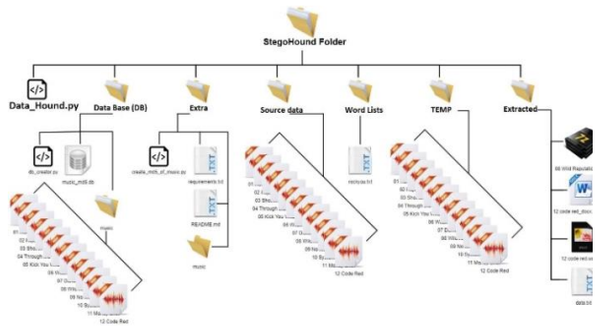


Fig. 7. StegoHound Toolkit Structure.

can be easily accomplished by simply changing the originating data folder and the hash dictionary output. The next step is to execute the 'db_creator.py' script.

This script creates an SQLite3 database containing the SHA1 and MD5 hash digests of the source audio files, which can later be compared. It is currently a remarkably simple database for testing purposes with one table and the three columns ID, song name, and song hash. Different tables per album could be created and stored in a single database, depending on the number of audio files to be checked.

Due to the time-constrained nature of the investigation requiring speed, and the checksums created being used only for file integrity, MD5 and SHA1 were chosen over SHA-256. The user executes StegoHound through all (batch) or individual audio files exported from the forensics image using the FTK imager. The audio files to be analysed for hidden data are saved in the/original_folder. StegoHound makes copies of these files and saves them to the /original_copy; this is for analysis, not the original. The copied files are hashed and compared to the hash of the original files in the database; if there is a difference, StegoHound notifies the user—this is the first sign of file tampering. Then, it uses the file signature to scan the audio file for any hidden files (magic number). An overview of this process can be found in Fig. 8.

Finally, after the detection process, the type of hidden file is identified, and any hidden data is extracted and placed in the extracted folder. If an audio file contains an encrypted zip file,

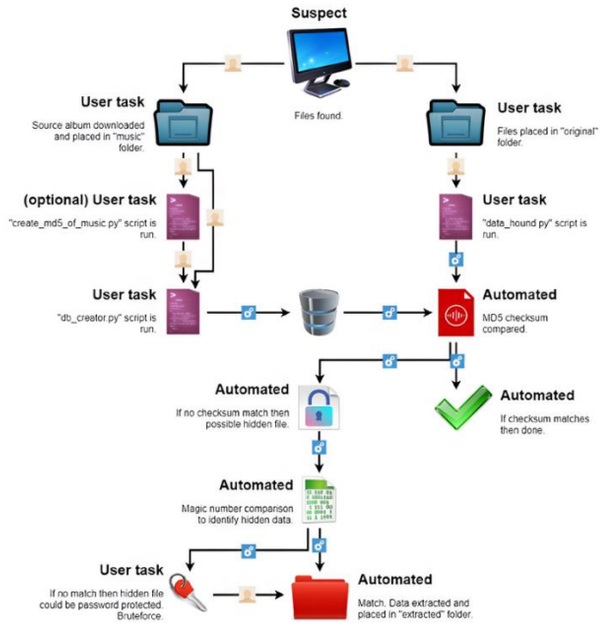


Fig.8. StegoHound Use Case Diagram.

StegoHound will, if prompted, perform a brute-force attack on the password before extracting the decrypted file

and placing it in the extracted folder. An overview of the automated methods is represented in Fig. 9.

### *B. StegoHound Scalability*

The toolkit is built in a modular structure, meaning expansion is possible with the addition of various file types, steganography methods, and encryption methods, all of which are insertable. File types are checked against file signatures, allowing identification of the file type even if the extension has been changed or is non-existent. An example of this is a.wav file that has been compared to the checksum of the source file and found to be incompatible.

This is the first indication that there is hidden content, and just underneath that, it can be observed that the magic number of a file type is being looped through the copied file, revealing the file to contain a 7-Zip archive. The current list of file signatures to check only features the most common file types. The final check of the if-else loop is when an unknown file type is presented to alert for its existence and No match comments.

