International Research Journal of Multidisciplinary Scope (IRJMS), 2026; 7(2): 1516-1530 IRJMS

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2026.v07i02.08967

An Adaptive Forensic Approach For the Investigation of Encrypted App Synchronised Portable Magnetic Stripe Card Skimming Fraud

Bapi Saha[1,2]*, Ajoy Kumar Khan[1]

[1]Department of Computer Engineering, Mizoram University, Mizoram, India, [2]Cyber Forensic Division, Tripura State Forensic Science Laboratory, Tripura, India. *Corresponding Author's Email: bapiagt@gmail.com

Abstract

The rapid advancement of cutting-edge digital technologies has significantly contributed to the escalation of organised criminal activity, especially in the field of plastic currency financial fraud. Every day, new categories of cybercrimes are reported and each case requires a specialized forensic approach to achieve accurate results. This research study proposes an adaptive forensic approach, a practically applicable and legally admissible method, for the analysis of credit and debit card fraud and its encrypted application files. Our research presents a comprehensive approach for retrieving, decoding and analyzing data from portable skimmer devices and their related encrypted applications. Furthermore, it also introduces a novel algorithm, implemented using Python scripts, designed to decrypt and examine encrypted mobile application files while maintaining data integrity, enhancing the understanding of digital forensic processes in financial fraud investigations. The precise 97.86% accuracy rate in retrieving data from the portable skimmer device and its connected native application, as well as the 100% success rate in decoding encrypted files, proves that our approach outperforms the conventional methods in terms of flexibility, adaptability and efficacy. The result of the examination revealed the entire modus operandi and helped the investigators and the law enforcement agencies to establish the fact. Future directions include developing an AI-based Integrated approach for automatic detection of encryption types and decoding measures.

Keywords: Credit and Debit Card Fraud, Cybercrime, Encrypted Files, Portable Skimmer, Python Script.

Introduction

The world has entered a new age of cybercrime and India is not an exception to it. The exponential increase in cybercrime has made India the 10th highest in the world for cybercrime, according to the World Cybercrime Index Report (1) and the cybercrime growth rate exceeds 25% every year (2). Cashless transactions, primarily through the use of debit/ credit cards, have revolutionised the economy by allowing the cardholders to travel anywhere in the world without carrying a large amount of cash. On the contrary, it has created a scope for the cybercriminals to execute crime in the Electronic Fund Transfer (EFT) domain. The rise of credit and Debit card fraud has become a major concern worldwide. These crimes are committed by cloning the original card data and then stealing the password /PIN. India records more than Rs. 67225 crore financial loss and 73147 cases in connection with credit and debit card internet frauds in the last three consecutive financial years (3). Common methods adopted by the fraudsters to perform Debit/Credit card cloning are as follows-

(a) Insertion of the skimming device in the ATM card swiping slot.
(b) Read/Write data into the skimming device from the magnetic strip.
(c) Retrieval of recorded data available in the skimming device through a computer and make a cloned card with available information.
(d) Collection of PIN/Secret password and fraudulently withdrawing money.

Nowadays, with the help of mobile phone applications, new techniques are being adopted by cyber criminals to collect Credit/Debit Card data on a real-time basis (4). These types of techniques help the criminals get more data with minimal risk of being caught by the people or law enforcement agencies. With technological advancement, the fraudster also uses different encrypted applications to hide their data. Encryption, which is generally employed to protect sensitive data, poses

(Received 02nd November 2025; Accepted 15th April 2026; Published 24th April 2026)

complex barriers for digital forensic examiners (5). These secure algorithms often hinder the process of forensic data analysis. For decoding such encrypted files, one must have knowledge of advanced computational techniques and algorithms, along with the experience of handling sophisticated analytical tools. So, it is necessary to adopt advanced decoding techniques to extract crucial digital evidence from such encrypted files during cybercrime investigations.

This research paper details a forensic approach for retrieving, decoding and analysing data from a portable skimmer device and its associated applications. It also proposes a new algorithm for decoding and analysing encrypted files linked to the portable skimmer device. The Introduction section also discusses the research problem and hypothesis, followed by the detailed literature review of the existing research works, along with the research novelty and case report. The next Section covers the methodology, followed by the discussion of the results and finally concludes with future work.

Research Problem and Hypothesis

RQ.1: Are the conventional digital forensics methods effective in retrieving data from a secured portable skimmer device and its associated applications?

H1: Traditional digital forensic methods have inadequate efficiency in extracting complete and reliable data from secured portable skimmer devices due to advanced security features.

RQ.2: Are the existing digital forensics methodologies capable of decoding encrypted files and applications from encrypted databases and vaults?

H2: Conventional forensic methodologies face several challenges in decrypting files and applications from encrypted databases.

RQ.3: Does the proposed method address how the data is shared through a private encrypted application and explain the process of collecting digital evidence from portable skimmer devices?

H3: The proposed forensic method effectively demonstrates a secure and highly effective procedure for decoding and analysing data shared via encrypted applications from suspected skimmer devices.

RQ.4: Does the proposed approach highlight the measures taken to decode these encrypted files?

H4 The proposed approach incorporates a novel decryption measure that significantly enhance the accuracy and reliability of decoding encrypted files compared to conventional techniques.

RQ.5 Does the proposed technique describe the process by which these devices were utilised to commit such fraud and does it provide a comprehensive method for obtaining legally admissible data while maintaining data integrity?

H5 The proposed forensic technique successfully explains the entire fraud mechanism involving skimmer devices and ensures the recovery of court-admissible evidence without compromising data integrity.

There are various cybercrimes reported globally related to credit and debit card fraud. Forensic examinations and analyses in such cases have been successfully conducted, leading forensic investigators to propose several methodologies. Past studies show the heavy reliance on credit cards, various types of fraud committed by perpetrators and some preventive measures that can be adopted to reduce these risks. They also mention how credit card components, such as the logo, hologram, magnetic stripe and security code, can be used to authenticate the card and prevent counterfeiting, supported by recent credit card fraud cases (6). However, their research does not explore the causes and consequences of credit card fraud. Another research provides an in-depth study of common techniques like phishing, skimming, data breaches and social engineering used by cybercriminals to steal credit and debit card data (7). The research findings suggest implementing a multi-layered approach involving users, financial institutions and regulatory bodies to combat such fraud. Previous researchers examined the forensic analysis of plastic currency, detailing its composition, magnetic stripe technology, card number, security features and fraud prevention mechanisms (8). This research emphasizes the importance of the Luhn algorithm in verifying the authenticity of card numbers used in investigations involving merchants and internet fraud, such as merchant collusion, triangulation, site cloning, fake merchant websites and plastic card generators. Nonetheless, it does not address potential vulnerabilities or ways to overcome weaknesses in these security features. In past studies, researchers have also highlighted how magnetic stripe card skimmers are used to

