
**E-ISSN:** 2707-6644
**P-ISSN:** 2707-6636
Impact Factor (RJIF): 5.43
www.computersciencejournals.com/ijcpdm
IJCPDM 2025; 6(2): 200-206
Received: 05-05-2025
Accepted: 09-06-2025

**Le Minh Tung**
Newton Secondary and High School, Newton Secondary and High School, Hanoi, Vietnam

**Corresponding Author:**
**Le Minh Tung**
Newton Secondary and High School, Newton Secondary and High School, Hanoi, Vietnam

# A mobile security architecture for encrypted media storage using anti-breaking password and alert systems

## Le Minh Tung

**DOI:** https://www.doi.org/10.33545/27076636.2025.v6.i2b.128

**Abstract**
With the growing reliance on smartphones to store personal photos and videos, the demand for mobile data protection has become increasingly urgent. This study proposes a mobile security architecture that integrates three layers of protection: encrypted media storage, anti-breaking password mechanisms, and intrusion alerts. The system employs robust encryption algorithms to secure multimedia files, applies hashed password authentication to resist brute-force attacks, and activates proactive alerts by capturing intruders' photos and logging failed attempts. A prototype was developed using the Flutter framework to ensure cross-platform compatibility, and tested on real devices to validate usability and performance. Results demonstrate that the system effectively safeguards private photos and videos, offering both strong data confidentiality and active intrusion monitoring. The key contribution lies in advancing mobile privacy protection by combining encryption, authentication, and intelligent alert systems into a unified architecture.

**Keywords:** Mobile security architecture, encrypted media storage, anti-breaking password, alert systems, flutter framework

## Introduction
In the current digital era, mobile phones have become an indispensable part of daily life, serving as central platforms for storing and accessing personal information, particularly images and videos. However, this convenience is accompanied by substantial security risks, as sensitive data has become increasingly vulnerable to attacks and breaches.

Rise Above Research statistics the proportion of photographs captured using smartphones was approximately 89% in 2020 and is projected to surpass 93% by 2023. The fact that people store large amounts of private image data on mobile devices means increasing security and privacy threats. Cybersecurity threats are becoming more sophisticated and frequent, from denial-of-service (DoS/DDoS) attacks, phishing, man-in-the-middle, to password-based attacks and malware (Sharma, V. *et al*., 2020) [13]. In the third quarter of 2021, there were 9.6 million malware (adware, riskware) attacks targeting mobile devices detected and blocked (Cinar, A. C., & Kara, T. B., 2023) [4]. Private photos/videos, if stolen or leaked, can lead to serious violations of users' privacy. Worryingly, there is still a segment of users who are subjective - 16% of smartphone users do not set up a screen lock or any security mechanism to protect their devices (Pew Research Center, 2023).

There are several common forms of attacks that directly threaten private photos/videos stored on smartphones. First is malware attacks: malicious software (spyware, trojans) can sneak into the device through malicious applications, malicious MMS/email messages or exploit system vulnerabilities. Spyware-like malware such as Redrop has the ability to secretly steal the victim's device information, files, images and recordings (Cinar, A. C., & Kara, T. B., 2023) [4]. Second is unauthorized access due to loss of control of the device: this happens when the phone is lost or stolen. Millions of smartphones are stolen every year worldwide, and if the device is not properly encrypted or protected, the finder can easily browse or copy all of the owner's private photos/videos. Even with a screen lock, password/PIN attacks are still a threat - attackers can try to guess simple passwords or use brute-force techniques(Ruffin, M. *et al*., 2022) [12].