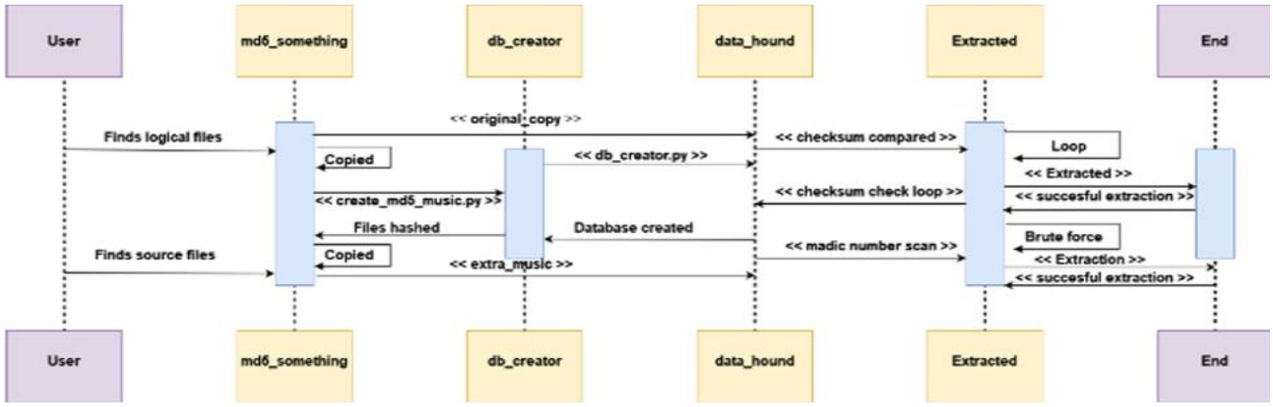


Fig. 9. StegoHound functioning Diagram.

This, like many functions within the toolkit, is expandable, as more file types and their identifying file signatures can be added. In summary, the toolkit focuses on audio files, more specifically .wav files, but the toolkit is expandable in the form of additional units to focus on other file types. Still, it should be noted that various file types can currently be extracted and decrypted.

*C. Testing and Validation*

Detecting steganography in MP3 and WAV files involves analyzing the audio data to identify any hidden information or alterations made through steganographic techniques. In this research, we simulated the masking of docx files, text files, PNG images, and zip files as hidden messages in different size WAV and MP3 audio recordings to evaluate the efficiency and effectiveness of the detection and extraction automation.

These two file extensions were chosen for this research as they are widely used and often picked by criminals to avoid attracting attention when transmitting information [20]. It was critical to test the sample data on current tools to allow a fair comparison between the StegoHound and current use cases, effectively creating a toolkit to remediate the issues previously discussed within the field of digital crime, as well as its vulnerabilities and weaknesses of current techniques.

It was decided to put one open-source solution and one proprietary tool, both of which are commonly used in law enforcement, to the test. The open-source solution was Autopsy, and the proprietary solution was FTK. Because of the need to use the tools correctly, it was also decided that the tools would be ones that the tester is certified to use and has professional knowledge to carry out the tests efficiently. These tools were simply chosen as comparisons due to their popularity and the tester's permission (full licence) to use them.

FTK (Forensic Tool Kit) claims to automatically extract data from PKZIP, WinZip, WinRAR, GZIP, and TAR compressed files [15] and to locate all evidence with 50% thoroughness [2]. In this experiment, FTK could not detect the presence of hidden data, encrypted data, or ZIP files when testing the sample data, so no data hidden within the audio files was extracted using the FTK tool as shown in Fig. 10.

The encrypted text file embedded within this WAV file is not indexed by FTK and AXIOM, with a minor investigative lead raised by FTK, which identifies a deleted file with an unknown format flagged as a potentially encrypted file within the set of recovered deleted files. Additionally, meta-data analysis and notably the Modification, Access, and Creation time data (MAC (Modification, Access, and Creation)) illustrated inconsistencies in the file changes and creation dates and times, which are often considered as an investigative lead for steganography in Windows OSs [27].

However, similar to FTK, Autopsy correctly identified the files as audio files, but it did not find any of the hidden data within them, as illustrated in Fig.11 and Fig. 12 for the number of hidden contents identified in the experiment.

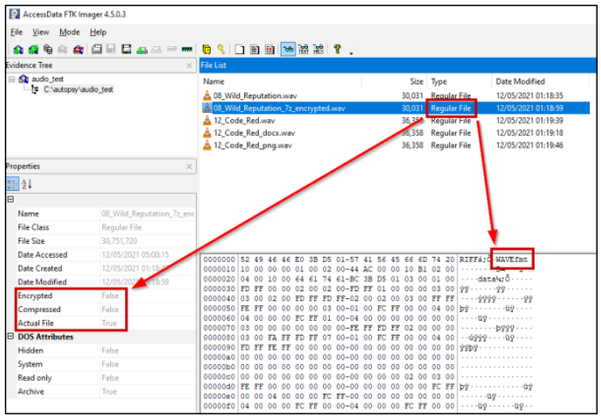

Fig.10. Testing Sample Data in Exterro FTK.