duplicate cards and manipulate data, explaining the tools involved and how skimming devices can be disguised as counterfeit ATMs using slot adapters to capture sensitive information from unsuspecting individuals (9). They recommend using digital evidence bags for secure storage of data from these devices, although their study is limited by the processing capabilities of the hardware and the lack of embedded security features. A comprehensive literature review of 40 peer-reviewed studies has been conducted, which focuses on detecting and predicting fraudulent credit card transactions (10). The study emphasises the need for further research in data analytics and cloud computing to tackle associated challenges. They introduce a prototype called Credit Card Fraud Detection System (FDS), which includes multiple detection layers: Terminal, Blocking Rules, Scoring Rules, Data-Driven Model (DDM) and Investigators. Their findings underscore the importance of integrating advanced technologies like Artificial Intelligence, machine learning and the Internet of Things (IoT), as well as understanding customer perspectives on digital payments. Researchers have also analysed security features of various note-taking apps like ColorNote, Notebook, Notepad, Daybook, Daylio, Journal with Lock, Diary with Lock, Moodie and Veggie Diary to identify storage locations of user data and master passwords stored in plaintext or with weak encryption (11). The research found that most apps store data unencrypted, though ColorNote encrypts user data, master passwords and backups. The study employed static analysis of APK files, database analysis with DB Browser for SQLite and decryption via Java and Eclipse. Android Debug Bridge (ADB) was used to extract app data and analyze system logs on both rooted and unrooted devices. This analysis was limited to Android apps and did not include iOS applications. A new forensic model was invented for extracting encrypted mobile data, outlining technical and legal standards for examiners (12). Their research highlights challenges posed by encryption and security features in modern mobile devices, including the need for decryption methods after data acquisition. Their model focuses on obtaining user authentication credentials or exploiting system vulnerabilities to bypass security. However, it cannot extract data from all mobile devices. A new forensic approach was suggested for unlocking backup data from Huawei smartphones that was secured with a password (13). The research shows that Huawei smartphone backups are protected by a password-based encryption system. The study also points out that the suggested method can unlock all the backup data that was encrypted on Huawei smartphones. However, it also notes that it's really hard to decode backup data that is password-protected without the password entered by the user. A new technique was proposed to decode all encrypted files from Signal, Wickr and Threema messengers (14). The researchers used Frida and IDA Pro tools to analyse the apps. The key findings show that the suggested method was able to successfully decode all encrypted database files and media files of those messengers. However, they forgot to mention that they need the user's password to bypass the messenger lock.Researchers have also highlighted different encryption algorithms such as DES, 3DES, AES, ChaCha20, Blowfish and RC4 to measure and compare their effectiveness, considering various aspects, such as key size, padding methods and operational modes (15). These algorithms were examined on an Android mobile device based on CPU usage by measuring the time required to encrypt and decrypt text files of different sizes. A comparison was also made among several Password-Based Encryption (PBE) algorithms. Each algorithm was tested using a range of cipher transformations, various feedback modes and padding methods. The research conducted is only applicable to a limited number of devices and algorithms and must be run in a controlled setting. A systematic examination of prior studies points out the methods for decrypting the databases of Telegram X and BBM-Enterprise (BBME) on both mobile devices and PCs, aiming to extract sensitive data using Hopper v4, IDA Pro and LLDB tools (16). They devised a structured approach to effectively analyze instant messaging (IM) apps. The methods involve four steps: data extraction from applications, selection of core data, identification of encryption algorithms and verification of data decryption. The analysis revealed that the encryption used by Telegram X and Unigram could be broken, but BBME's encryption was inconsistent due to varying random value lengths across different operating systems. Information about the decryption key can be collected through memory analysis and the passphrase can be

determined using BASE64 encoding. Regular updates to the encryption schemes of various instant messenger apps may hinder data extraction and decrypting data from Android devices is more complex than from iOS devices. The research also emphasizes that accessing the KeyStore or Keychain is necessary for data decryption. The challenges faced by digital forensic investigators in maintaining evidence integrity were also discussed in past research, as well as solutions for digital forensics and data encryption systems were also provided (17). The study focuses on creating a digital forensic and data encryption system using the Advanced Encryption Standard (AES) algorithm to encrypt and decrypt evidence files. This method ensures each block is decrypted separately, improving security and performance. The research found that strong passwords and data backups are effective ways to secure digital evidence and the proposed forensic model can assist investigators in preserving evidence integrity.

In the past study, researchers looked into Android file systems architecture and pointed out the importance of digital forensic investigations. It described the role of a forensic examiner to locate and examine digital artefacts stored within system partitions, application folders and databases (18). Their study also addresses key challenges, including device encryption, data protection techniques and continuously evolving Android security features that make evidence collection and analysis more complex. Researchers also conducted a comprehensive forensic, security and privacy analysis of 18 popular Android vault apps. Reverse engineering revealed that 12 of these apps concealed their code, 5 used native libraries and 6 failed to encrypt photos, while 8 did not encrypt videos (19). Many vault apps exhibited vulnerabilities such as unencrypted data storage and weak password protection, enabling data extraction without root access. The study, however, focused solely on Android vault apps and did not explore network traffic analysis. A new method to identify and decode wxSQLite3-encrypted databases was developed by the researchers, which focuses on the LINE messaging app (20). The research analyzed the structure of encrypted databases and the coding elements of wxSQLite3 encryption, performing reverse engineering to locate where wxSQLite3 was used within the app's code. This approach enabled the successful decryption of chat histories and user artefacts relevant to digital forensics. However, the study does not discuss that modifications in the wxSQLite3 encryption process could impact data decoding. The past study reveals that the AES algorithm is highly secure and works better than other algorithms like DES and 3DES (21). It also points out that AES produces fewer output bytes than the other algorithms. However, the research only looks at how well the AES algorithm performs compared to a few other algorithms and only checks a small number of factors.The Advanced Encryption Standard (AES) algorithm relies on the same key for both encryption and decryption (22). Research findings indicate that the AES cryptographic file security system is capable of performing encryption and decryption. The research concludes that the AES algorithm is quite sensitive to changes in the input keys. However, it does not address the impacts of an attack on the AES algorithm. The researchers conducted a study where they used a mix of academic analysis and different evaluation parameters to compare how well an efficient and secure encrypted search on mobile cloud performs compared to other traditional encrypted search engines (23). The research also shows that ENSURE defends against security risks from the chaotic and unreliable cloud. Researchers conducted a critical study on forensic procedures to retrieve and interpret the evidence stored by WhatsApp's encrypted SQLite databases on unrooted Android devices (24). The authors performed controlled experiments to locate these database files, explain how to decrypt them and explain the procedure to analyse their contents. In a past study, the researchers have explored ways to apply the AES algorithm for encrypting and decrypting files and images on Android smartphones (25). The research highlights that AES encryption and decryption processes are quicker on Android devices than with other algorithms. It proves that the AES algorithm is a great choice for secure data communication, particularly on smart mobile devices.