Given the above situation, the need to apply advanced security technology to protect personal photos/videos is of particular concern. The first focus is data encryption: all sensitive photos and videos should be stored in an encrypted form so that even if an attacker

gets the file, they cannot view the content without the decryption key. Strong encryption will ensure that private photos can only be decrypted by legitimate users (Aldosarry, D. S. *et al*., 2021) [2]. In addition to encryption, there should be a password-proof mechanism to deal with the risk of password cracking. This includes using strong passwords/PINs combined with limits on the number of failed logins and delays between attempts to prevent brute-force attacks. In addition, an important trend is to deploy early warning systems when there are signs of unauthorized access. This system can send notifications to the owner, trigger an alarm, or even take pictures of the intruder with the front camera. Many average users currently lack convenient tools to encrypt and securely manage their private photo libraries. Although "vault" apps on the market offer photo hiding functionality, many of them have security vulnerabilities. Ruffin, M. *et al*. (2022) [12] shows that most popular vault apps do not implement file camouflage or protection well enough that even an average attacker can detect and extract hidden files from the vault. This points to a gap in protecting private photos/videos: a dedicated mobile security architecture is needed that ensures both strong encryption and the ability to detect and prevent intrusion attempts in a timely manner.

Based on that practical requirement, this research topic is chosen to propose a security architecture for mobile media storage with a focus on protecting users' private photos/videos. The solution we aim for will tightly integrate personal data encryption, anti-vandal password mechanism and early warning system when there is unauthorized access.

## Literature Review

### Vault Apps to Protect Private Photos/Videos

Mobile "vault" apps are apps designed to create a private storage space for sensitive photos, videos, and files on a smartphone. They often disguise themselves as a normal app (e.g., a calculator or calendar) and require a password or additional authentication to access the content inside (Ruffin, M. *et al*., 2022) [12]. Many vault apps offer features such as setting a separate password for the photo folder, and even allowing the setting of a "decoy" mode - that is, a secondary password that opens a fake set of content to distract unwanted viewers. Dorai *et al*. (2020) [6] surveyed 2,364 suspected "vault" iOS apps and identified 1,118 that actually hid content; the research team also noted that many applications integrate features such as decoy mode, data encryption capabilities, or password storage.

Despite their privacy-enhancing properties, many vault applications reveal significant security shortcomings. Some vaults do not actually secure data; instead, they rely primarily on obfuscation techniques to avoid detection and, in some cases, have even been misused to conceal illicit information (Xie *et al*., 2020) [14]. Ruffin *et al*. (2022) [12] conducted a security analysis of 20 popular Android vault apps and found that only 5 out of 20 (25%) implemented genuine file-level encryption. The majority merely concealed content by altering file extensionXies or hiding directories, leaving data easily recoverable once system-level access was obtained. Their study further demonstrated that an adversary with only basic technical knowledge could still identify the presence of most vault applications on a device and extract hidden files without the need for advanced forensic techniques.

### Intrusion Alerts and Prevention Mechanisms

Given that many vault applications can be identified or bypassed, researchers have proposed automated detection approaches and proactive defense mechanisms. Xie *et al*. (2020) [14] applied machine learning techniques, specifically a Support Vector Machine (SVM) classifier, to distinguish vault applications from regular apps based on behavioral patterns and permission usage, achieving an accuracy rate of 93.33%. More recently, Johnstone *et al*. (2025) [9] even employed advanced machine learning models to detect vault applications on Android with an accuracy approaching 98%.

Beyond detection, intrusion alert and prevention systems have also been integrated to safeguard data against unauthorized access. Many vault applications implement features such as automatically capturing an intruder's photo after multiple failed login attempts or sending email alerts to the device owner. Koh, Nieh, and Bellovin (2021) [7] introduced the Easy Secure Photos system, which integrates real-time alert mechanisms with client-side encryption to protect personal images even if the device is stolen (ACM MobiSys). Similarly, research in the field of mobile security (Xie *et al*., 2020) [14] emphasizes that instantaneous alerts - such as push notifications, temporary account lockouts, or intruder snapshots - are indispensable components of a multi-layered security architecture. These proactive mechanisms not only enable timely detection but also provide forensic evidence to help prevent or deter unauthorized access to users' private photos and videos.