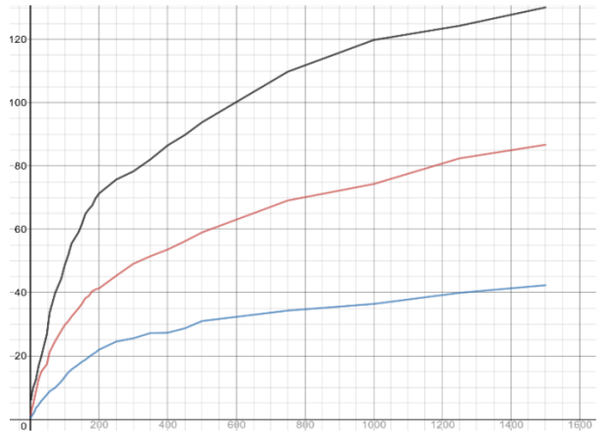


Fig. 11. Number of hidden objects (text or graphics) detected in distinct size WAV audio files (in seconds) using StegoHound automated (black), FTK (red), and manual HEX-Search (blue).

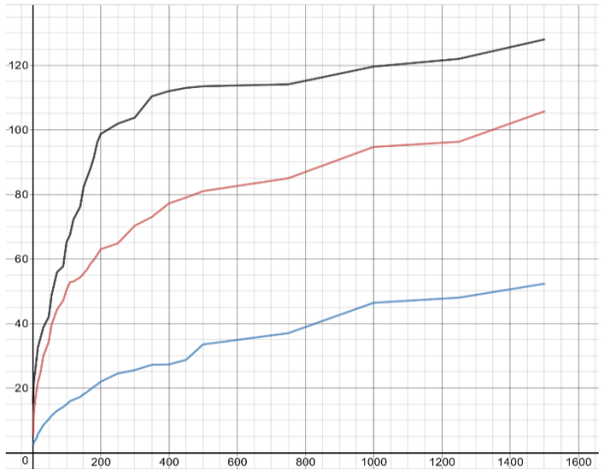


Fig. 12. Number of hidden objects (text or graphics) detected in distinct size MP3 audio files (in seconds) using StegoHound automated (black), FTK (red), and manual HEX-Search (blue).

For comparison and consistency purposes, we carried out a manual hexadecimal investigation using WinHEX, following expert forensics examiner recommendations.

The obtained results confirm the fact that StegoHound outperforms both manual and FTK automated methods in terms of the number of extracted data masked by steganography and cryptographic techniques. The main differences in the number of data extracted are heavily affected by the audio file format (WAV or MP3). The findings suggest that data hidden within MP3 files are more likely to be discovered in different size audio files with lengths varying from 50 seconds to 1500 seconds.

This is due to the compressed nature of MP3 files, which are often smaller (compressed) compared to WAV. Nonetheless, the gap gradually closes, and the detection rates for masked and hidden artefact using steganographic and cryptographic techniques in longer audio files are almost identical.

In addition to these suggestions, an expansion of file signature types would be ideal to enable the scanning and extraction of additional file types, ranging from the most used files to the most obscure documents.

The last set of testing covered the accuracy of detection and extraction through the measure of False Negatives (FN) rate related to the detection of files hidden in WAV and MP3 files. The findings suggest that WAV files produce a higher rate of false negatives but with lower probabilities, while MP3 account for a lower FN rate but with higher probabilities

The FN rate in MP3 is much lower than the data that is accurately identified, but there is room for improvement. This analysis can be visualised in Fig. 13. It is worth highlighting that the StegoHound toolkit includes a database creation script, and it could be expanded to loop through distinct types of data for further FN processing and improvement using file checksums and the use of an industry DB of blacklisted hashes, which would significantly improve the FN reduction.