Novelty

Most of the existing studies focus on detecting credit card fraud, describing preventive mechanisms and security features. Even in the case of encrypted files, the existing works discuss

different methods for decoding data from test cases. However, these studies fail to address the techniques required for real-time extraction, decoding and analysis of data retrieved from detachable skimmer devices and their associated applications, nor the decryption of various encrypted files. Our research bridges these gaps by introducing an approach designed to mitigate the identified limitations. The novelty of our research work is as follows-

(a) It proposes a structured forensics approach for extracting, analysing and decoding digital evidence from portable skimmer devices.
(b) Helps in detecting the type of encryption used to encrypt the files.
(c) Enables developing a computational algorithm for decoding encrypted files.
(d) Enable real-time extraction, decoding and analysis of the digital evidence to determine the modus operandi.
(e) Authenticate the usefulness of the proposed approach for solving real-world forensic investigations.

Case report

The cybercriminal in this case was observed loitering near the ATM counter and closely watching the customers. After some time, two/three customers approached the ATM counters to withdraw cash but were unable to do so due to a technical error. The cybercriminal approached and wanted to see their ATM cards, stating that he might be able to help them. On good faith, the cards were handed over to him. Taking the opportunity, the perpetrator swiped the card with a device in a twinkling of an eye. One of the friends noticed the swiping and screamed for help. The locals gathered and forcibly took away the device and reported it to the police. The police immediately arrested the perpetrator and started interrogation. The perpetrator's mobile phone was also seized along with the suspected device. The police had some doubt about whether the device was connected to a mobile phone, but could not reveal any information. The seized portable skimmer device (Marked as “A”), along with a mobile phone (Marked as “B”), shown in Figure 1, were submitted to the Cyber Forensic division for further investigation, examination and data analysis.

A physical extraction of the mobile device was performed using the MSAB XRY tool to acquire the device data. The acquired memory dump was subsequently analysed using the XRY XMAN analysis tool. During the examination, the device was identified as a smartphone running the Android operating system, version 13. At the time of acquisition and analysis, the device was found to be in an unrooted condition.

Figure 1: Seized Electronic Evidence: A. Portable Skimmer Device, B. Mobile Phone

Methodology

During this experimental evaluation, the seized digital evidence, comprising a suspected skimmer device and the mobile phone, was examined and analysed to extract crucial data from it. Chain of custody has been maintained well in the study, as there was proper documentation done in the examination case file (26). These records keep the information about the device receiving date, examination tools and techniques, examination logs and final examination report containing all the

data. The examination done as per forensic protocol making extraction dump of the phone memory by acquiring the device memory through write protected system without altering any content in the evidence phone. The hash verification process performed on the acquired phone memory dump to check its integrity (27). The proposed methodology, as illustrated in Figure 2, incorporates the procedure used to successfully extract and analyse the data.

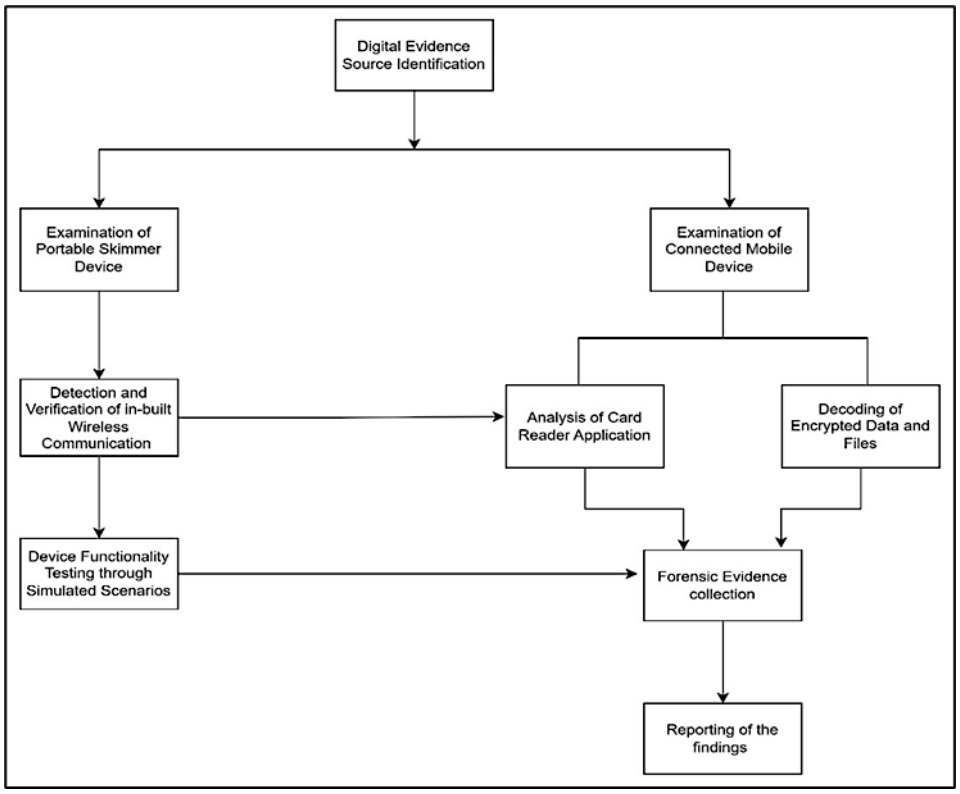


Figure 2: Flowchart of the Proposed Methodology

Analysis of Suspected "Skimmer" Device and its Associated Apps

To extract the digital information stored, the suspected device is connected to the computer system, after detaching from the ATM chamber, but no visible data is found. However, the targeted Physical inspection of the suspected skimming device reveals the presence of a Bluetooth connectivity option. we decided to extract and examine data from the phone memory of the seized mobile device using Mobile Forensics software known as MSAB XRY, in order to locate any suspicious applications and files that might be related to card-skimming activities. During the analysis, an encrypted application, named 'EasyMSR.apk', was discovered in an encrypted form, along with an ADB-format database file containing no data. The APK file of the encrypted application was also found. So, to extract data from the encrypted application, while maintaining the data integrity, we first transferred the file to another sterile mobile device and installed it. The generic structure of 'EasyMSR.apk', including the source code, was analysed using a Java decompiler and it was discovered to be an App for cloning credit/debit card data connected to the skimmer device through Bluetooth, as shown in Table 1.