### Image/Video Data Encryption

To thoroughly protect photos and videos, encryption plays a pivotal role. However, applying encryption on mobile devices requires a careful balance between security and usability. Koh *et al*. (2021) [7] proposed the Easy Secure Photos (ESP) system - a client-side security architecture that enables users to encrypt images before uploading them to cloud services (e.g., Google Photos) while still maintaining the original image format to ensure compatibility with existing platforms. ESP leverages format-preserving image encryption, combined with encrypted thumbnail previews and a user-friendly key management mechanism. As a result, encrypted photos remain in standard JPEG format, allowing them to be stored and previewed on the cloud, while the actual content is securely protected. This research demonstrates that it is possible to achieve both strong security and high usability, enabling users to benefit from mainstream cloud services without sacrificing the privacy of their personal images. In addition, other research directions have explored selective encryption (focusing only on sensitive regions of the image) and the application of chaotic cryptography to secure media content while saving resources on mobile devices (Ruffin *et al*., 2022) [12].

An important aspect of secure media protection is encryption key management in multi-device environments. The aforementioned ESP system implemented a lightweight key management scheme that allows device authorization by scanning a QR code via the cloud service, thereby securely sharing decryption keys among a user's devices (Koh *et al*., 2021) [7]. This suggests that future photo/video protection applications should incorporate mechanisms for secure key

synchronization and backup, ensuring users do not lose access to encrypted data when changing devices or forgetting their passwords. Some studies have explored the concept of honey passwords for vault applications - creating decoy vaults with fabricated content whenever an incorrect password is entered, thereby misleading attackers and complicating brute-force attempts (An *et al*., 2024; Ruffin *et al*., 2022) [3,. 12].

**Methodology**

The application was developed using Flutter, a cross-platform framework that enables simultaneous deployment on both Android and iOS from a single codebase. During the implementation phase, the functional modules were progressively realized: programming the user interface according to the design specifications, integrating cryptographic libraries, configuring the database for metadata storage, and incorporating device APIs (e.g., camera, notifications) to support the intrusion alert system. The source code was continuously tested and refined throughout development to ensure that each component operated precisely as intended.

The media security architecture was designed following a multi-layered model, tightly integrating all security components, which is illustrated in Figure 1