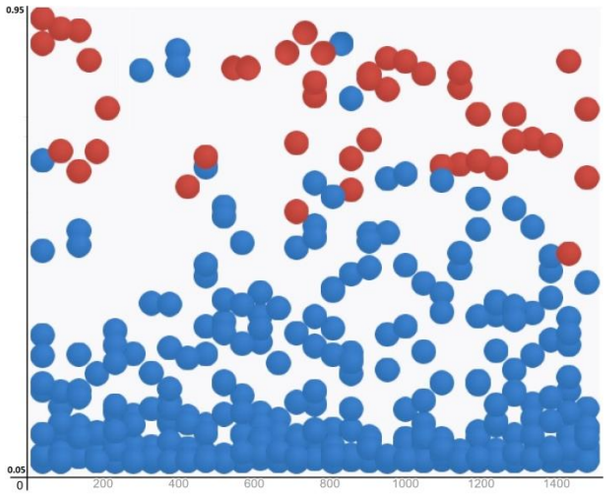


Fig.13. False Negative (FN) steganography and cryptography masked content detection distribution in WAV (Red) and MP3 (blue) audio files.

## VI. Conclusion and Discussions

The use of anti-forensics techniques has been democratised in recent decades, with cybercriminals weaponizing modern technologies to complicate LAE investigative tasks. The results of this work reveal the impacts of combining different steganography detection techniques to enhance the accuracy and efficiency of digital crime investigations. This research proposes a novel, sequential, and multi-approach automation that is considered reliable in addressing the current gap in between efficiency and cost (time and human labour) in steganography detection for law enforcement and corporate purposes. This approach aims to avoid common cases of miscarriage of justice resulting from the complexity of investigations.

The second contribution of the proposed method lies in covering more ground during digital forensics analysis, thereby enhancing the reliability of results and overall case confidence. In the context of audio files, detecting steganography in MP3 and WAV files poses several challenges due to the nature of steganographic techniques and the characteristics of audio files. Current cybercrime trends show a wider adoption of encryption and advanced techniques to mask and secure important messages and data within host files, including audio files. This makes it challenging to detect hidden information and results in Steganalysis Resistance.

In practice, steganography tools are designed to resist detection by employing sophisticated methods that minimize statistical, audible, or perceptual changes in the audio data, fooling most industry digital forensic tools and frameworks. The proposed multi-approach automation validated the impact in terms of efficiency and accuracy, notably on large audio files (MP3 and WAV). Forensic analysis of such files is time-consuming and requires significant computational resources and memory, occasionally producing false positives (detecting steganography where none exists) or false negatives (failing to detect steganography that is present).

Overall, the method tested in StegoHound demonstrated a good balance between accurately detecting hidden data and avoiding false alarms-a challenge in automated steganography detection. The adopted method for automating steganography detection and extraction has proven to be more efficient than existing tools, as evidenced by testing where existing tools failed to uncover the data. The method implemented in the StegoHound is designed to be expandable, due to the modular structure of the scripts. In future works, additional steganographic techniques for audio and video file types could be added to create a more versatile method, with a focus on new identification techniques, notably using AI and ML.

## Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

## Conflict of Interest

Authors declare that they have no conflict of interest.

## References

[1] A. SaiKrishna, S. Parimi, G. Manikandan, and N. Sairam, "A clustering-based steganographic approach for secure data communication," in *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, Nagercoil, India, 2015, pp. 1-5. doi: 10.1109/ICCPCT.2015.7159515.

[2] E. Y. Baagyere, P. A. -N. Agbedemnab, Z. Qin, M. I. Daabo, and Z. Qin, "A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers," in IEEE Access, vol. 8, 2020, pp. 100438-100447. doi: 10.1109/ACCESS.2020.2997838.

[3] B. Geethavani, E. V. Prasad, and R. Roopa, "A new approach for secure data transfer in audio signals using DWT," in *2013 15th International Conference on Advanced Computing Technologies (ICACT)*, Rajampet, India, 2013, pp. 1-6. doi: 10.1109/ICACT.2013.6710492.

[4] A. Delforouzi and M. Pooyan, "Adaptive Digital Audio Steganography Based on Integer Wavelet Transform," in *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007),* Kaohsiung, Taiwan, 2007, pp. 283-286. doi: 10.1109/IIH-MSP.2007.69.

[5] A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT),* Greater Noida, India, 2015, pp. 346-351. doi: 10.1109/ICGCIoT.2015.7380486.

[6] N. Aroukatos, K. Manes, S. Zimeras, and F. Georgiakodis, "Data Hiding Techniques in Steganography Using Sub-Fibonacci Sequences," in *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Piraeus-Athens, Greece, 2012, pp. 89-93. doi: 10.1109/IIH-MSP.2012.27.