Table 1: Findings of EasyMSR APK File Analysis

Component Analysed	Findings
AndroidManifest.xml	Permission for Bluetooth connectivity, writing external data and activities linked to the portable skimmer device (minidx) were detected
Classes.dex (Decompiled via JD-GUI)	Contains Bluetooth device communication classes, along with login info classes with password length limited to 4 digits. An activity class describing the details of the supported portable skimmer device was identified

	and the interaction function for collecting card data via the skimmer device was also discovered.
Resource Directory	Multiple URL templates and configuration details were discovered
APK Signature	Type: X.509 Version: 3 Serial number: 0x6a174218 Subject: CN=gbtf, OU=gbtf, O=gbtf, L=shenzhen, ST=guangdong, C=CN Public key type: RSA Exponent: 65537 Modulus size (bits): 2048 Signature type: SHA256withRSA Signature OID: 1.2.840.113549.1.1.11
API endpoints	http://www.deftun.com
Database	The application stores files internally or externally instead of using SQLite database.
Data export logs	Internal logs '/data/data/com.gbtf.msrx6pro/files/ External logs '/sdcard/MSR/'

While checking its functionality, it was noted that the app required a password to start. We then performed a brute force attack to recover the password to unlock the app. After unlocking, the app connects to the suspected skimming device via Bluetooth. The user interface displays options for reading from and writing to magnetic stripe media. By using the app's "read" feature, data from an ATM card was retrieved, including cardholder details and track information, which were saved as images and logs. However, it displayed only a small amount of data. The analysis of the logs reveals that the data automatically gets transferred to the app database. Therefore, the next step is to examine the device's phone memory to look for any other associated data related to the case. Despite thorough analysis, we could not recover the data that we hoped for; instead, we discovered a suspected app named "XEN Mobile Gallery Files Vault: Lock Apps" and some encrypted files.

The brute-force recovery of application passwords was conducted strictly within the framework of digital forensic legal and procedural guidelines (28). In practical cases, these procedures are performed after obtaining appropriate legal authorisation, such as a court-issued warrant or formal investigative approval. To perform this, we generally follow a laboratory-approved standard operating procedure (SOPs) that oversees evidence handling, data acquisition and password recovery attempts. Additionally, to ensure digital evidence integrity, the brute-force attack to bypass the lock was conducted in controlled rate, as well as implementing precautionary mechanisms. These mechanisms were used to avoid excessive authentication attempts that could potentially trigger account lockouts, data overwriting, or corruption within the backup environment. However, all recovery attempts were performed on forensic copies of the backup data rather than on the original evidence.

Decoding and Analysis of Encrypted Files

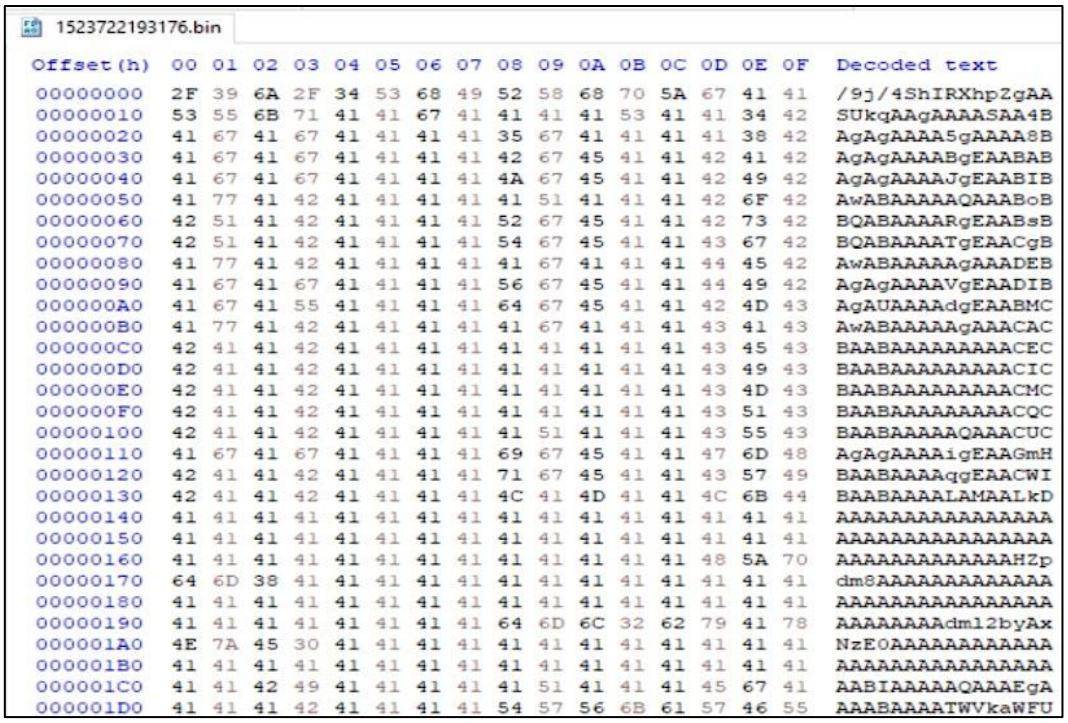
This section discusses the implementation techniques used for decoding and analysing the encrypted files.

Analysis of the Gallery Vault app files

The analysis of "XEN Mobile Gallery Files Vault: Lock Apps" reveals that the suspected application is a photo locker app. The photo locker app allows the user to secretly hide and lock private files like photos, important documents and videos. The data stored in this app is in an encrypted format to protect the data from unauthorised access. To determine the type of encryption used to secure the data, we performed a Hex analysis using HxD decoder (29). The analysis findings are presented in Figure 3.

The decoded text data, using the Hex analysis, at offset 0 displays "/9j/". As we know, having /9j/ at the start of some text heavily indicates that the data is a JPEG file with base64 encoding (30). To confirm this, if we start decoding /9j/ back, the decoded output shows "FF D8 FF", which is the magic number for a JPEG image file.

For decoding the JPEG files with base64 encoding, we developed an algorithm and its corresponding program (Python script) and applied it to the scripts section of MSAB XRY's built-in analysis software, "XAMN," presented in Figure 4.