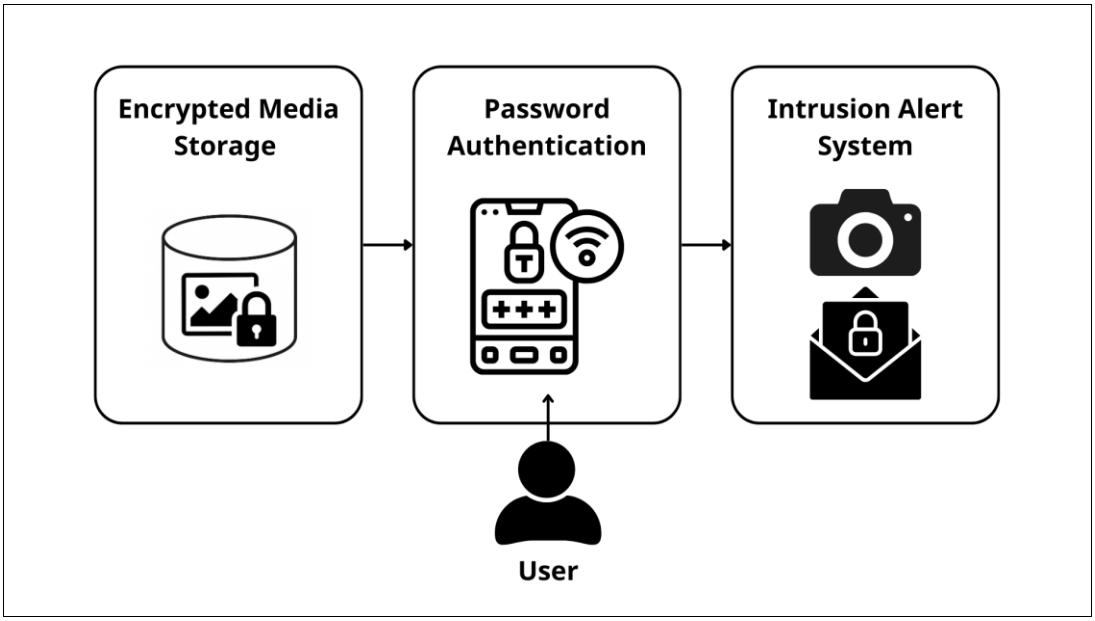


**Fig 1:** System Architecture

**Encrypted Media Storage Module**

The encrypted media storage module is responsible for the encryption and decryption of users' image and video files. When a user imports photos or videos into the application, each file is encrypted using a symmetric encryption algorithm and stored solely in encrypted form, either in the device's local memory or within the database. Each file may be associated with a dedicated secret encryption key or utilize a key derived from the user's password. The metadata of the file - such as filename, size, and creation date - is stored in the database (either local SQLite or Firebase Firestore in the cloud) to facilitate management and retrieval, while the actual content of the photo/video remains securely protected in its encrypted format.

**Password Authentication**

The password authentication layer serves as the first line of defense in the system, ensuring that only legitimate users can access the encrypted media vault. Upon initial setup, the application requires the user to define a master password (or PIN). This credential is securely stored in the application memory in the form of a cryptographic hash rather than plaintext. Each time the application is launched, users must provide the correct password to be granted access. This layer effectively prevents unauthorized entry into the application and also acts as the trigger point for subsequent intrusion detection and alert mechanisms.

**Intrusion Alert System**

The intrusion alert system continuously monitors login attempts and identifies suspicious activity. If the user (or an intruder) enters incorrect credentials beyond a predefined threshold (e.g., 5 consecutive failed attempts), the alert mechanism is activated. The system discreetly utilizes the device's front-facing camera to capture an image of the individual attempting unauthorized access. This evidence is recorded in the application's security log (either locally or in Firestore) and may also trigger a notification to the legitimate user. To avoid detection, the process is designed to be covert - for instance, the camera captures without flash and alerts can be hidden in the notification tray. Additionally, once the alert is triggered, the system can temporarily enforce login delays or account lockout to defend against brute-force attacks, thereby limiting the intruder's ability to attempt continuous password guessing.

**Results**

This study aims to propose a security architecture for mobile media storage, with a particular focus on safeguarding users' private photos and videos. The architecture tightly

integrates personal data encryption, an anti-breaking password mechanism, and an early intrusion alert system to mitigate unauthorized access risks. Specifically, a prototype application - named PhotoGuard - was developed as a proof of concept. PhotoGuard enables users to securely store personal photos and videos within a protected vault. The system requires users to configure a 6-digit PIN code, which is securely hashed and stored to prevent exposure or leakage. Furthermore, the application incorporates an intrusion-capture feature, whereby the device's front-facing camera automatically takes a photo of the intruder upon repeated failed login attempts and logs unauthorized access events for forensic tracking.

**Private Photo/Video Album Storage**

The application allows users to create private albums containing photos or videos, each secured with a user-defined password. On the main interface, albums are displayed with a red lock icon, indicating that their contents are protected. To access any album, the user must first unlock it by entering the correct password. All photo and video data within the album is stored in the device's internal memory and is either encrypted or concealed under the authentication layer. This ensures that, without using the application (i.e., without the correct password), external parties cannot directly read or retrieve the actual media files.