[7] C.C. Lin, and P.F. Shiu, "High-Capacity Data Hiding Scheme for DCT-based Images," *J. Inf. Hiding Multim. Signal Process.,* vol. 1, no. 3, 2020, pp. 220-240.

[8] V. K. Singh, S. Pandey, S. Degadwala, and D. Vyas, "DNA and KAMLA Approaches in Metamorphic Cryptography: An Evaluation," in *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, Coimbatore, India, 2022, pp. 1173-1178. doi: 10.1109/ICAIS53314.2022.9742764.

[9] A. Solichin and E. W. Ramadhan, "Enhancing data security using DES-based cryptography and DCT-based steganography," in *2017 3rd International Conference on Science in Information Technology (ICSITech),* Bandung, Indonesia, 2017, pp. 618-621. doi: 10.1109/ICSITech.2017.8257187.

[10] A. A. Krishnan, C. S. Chandran, S. Kamal, and M. H. Supriya, "Spread spectrum based encrypted audio steganographic system with improved security," in *2017 International Conference on Circuits, Controls, and Communications (CCUBE),* Bangalore, India, 2017, pp. 109-114. doi: 10.1109/CCUBE.2017.8394128.

[11] D. Dunsin, MC. Ghanem, and K. Quazzane, "The use of artificial intelligence in digital forensics and incident response in a constrained environment," *Int. J. Inf. Commun. Eng.*, vol. 16, no. 8, 2022, pp. 280-285.

[12] M. Gomathymeenakshi, S. Sruti, B. Karthikeyan, and M. Nayana, "An efficient arithmetic coding data compression with steganography," in 2013 *IEEE International Conference ON Emerging Trends in Computing, Communication and Nanotechnology (ICECCN),* Tirunelveli, India, 2013, pp. 342-345. doi: 10.1109/ICE-CCN.2013.6528520.

[13] B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S. Sruti, and M. Gomathy, "An improved steganographic technique using LSB replacement on a scanned path image," *Int. J. Netw. Secur.*, vol. 16, no. 1, 2014, pp. 14-18.

[14] B. Karthikeyan, J. Chakravarthy, and S. Ramasubramanian, "An amalgamation of scanning paths and modified hill cypher for secure steganography," *Aust. J. Basic Appl. Sci.*, vol. 6, no. 7, 2012, pp. 55-61.

[15] B. Karthikeyan, J. Chakravarthy, V. Vaithiyanathan, "An enhanced Hill cypher approach for image encryption in steganography," *Int. J. Electron. Secur. Digit. Forensics*, vol. 5, no. 3-4, 2013, pp. 178-187.

[16] H. Dutta, R.K. Das, S. Nandi, and S.M. Prasanna, "An overview of digital audio steganography," *IETE Tech. Rev.*, vol. 37, no. 6, 2020, pp. 632-650.

[17] N. Cvejic and T. Seppanen, "Increasing the capacity of LSB-based audio steganography," in *2002 IEEE Workshop on Multimedia Signal Processing*, St. Thomas, VI, USA, 2002, pp. 336-338. doi: 10.1109/MMSP.2002.1203314.

[18] P. Agbedemnab, E. Baagyere, and M. Daabo, "A novel text encryption and decryption scheme using the genetic algorithm and residual numbers," in Proc. 4th Int. Conf. on Internet, Cyber Security, and Inf. Syst., vol. 12, K. Njenga, Ed., London, U.K, 2019, pp. 20–31.

[19] M. Zamani, A. Manaf, R. Ahmad, A. Zeki, and S. Abdullah, "A genetic algorithm-based approach for audio steganography," *Int. J. Comput. Inf. Eng.*, vol. 3, no. 6, 2009, pp. 1562-1565.

[20] L. Indawati and R. Siburian, "Steganography implementation on android smartphone using the LSB (least significant bit) to MP3 and WAV audio," in *2017 3rd International Conference on Wireless and Telematics (ICWT)*, Palembang, Indonesia, 2017, pp. 170-174. doi: 10.1109/ICWT.2017.8284161.

[21] B. M. Amine and S. El Mamoun, "Introduction to steganography in RRNS-based communications," in Proc. 2nd Int. Conf. on Netw., Inf. Syst., and Security, 2019, pp. 1–7.