1523722193176.bin

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	2F	39	6A	2F	34	53	68	49	52	58	68	70	5A	67	41	41	/9j/4ShIRXhpZgAA
00000010	53	55	6B	71	41	41	67	41	41	41	41	53	41	41	34	42	SUkqAAgAAAASAA4B
00000020	41	67	41	67	41	41	41	41	35	67	41	41	41	41	38	42	AgAgAAAA5gAAAA8B
00000030	41	67	41	67	41	41	41	41	42	67	45	41	41	42	41	42	AgAgAAAABgEAABAB
00000040	41	67	41	67	41	41	41	41	4A	67	45	41	41	42	49	42	AgAgAAAAJgEAABIB
00000050	41	77	41	42	41	41	41	41	41	51	41	41	41	42	6F	42	AwABAAAAAQAAABoB
00000060	42	51	41	42	41	41	41	41	52	67	45	41	41	42	73	42	BQABAAAARgEAABsB
00000070	42	51	41	42	41	41	41	41	54	67	45	41	41	43	67	42	BQABAAAATgEAACgB
00000080	41	77	41	42	41	41	41	41	41	67	41	41	41	44	45	42	AwABAAAAAgAAADEB
00000090	41	67	41	67	41	41	41	41	56	67	45	41	41	44	49	42	AgAgAAAAVgEAADIB
000000A0	41	67	41	55	41	41	41	41	64	67	45	41	41	42	4D	43	AgAUAAAAdgEAABMC
000000B0	41	77	41	42	41	41	41	41	67	41	41	41	43	41	43	43	AwABAAAAAgAAACAC
000000C0	42	41	41	42	41	41	41	41	41	41	41	41	41	43	45	43	BAABAAAAAAAAACEC
000000D0	42	41	41	42	41	41	41	41	41	41	41	41	41	43	49	43	BAABAAAAAAAAACIC
000000E0	42	41	41	42	41	41	41	41	41	41	41	41	41	43	4D	43	BAABAAAAAAAAACMC
000000F0	42	41	41	42	41	41	41	41	41	41	41	41	41	43	51	43	BAABAAAAAAAAACQC
00000100	42	41	41	42	41	41	41	41	41	51	41	41	41	43	55	43	BAABAAAAAQAAACUC
00000110	41	67	41	67	41	41	41	41	69	67	45	41	41	47	6D	48	AgAgAAAAigEAAGmH
00000120	42	41	41	42	41	41	41	41	71	67	45	41	41	43	57	49	BAABAAAAqgEAACWI
00000130	42	41	41	42	41	41	41	41	4C	41	4D	41	41	4C	6B	44	BAABAAAALAMAALkD
00000140	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00000150	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00000160	41	41	41	41	41	41	41	41	41	41	41	41	41	48	5A	70	AAAAAAAAAAAAAHZp
00000170	64	6D	38	41	41	41	41	41	41	41	41	41	41	41	41	41	dm8AAAAAAAAAAAAA
00000180	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
00000190	41	41	41	41	41	41	41	41	64	6D	6C	32	62	79	41	78	AAAAAAAAdml2byAx
000001A0	4E	7A	45	30	41	41	41	41	41	41	41	41	41	41	41	41	NzE0AAAAAAAAAAAA
000001B0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	AAAAAAAAAAAAAAAA
000001C0	41	41	42	49	41	41	41	41	41	51	41	41	41	45	67	41	AABIAAAAAQAAAEgA
000001D0	41	41	41	42	41	41	41	41	54	57	56	6B	61	57	46	55	AAABAAAATWVkaWFU

Figure 3: Results of the Hex Analysis

```
BEGIN

  DISPLAY "Enter the full path of the base64 .bin file:"
  INPUT input_file_path
  IF file at input_file_path does not exist THEN
     DISPLAY "Error: File does not exist."
     TERMINATE program
  ENDIF

  OPEN input_file_path in binary read mode
  READ the entire content into the variable base64_data
  CLOSE the input file

  DECODE base64_data using base64 decoding
  STORE result in variable decoded_image
  DISPLAY "Enter the full path for the output image file (e.g., C:\output.jpg):"

  INPUT output_file_path
  OPEN output_file_path in binary write mode
  WRITE decoded_image to the output file
  CLOSE the output file

  DISPLAY "Image successfully saved to: " + output_file_path
END
```

Figure 4: Algorithmic Pseudocode for Decoding Encrypted JPEG Files

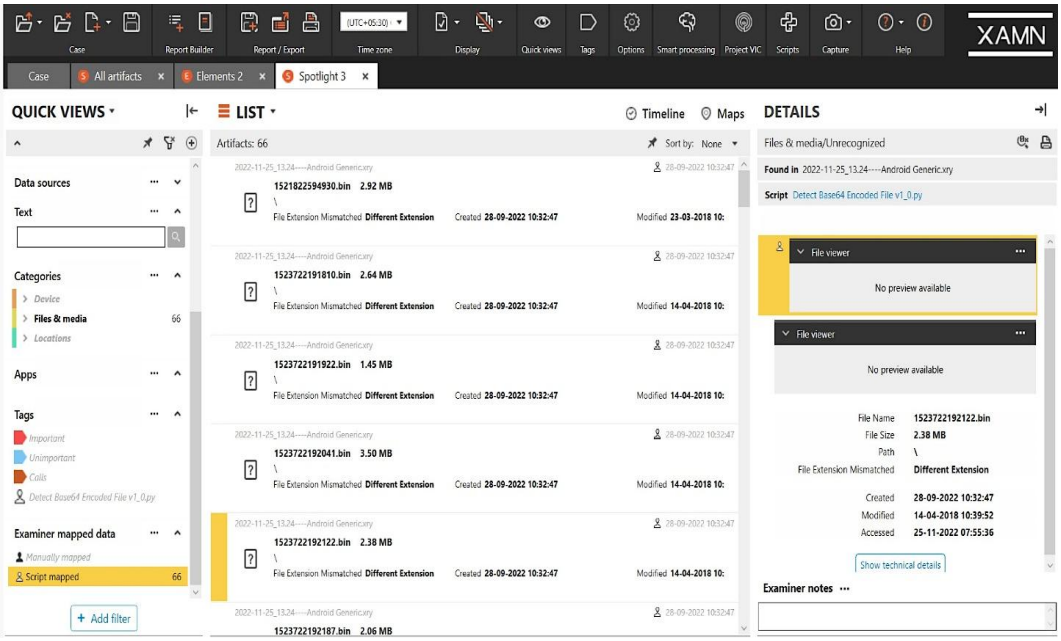


Figure 5: Image Showing Successful Decoding of the Encrypted JPEG Files

The data decoding process through mapping of our script is shown in Figure 5.

This allowed us to decrypt the image files successfully.

Decoding and Analysis of iManager Encrypted Files

During the analysis of the phone memory, we discovered several encrypted private video files. The in-depth analysis of the file path and file tree view reveals that these hidden, encrypted files were stored inside an application called iManager. For decoding these encrypted files, we developed an algorithm and its corresponding program using Python scripting and applied it to the scripts section of XAMN. The algorithm pseudocode of the script is presented in Figure 6.

```
BEGIN

  FOR each file in the forensic image's Files View DO

    SET file_name = get the file's name
    SET file_path = get the file's path

    IF file_path includes ".do_not_delete_private_files" AND contains "image" OR "video"
THEN

      READ raw data of the file into memory
      SET first_part = first 1024 bytes of data
      SET second_part = remaining data after 1024 bytes

      SET key = generate decryption key using predefined logic
      DECRYPT first_part using AES-ECB and key
      COMBINE decrypted first_part with second_part into final_content

      IF file is an image OR ends with "_tb" THEN
        ADD a new picture item to the report
        SET its file name and raw content
        LINK the picture to the original file
      ELSE IF file is a video THEN
        ADD new video item to the report
        SET its file name and raw content
        LINK the video to the original file
      ENDIF

    ENDIF

  ENDFOR

END
```