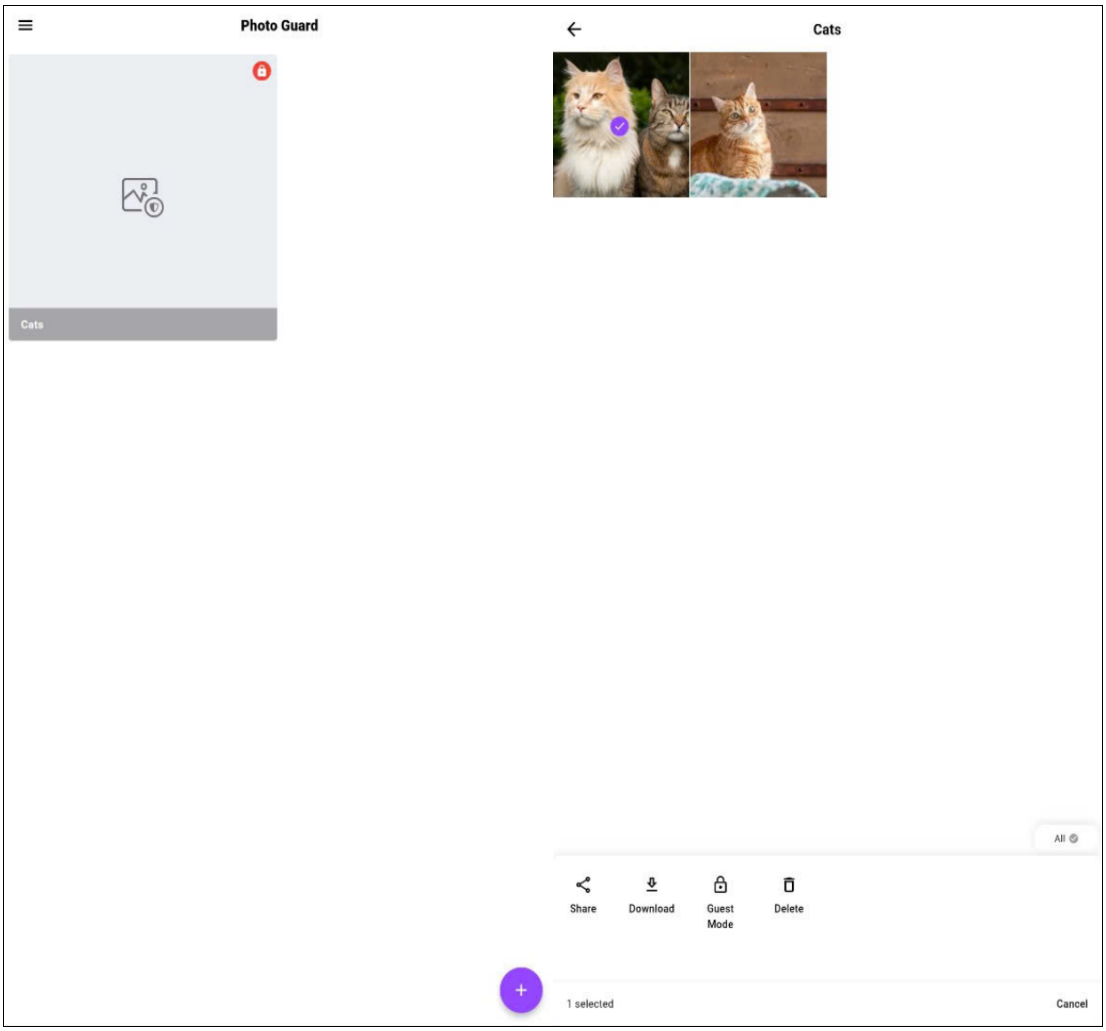


**Fig 2:** Photo/Video Album Storage

**Cryptographic Mechanism**

The application employs a cryptographic mechanism to protect the user-defined unlock password. Specifically, the password (a 6-digit PIN) is never stored in plaintext; instead, it is securely hashed or subjected to one-way encryption before being saved in the system. This ensures that even if attackers extract the application's data, they cannot recover the user's original password. During authentication, the application compares the input with the stored hashed value, thereby enabling secure verification while keeping the actual password confidential. In addition, the application integrates the device's biometric authentication (fingerprint recognition) to provide faster and more convenient access. Fingerprint credentials are bound to the device's native security subsystem, ensuring both improved usability and strong protection for private media content.