[22] W.S. Ahmed and L.E. George, "Audio Hiding Using Wavelet Transform with Amplitude Modulation," *J. Al-Nahrain Univ.*, vol. 16, no. 1, 2013, pp. 183-188.

[23] S. Rekik, D. Guerchi, S. Selouani, and H. Hamam, "Speech steganography using wavelet and Fourier Transforms," EURASIP J. on Audio, Speech, and Music Processing, 2012.

[24] M. C. Ghanem, P. Mulvihill, K. Ouazzane, R. Djemai, and D. Dunsin, "D2WFP: A Novel Protocol for Forensically Identifying, Extracting, and Analysing Deep and Dark Web Browsing Activities," *J. Cybersecur. Priv.*, vol. 3, 2023, pp. 808–829, https://doi.org/10.3390/jcp3040036.

[25] B. Santhi, G. Radhika, and S. Ruthra Reka, "Information Security using Audio Steganography - A Survey," *Research Journal of Applied Sciences, Engineering and Technology*.

[26] N. Aroukatos, K. Manes, S. Zimeras, and F. Georgiakodis, "Data Hiding Techniques in Steganography using Fibonacci and Catalan numbers," *ITNG 2012*, April 16-18, 2012, Las Vegas, Nevada, USA.

[27] H. M. Bahig and D. I. Nassr, "DNA-Based AES with Silent Mutations," *Arab. J. Sci. Eng.*, vol. 44, no. 4, pp. 3389–3403, Apr. 2019.

[28] J. C. Vijesh and J. S. Raj, "Deniable Authentication Encryption for Privacy Protection using Blockchain," *Journal of Artificial Intelligence and Capsule Networks*, vol. 3, no. 3, pp. 259-271, 2021.

[29] M. K. Ramaiya, "Improvisation of the security aspect of steganographic system by applying RSA algorithm," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, pp. 245–249, 2016.

[30] S. Panghal, S. Kumar, and N. Kumar, "Enhanced security of data using image steganography and AES encryption technique," *International Journal of Computer Applications*, vol. 42, 2016.

[31] P. Jayaram, H. R. Ranganatha, and H. S. Anupama, "Information hiding using audio steganography - a survey," The International *Journal of Multimedia & Its Applications (IJMA)*, vol. 3, pp. 86-96, 2011.

[32] R. Chandramouli, "Mathematical approach to steganalysis," in Security and *Watermarking of Multimedia Contents IV*, vol. 4675, SPIE, 2002, pp. 14-25, http://dx.doi.org/10.1117/12.465273.

[33] H. A. Muh and I. Riadi, "Analysis of Steganographic on Digital Evidence using General Computer Forensic Investigation Model Framework," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020, http://dx.doi.org/10.14569/IJACSA.2020.0111141.

[34] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," *EURASIP Journal on Audio, Speech, and Music Processing*, 2012(1), pp. 1-16.

[35] I. I. Araujo and H. Kazemian, "Enhancement of Capacity, Detectability and Distortion of BMP, GIF and JPEG images with Distributed Steganography," *MECS Press - International Journal of Computer Network and Information Security (IJCNIS),* vol. 11, no. 11, pp. 21-27, 2019, DOI: 10.5815/ijcnis.2019.11.03.

[36] M. Ghanem, A. Mouloudi, and M. Mourchid, "Towards a scientific research based on semantic web," *Procedia Computer Science*, vol. 73, pp. 328-335, 2015.

[37] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33-37, 2020.

[38] K. Sahu and R. K. Srivastava, "Predicting software bugs of new and large datasets through a unified neuro-fuzzy approach: Reliability perspective," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543-555, 2021.

[39] M. C. Ghanem and D. N. Ratnayake, "Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack: A novel re-authentication protocol," in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA),* London, UK, 2016, pp. 1-7, doi: 10.1109/CyberSA.2016.7503286.

[40] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. Gupta, and R. A. Khan, "Analyzing the Big Data Security Through a Unified Decision-Making Approach," *Intelligent Automation & Soft Computing*, vol. 32(2), 2022.

[41] K. Sahu, F. A. Alzahrani, R. K. Srivastava, and R. Kumar, "Evaluating the Impact of Prediction Techniques: Software Reliability Perspective," *Computers, Materials & Continua,* vol. 67(2), 2021, https://doi.org/10.32604/cmc.2021.014868.

[42] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *Neural Networks*, vol. 17, p. 19, 2018