Figure 6: Algorithmic Pseudocode for decoding encrypted Video files

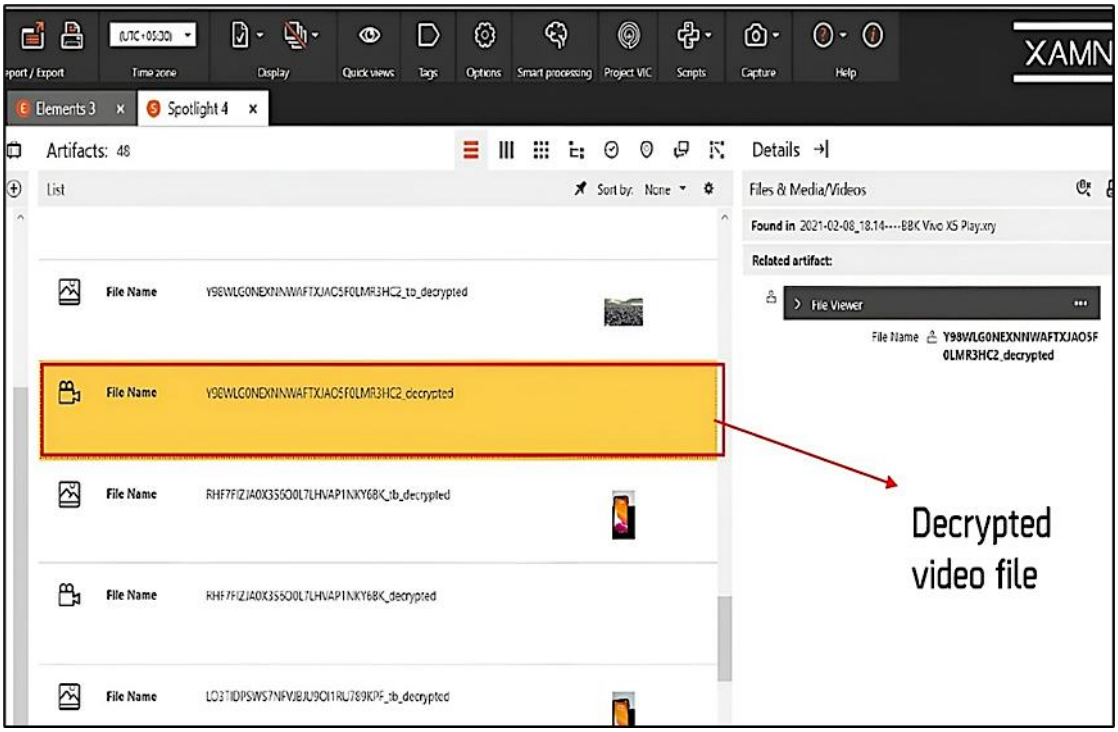


Figure 7: Image Showing Successful Decoding of the Encrypted Video Files

The successful decoding of the video file through the mapping of our script is shown in Figure 7.

The proposed algorithms are innovative in its structured decoding pipeline, where encoded forensic artifacts are systematically validated, extracted and reconstructed. Unlike conventional decoding methods, it integrates input verification, controlled data handling, source code analysis and base64 reconstruction of evidence files, enabling reliable recovery of hidden image data from the gallery vault application while maintaining forensic integrity. These algorithms also help to identify protected media files, extracts encrypted segments and reconstructs them using a predefined key-generation mechanism. By combining pattern-based file identification, partial AES decryption and automated evidence reconstruction, the method enables efficient recovery of hidden images and videos from protected backup directories.

Modern mobile backup applications typically use standardised cryptographic algorithms such as AES-based encryption and other secure key derivation mechanisms to protect user data. So, several detection methods, such as hex analysis and the source code analysis, are performed to identify and specify which type of encoding is done. These methods rely on analysing metadata, header structures and entropy distribution, which allows investigators to determine the nature of the stored data without compromising evidence integrity. From a computational perspective, the time complexity of the proposed algorithm for decoding Base64 encoded data is O(n), where n represents the size of the encoded input. In the case of decrypting AES-encrypted video files, the time complexity becomes O(m × n), where m denotes the number of files being processed and n represents the size of each file.

Results and Discussion

The results derived from the detailed analysis of every possible aspect facilitate the investigative consistency and working utility of our proposed approach. It also paves the way for other forensic experts to mitigate similar situations via utilising our approach. This section assesses the key findings of the research, the success rate of the proposed approach and positions them alongside the previous notable research works.

Interpretation of the Outcomes

By decrypting and analysing the data retrieved from the skimmer(cloning) device, as well as decoding files of different applications installed in the phone memory of the seized devices, we were able to understand the whole situation and reach a decisive conclusion. The decoded data includes a significant amount of user-level data. The successful extraction, analysis and decryption of

the encrypted files indicate that our approach is highly efficient and effective in handling similar situations. The summary of the findings of the experimental analysis is presented in Table 2.

Table 2: Experimental Evaluation Results Summary

Parameter	Results	Remarks
Credit/Debit user customer data including media files	Successfully retrieved	Analysis of the extracted data reveals the presence of several images and screenshots of transactions, card details, personal information of various individuals and videos of individuals' movements and PIN actions during transactions via debit/credit cards.
Total digital evidence files recovered from the portable skimmer device	183 files out of 187 files (Card info txt files-66 Customer info txt files- 65 Image files – 49)	The extracted files primarily comprised, credit/debit card information, customer details, including transaction visuals and related metadata.
Partial files recovered from the portable skimmer device	4 files	These files were partially recovered either due to data corruption or encryption inconsistencies.
Accuracy in retrieving data from the skimmer device	97.86%	The high success rate in retrieving data from the portable skimmer device shows the flexibility and reliability of our approach
Encrypted files	Present	Several encrypted files were identified during the forensic analysis.
Storage path of encrypted files	EasyMSR.apk, XEN Mobile Gallery Files Vault: Lock Apps, iManager	The files stored in these apps were discovered to be encrypted.
Type of encoding	Base64	Files, particularly gallery vault images, were found to be encoded using Base64 encoding.
No. of encrypted files extracted	114	Extracted data included multiple encrypted image and video files.
No. of encrypted files and applications successfully decoded	114	Encrypted files were analyzed and decoded using Java decompiler, HxD decoder, a new Python script and forensic software tools
Accuracy in decoding encrypted files	100%	The full success rate demonstrates the effectiveness of the proposed approach in decoding encrypted files.