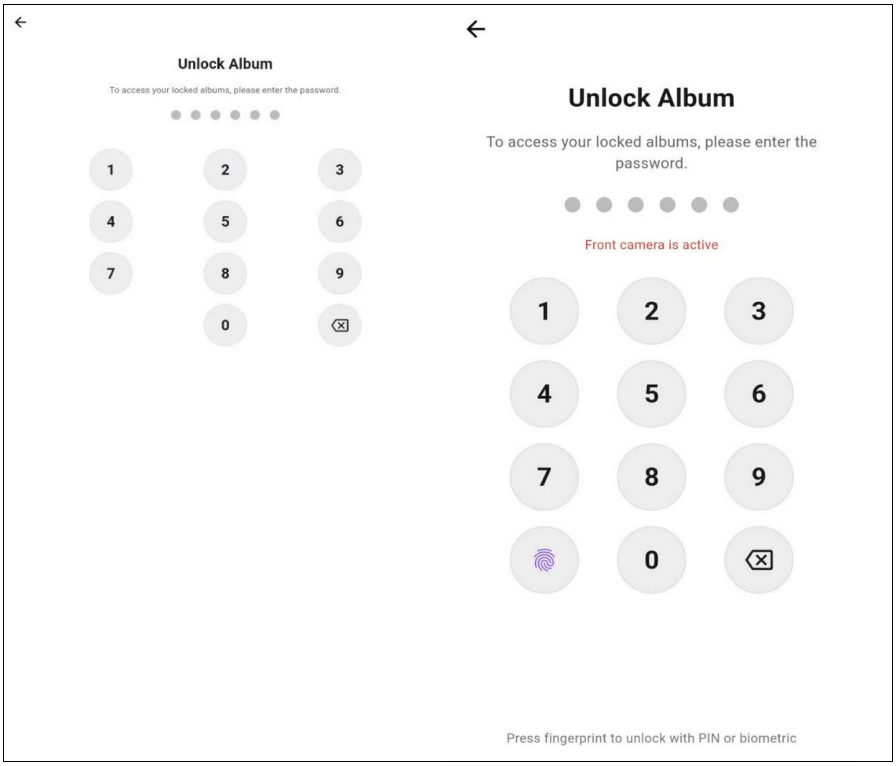


**Fig 3:** Cryptographic Mechanism

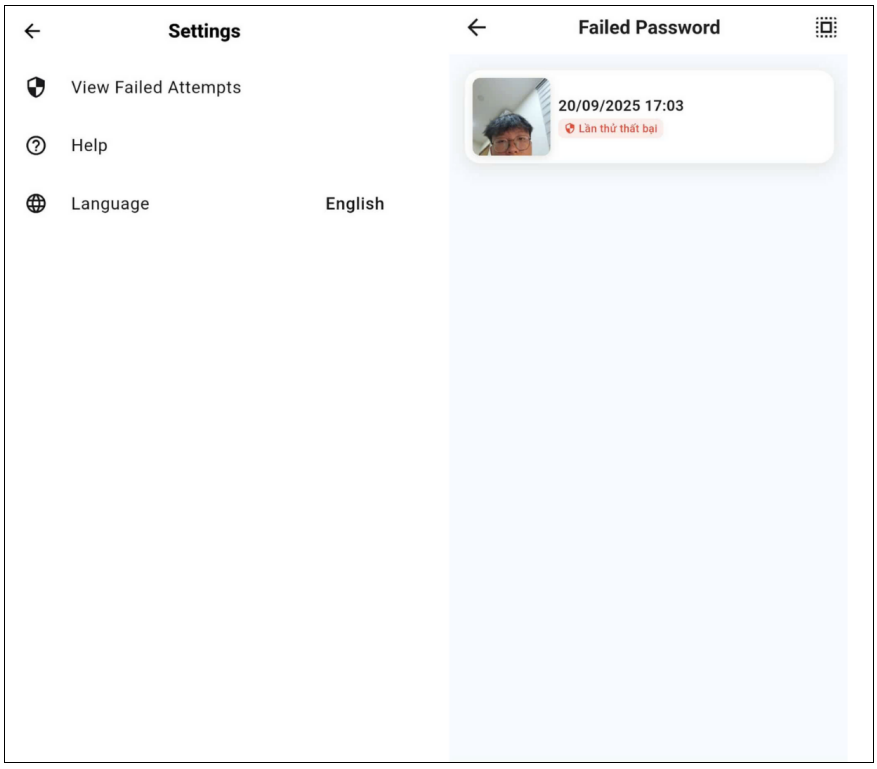


**Fig 4:** View Failed Attempts

**Intrusion Detection and Alert Mechanism**

One of the system's key features is its ability to capture intruder evidence whenever an incorrect password is entered. Immediately upon a failed authentication attempt, the application automatically activates the device's front-facing camera to capture the face of the individual attempting unauthorized access, while simultaneously logging the exact timestamp of the event. Both the captured images and corresponding timestamps are stored in the application's "Failed Login Management" module.

Users can review this section to access a complete record of unsuccessful login attempts, including visual evidence of the intruder and the time of occurrence. This enables legitimate users to identify who attempted to breach their private album and when the attempt took place. The alert mechanism was validated through real-world testing by intentionally entering incorrect passwords multiple times. Results confirmed that the system reliably captured images and recorded logs for every attempt, thereby ensuring 24/7

monitoring and forensic traceability of unauthorized login activities.

## Discussion

The PhotoGuard system integrates three layers of security more rigorously and with notable improvements compared to previous solutions.

First, regarding secure photo/video album storage, earlier "vault" applications often exhibited critical weaknesses by failing to encrypt content comprehensively. Zhang *et al*. (2017) [15] analyzed 18 popular vault apps and found that 6 of them did not encrypt stored photos at all, while 8 did not encrypt videos. Similarly, a 2021 report by the Department of Defense Cyber Crime Center (DC3) revealed that many first-generation vault apps stored passwords in plaintext and left multimedia content unencrypted, thereby facilitating unauthorized access to private data. In contrast, PhotoGuard addresses these shortcomings by encrypting all photos and videos within albums using a strong symmetric algorithm (AES-256) and granting access only after successful user authentication. This approach ensures that multimedia data remains strictly protected, significantly enhancing privacy compared to earlier vault apps that merely "hid" files without guaranteeing encryption. Furthermore, access passwords for the vault are stored as one-way cryptographic hashes, rather than plaintext, thereby strengthening resistance against credential theft and unauthorized recovery attempts.