Table 3: Comparative Analysis with Existing Methods

Year	Strengths	Challenges	Encrypted apps and decoding accuracy	Reference
2025	Mentions the necessity of integrating machine learning in detecting fraud.	Focuses only on detecting fraud rather than recovery or extraction.	Not applicable	(7)
2024	Provides decryption techniques for modern note apps by identifying key weaknesses in app data storage encryption.	Conducted on a limited set of data (test case), the results depend heavily on OS and device permissions.	Successful in test cases, but no percentage is mentioned	(11)
2024	Explores decoding steps for wxSQLite3 databases	Limited to specific encryption library and versions	Successful in test cases, but no percentage is mentioned	(20)

2023	Includes an Analysis of AI and blockchain-based fraud detection techniques	Limited to the prevention and detection of credit card fraud	Not applicable	(10)
2022	Practical-based approach, Used key-based system for securing data. Protect user data through encryption.	Limited evaluation against brute force attack. Hardware performance overhead not checked.	Successful in decoding data with the correct key. No formal metrics shown in the success rate.	(5)
2025	Provides a comprehensive forensic approach for decrypting data from card reading app, password breaking, secured storage access and secret sharing	Requires expertise to find the correct card reader app and encryption type	97.86% accuracy in retrieving data from a portable skimmer device and 100% accuracy in decoding encrypted files	Our approach

Comparative Analysis with Other Notable Research Works

Table 3 details the comparative analysis conducted with the previously existing research works.

Most of the previous research work on skimmer fraud or credit/ debit card fraud only focuses on the detection of skimming, rather than on the extraction accuracy from devices. Similarly, existing research works do not explicitly mention the accuracy of decrypting data using the models they present. The data recovery and decoding accuracy in of 97.86% was achieved, determined by comparing the number of successfully recovered and decoded files with the total number of files. Based on the experimental evaluations, one existing study reported an accuracy of approximately 58% (19), whereas another study (16) estimated the data decoding accuracy of the tested applications to be around 91%**.** Figure 8 shows the comparison between the accuracy of our approach and the previously published research work.

Overall, the results of this research support that the proposed approach is practically substantial, legally thorough and can be easily adopted in forensic examination procedures to mitigate similar cases.

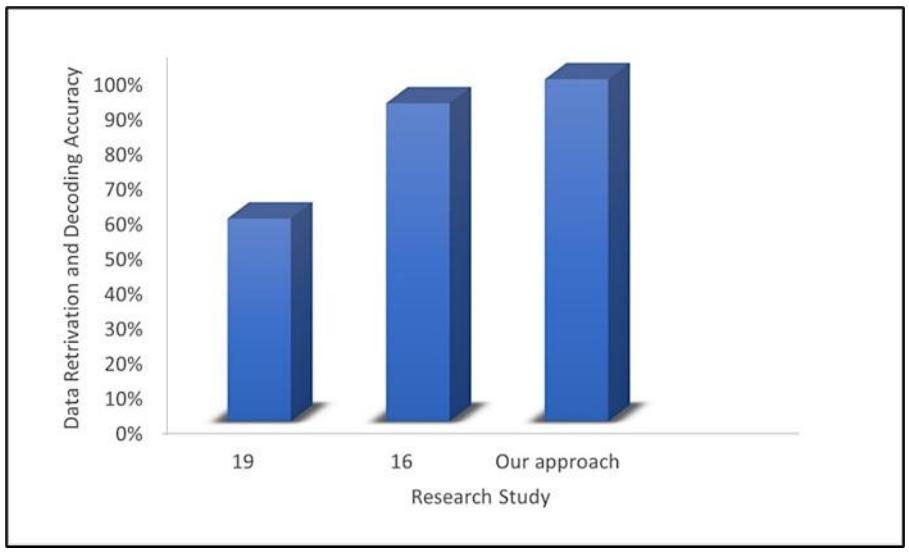


Figure 8: Accuracy Comparison: Proposed Approach Vs Existing Studies

Conclusion

In this experimental forensic study, all sources of digital evidence, such as mobile phone memory, portable skimmer devices, installed applications and app databases, were carefully examined. We

implemented different procedures, including app reverse engineering and decoding encrypted files using new algorithms with Python scripts, along with available forensic tools and techniques, to determine the modus operandi. The 97.86% accuracy in retrieving data from the portable skimmer device and its connected native application, as well as the successful decoding of encrypted files, demonstrates the adaptability of our approach. The data decoding and analysis, combined with other information, revealed the entire crime network, aiding law enforcement authorities in dismantling the organised cybercrime syndicate. Our practical-oriented study highlights various boundaries that also have scope for future improvements. The Android app used for skimming was decrypted with the implementation of brute force attack, which gave a clear and structured way to assess the decryption process. For the Doc Vault and iManager apps, the forensic examination focused on data protected by the AES encryption algorithm, allowing for a detailed study of this widely used security method. The detection of encryption techniques was performed through manual reverse engineering of the applications, which allowed for a better understanding of how the encryption was set up but there is a scope for inclusion of automatic detection procedure. Additionally, the experimental evaluation was performed on three mobile phone applications used for data encryption providing focused insights that can serve as a basis for extending the analysis to a broader range of applications in future work.

Future research directions may include—

(a) Developing tools to decode skimmer data within the widely used forensic software.
(b) AI-based Integrated approach for automatic detection of encryption types and decoding measures.
(c) Collaboration with the global scientific communities for further research on developing new and effective methods to overcome the challenges of different encryption.

Abbreviations

AI - Artificial Intelligence, ATM- Automated Teller Machine, H – Hypothesis, OS - Operating System, RQ - Research Question.

Acknowledgement

The authors sincerely acknowledge the value of MSAB's mobile forensics technical team for their technical support in digital forensics. We also extend our gratitude to the Cyber Forensic Division, Tripura State Forensic Science Laboratory, for facilitating the research.

Author Contributions

Bapi Saha: conceptualization, literature review, performed laboratory examinations, manuscript draft, writing, revision, Ajoy Kumar Khan: supervision- method design and the result analysis process, writing, revision. All authors approved the final version of the manuscript

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Declaration of Artificial Intelligence (AI) Assistance

Artificial intelligence tools were used only for language refinement and formatting support. All research ideas, data interpretation, analysis and conclusions were developed solely by the authors.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Ethics Approval

This study does not involve human participants, animals, or sensitive personal data requiring formal ethical approval. All methods and processes used comply with standard research ethics and academic guidelines.

Funding

The authors confirm that this research was conducted without any external financial support.

References

1. Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F. Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS ONE. 2024;19(4): e0297312. doi:10.1371/journal.pone.0297312
2. Joshi D. Emerging issues of Cyber Crimes in India: Statistics, Modus Operandi of online frauds and Remedies to curb Cyber Crimes. International Journal of Science and Research Archive. 2025;

17(1):408–418.
https://doi.org/10.30574/ijsra.2025.17.1.2799
3. Reserve Bank of India. Annual Report 2023–24. Mumbai: Reserve Bank of India, 2024; https://rbi.org.in/Scripts/AnnualReportMainDisplay.aspx
4. Alashwali E, Chandrashekar R.M, Lanyon M, *et al.* Detection and Impact of Debit/Credit Card Fraud: Victims' Experiences. Cornell University, arXiv. 2024.
doi: https://doi.org/10.48550/arxiv.2408.08131
5. Aziz A.A, Bawamohiddin A.B. The Development of Mobile Application Security Through Encryption. Journal of Technology and Humanities.2022;3(2): 26–36.
doi: 10.53797/jthkkss.v3i2.5.2022
6. Sivakumar N, Balasubramanian R. Fraud detection in credit card transactions: classification, risks and prevention techniques. International Journal of Computer Science and Information Technologies. 2015;6(2):1379–1386.
https://www.ijcsit.com/docs/Volume%206/vol6issue02/ijcsit20150602104.pdf
7. Sharipova N. Fraud involving debit, credit and virtual cards and ways to prevent it. Role and Importance of Science in the Modern World. 2025; 2(5): 221–224.
https://zenodo.org/records/15561777
8. Kumar P, Sharma P, Bhandari D, Khandekar H, Prema, Chouhan J. S. Comparative analysis of plastic currency-debit and credit cards using VSC-8000/HS. International. Journal of Recent Scientific Research.2023;14(11):4378–4385.
doi: 10.24327/ ijrsr.20231411.0822
9. Masters G, Turner P. Forensic data recovery and examination of magnetic swipe card cloning devices. Digital Investigation.2007;4:16–22.
doi: 10.1016/j.diin. 2007.06. 018
10. Cherif A, Badhib A, Ammar H, Alshehri S, Kalkatawi M, Imine A. Credit card fraud detection in the era of disruptive technologies: a systematic review. Journal of King Saud University Computer and Information Sciences. 2023; 35(1):145–174.
doi: 10.1016/j.jksuci.2022.11.008
11. Yoon S, Park M, Jang K, Seo H. Data Decryption and Analysis of Note-Taking Applications. Cryptology. 2024; 2006.
https://eprint.iacr.org/2024/2006.pdf
12. Fukami A, Stoykova R, Geradts Z. A New Model for Forensic Data Extraction from Encrypted Mobile Devices. Forensic Science International Digital Investigation.2021; 38: 301169.
doi: 10.1016/j.fsidi.2021.301169.
13. Park M, Kim G, Park Y, Lee I, Kim J. Decrypting Password-Based Encrypted Backup Data for Huawei Smartphones. Digital Investigation.2019;28:119–125.
doi: 10.1016/j.diin.2019.01.008.
14. Son J, Kim YW, Oh DB, Kim K. Forensic Analysis of Instant Messengers: Decrypt Signal, Wickr and Threema, Forensic Science International Digital Investigation.2022;40: 301347.
doi: 10.1016/j.fsidi.2022.301347
15. Salkanovic A, Ljubic S, Stankovic L, Lerga J. Analysis of Cryptography Algorithms Implemented in Android Mobile Application. Information Technology and Control. 2021; 50(4):786–807.
doi: 10.5755/j01.itc.50.4.29464
16. Kim G, Park M, Lee S, Park Y, Lee I, Kim J. A study on the decryption methods of Telegram X and BBM-Enterprise databases in mobile and PC. Forensic Science International Digital Investigation. 2020;35: 300998.
doi: 10.1016/j.fsidi.2020.300998
17. Dukundane N, Mutongwa SM. Digital Forensic Setup and Data Encryption: Underpinning Advanced Encryption Standard (AES) Algorithm. International Journal of Innovative Science and Research Technology. 2023; 8(2):1445–1454.
https://ijisrt.com/assets/upload/files/IJISRT23FEB648
18. Alkattan S, Chiziba A, Pronichev V D. Examining the File System of Android Devices: Implications for Digital Forensics. International Journal of Human and Natural Sciences. 2024; 10(1):228–232.
doi: 10.24412/2500-1000-2024-10-1-228-232
19. Zhang X, Baggili I, Breitinger F. Breaking into the vault: Privacy, security and forensic analysis of Android vault applications. Computers & Security. 2017; 70: 516–531.
doi: 10.1016/j.cose.2017.07.011
20. Kang S, Kim G, Hur U, Kim J. Forensic Analysis of wxSQLite3-Encrypted Databases and Its Application. Electronics. 2024; 13(7): 1325.
doi: 10.3390/electronics13071325
21. Abdullah AM. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. Cryptography and Network Security. 2017;16(1): 1-11.
https://www.researchgate.net/publication/317615794
22. Muttaqin K, Rahmadoni J. Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based. Journal of Applied Engineering and Technological Science. 2020; 1(2): 113–123.
doi: 10.37385/jaets.v1i2.78
23. Guo Y, Liu F, Cai Z, Xiao N, Zhao Z. Edge-Based Efficient Search over Encrypted Data Mobile Cloud Storage. Sensors.2018; 18(4): 1189.
doi: 10.3390/s18041189
24. Fayyad-Kazan H, Kassem-Moussa S, Hejase HJ, Hejase AJ. Forensic analysis of WhatsApp SQLite databases on unrooted Android phones. HighTech and Innovation Journal. 2022; 3(2):175–195.
https://doi.org/10.28991/HIJ-2022-03-02-06
25. Tayde S, Siledar S. File Encryption Decryption using AES Algorithm in Android Phone. International Journal of Advanced Research in Computer Science and Software Engineering. 2015; 5(5): 550–554.
https://www.researchgate.net/publication/3156693
25_File_Encryption_Decryption_Using_AES_Algorithm_in_Android_Phon
26. Narasimhan P, Kala N. Ensuring the Integrity of Digital Evidence: The Role of The Chain of Custody in Digital Forensics. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2024;10(6):2438-50.
https://doi.org/10.32628/CSEIT2410612443

27. Boyanov P. Practical Applications of Hash Functions MD5, SHA-1 and SHA-256 Using Various Software Tools to Verify the Integrity of Files. Journal Scientific and Applied Research. 2024;27(1):120–37. https://doi.org/10.46687/jsar.v27i1.413
28. Ibrahim A, Albugami M, Alkhwaja A, *et al.* Password Cracking with Brute Force Algorithm and Dictionary Attack using Parallel Programming. Applied Sciences. 2023;13(10):5979–9. https://doi.org/10.3390/app13105979
29. Fakiha BS. The application and effectiveness of Hex Editor Forensic in Investigating Cybercrime. Social Medicine. 2023;16(1):43–47. doi:10.71164/socialmedicine.v16i1 .2023.1523
30. Baso F. Analysis and Utilization of the Base64 Algorithm for Image Encryption and Decryption Security in Web-Based Images. Journal of Security Computer Information Embedded Network and Intelligence System. 2023;52–57. https://doi.org/10.61220/scientist.v1i2.20233

How to Cite: Saha B, Khan AK. An Adaptive Forensic Approach For the Investigation of Encrypted App Synchronised Portable Magnetic Stripe Card Skimming Fraud. Int Res J Multidiscip Scope. 2026; 7(2): 1516-1530. DOI: 10.47857/irjms.2026.v07i02.08967