The second layer of our system integrates password encryption and secure identity management. This aligns with prior researches on mobile authentication security, which emphasizes the importance of protecting credentials through cryptographic hashing and encryption techniques to mitigate risks from password-guessing or database theft attacks. Xie *et al*. (2020) [14] observed that several Android vault applications fail to provide "true privacy protection" - they primarily rely on interface obfuscation (e.g., disguising themselves as calculator apps) to conceal data, while not applying comprehensive encryption to the underlying content. Similarly, Ruffin *et al*. (2022) [12] , in their evaluation of vault app security, identified severe vulnerabilities in both camouflage capabilities and file protection mechanisms, across adversaries ranging from basic users to more advanced attackers. These findings reaffirm that camouflage alone is insufficient, our system prioritizes robust encryption combined with strict authentication, representing a necessary improvement over prior solutions. In other words, the system shifts its emphasis from "hiding" to "true protection" - ensuring that even if adversaries discover the data, the content remains unreadable without the correct password.

A prominent contribution of the system is its intrusion alert mechanism, which enables proactive responses to unauthorized access attempts. In the domain of mobile anti-theft solutions, recent studies have proposed the use of device cameras to capture intruder images and transmit evidence to users or law enforcement agencies upon detecting unauthorized activity (Agbonifo *et al*., 2022). Our system extends this approach by integrating a proactive intrusion-alert module: if an individual attempts to access the vault and repeatedly enters an incorrect password, the application activates the front-facing camera to capture the intruder's image, while simultaneously recording timestamp entered into the security log. Immediately, an alert notification is dispatched to the legitimate user's device or email. This mechanism establishes a proactive defense layer analogous to anti-theft systems, enabling both timely detection and the collection of forensic evidence regarding unauthorized access attempts.

## Conclusion

The study successfully designed and implemented a mobile security system that encrypts and securely protects private photos and videos on mobile devices. Experimental results demonstrated that the system operates effectively, preventing unauthorized access and enhancing the confidentiality of personal data. The proposed solution shows strong practical applicability, enabling users to safely store sensitive information while contributing a novel approach to safeguarding privacy on smartphones.

Despite its strengths, the system still presents certain limitations. Encryption performance may degrade when processing large video files, and data protection partly depends on user awareness (e.g., the need to delete original copies from the gallery after importing them into the encrypted vault). Moreover, the current solution has been deployed on a single mobile platform only, and has not yet been tested under conditions such as rooted/jailbroken devices or hardware-level attacks.

Looking forward, the system can be further enhanced through several directions: optimizing encryption performance, integrating biometric authentication alongside passwords to strengthen access control, and adding secure cloud backup for encrypted data. These improvements would help refine the solution, increase resilience against intrusion, and ensure greater data safety for users in mobile environments.

## References


1. Agbonifo OC, Afolayan AH, Akinola OH. Design of a mobile smartphone anti-theft system. Niger J Technol. 2022;40(6):1086-1095. DOI:10.4314/njt.v40i6.11 African Journals Online+1
2. Aldosarry DS, *et al*. Preserving Image Encryption for Smart Android System. TEM J. 2021;10(2):546-553.
3. An C, Xiao Y, Liu H, *et al*. Honey password vaults tolerating leakage of both personally identifiable information and passwords. Cybersecurity. 2024;7:42.
4. Cinar AC, Kara TB. The current state and future of mobile security in the light of the recent mobile security threat reports. Multimed Tools Appl. 2023;82(13):20269-20281. DOI:10.1007/s11042-023-14400-6
5. Department of Defense Cyber Crime Center. DC3 Technical Advisory File Concealment Smartphone Apps. 2021.
6. Dorai G, Aggarwal S, Patel N, Powell C. VIDE - Vault App Identification and Extraction System for iOS Devices. Forensic Sci Int Digit Invest. 2020. DOI:10.1016/j.fsidi.2020.301007
7. Koh E, Nieh J, Bellovin SM. Easy Secure Photos: Privacy-focused photo storage in the cloud. In: Proc 19th Annual Int Conf Mobile Systems, Applications, and Services (MobiSys). ACM; 2021.
8. Koh E, Nieh J, Bellovin SM. Encrypted Cloud Photo Storage Using Google Photos. In: The 19th Annual International Conference on Mobile Systems,

Applications, and Services (MobiSys '21). 2021. DOI:10.1145/3458864.3468220
9. Johnstone MN, *et al*. Using Machine Learning to Detect Vault (Anti-Forensic) Apps. Future Internet. 2025;17:186. DOI:10.3390/fi17050186
10. Pew Research Center. How Americans View Data Privacy: Section "How Americans protect their online data." 2023.
11. Rise Above Research. Worldwide Image Capture Forecast: 2020-2025. 2021.
12. Ruffin M, Lopez-Toldeo I, Levchenko K, Wang G. Casing the Vault: Security Analysis of Vault Applications. In: Proc 21st ACM Workshop on Privacy in the Electronic Society (WPES '22). 2022. DOI:10.1145/3559613.3563204
13. Sharma V, You I, Andersson K, Palmieri F, Rehmani MH, Lim J. Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. IEEE Access. 2020;8:167123-167163. DOI:10.1109/ACCESS.2020.3022661 OUCI+1
14. Xie N, Bai H, Sun R, Di X. Android Vault Application Behavior Analysis and Detection. In: Zeng J, Jing W, Song X, Lu Z, editors. Data Science. ICPCSEE 2020. Commun Comput Inf Sci. Vol 1257. Singapore: Springer; 2020. p. DOI:10.1007/978-981-15-7981-3_31
15. Zhang X, Baggili I, Breitinger F. Breaking into the vault: privacy, security and forensic analysis of android vault applications. Comput Secur. 2017. DOI:10.1016/j.cose.2017.07.011