IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2

StegaVault: Secure Note Management using Encryption and Image Steganography

Aryan Kalekar[1], Kripa Doshi[2], Sakshi Jagtap[3], Shounak Dhepe[4], Vijaya Patil[5]
Department of Computer Science and Engineering[1-5]
MIT School of Computing, MIT Art, Design and Technology University, Loni Kalbhor, Pune, India
[1]aryankalekar123@gmail.com, [2] kripandoshi@gmail.com, [3]sakshijagtap456@gmail.com
[4] shounakdhepe14@gmail.com, [5]vijaya.patil@mituniveristy.edu.in

Abstract : *The development of digital storage of personal and academic information has raised concerns regarding the level of confidentiality of the stored information. Traditional note taking apps and text files expose users to potential sensitivities in the event that the stored files or devices are accessed by unauthorized parties. Even though the encryption guarantees the security of the information, this does not mean that the information will go unnoticed. This paper provides information about StegaVault which is a note management system which uses AES-GCM algorithm in conjunction with image steganography. The system encrypts notes provided by users then hides the notes in PNG images. In retrieving information the users have to first extract the encrypted data then use AES-GCM authentication decryption algorithm to revert the information back to its original state. Moreover, it is important for the users to note that the authentication process enables the users to identify any incorrect key or alteration of the information. A model has been developed to describe how storing and retrieving of information takes place. The software is meant to provide an extra layer of protection for the users through the combination of steganography and cryptography.*

Keywords: AES-GCM, Image Steganography, Information Security, Data Confidentiality, Secure Note Management, Data Integrity.

I. INTRODUCTION

The development of digital storage of personal and academic information has raised concerns regarding the level of confidentiality of the stored information. Traditional note taking apps and text files expose users to potential sensitivities in the event that the stored files or devices are accessed by unauthorized parties. Even though the encryption guarantees the security of the information, this does not mean that the information will go unnoticed. This paper provides information about StegaVault which is a note management system which uses AES-GCM algorithm in conjunction with image steganography. The system encrypts notes provided by users then hides the notes in PNG images. In retrieving information the users have to first extract the encrypted data then use AES-GCM authentication decryption algorithm to revert the information back to its original state. Moreover, it is important for the users to note that the authentication process enables the users to identify any wrongful key or alteration of the information. A model has been developed to describe how storing and retrieving of information takes place. The software is meant to provide an extra layer of protection for the users through the combination of steganography and cryptography [1], [3].

A. Motivation

The concept underlying StegaVault is related to the requirement for a practical method of securing personal notes, taking into consideration the aspects that go beyond just storing text. One might want to have some protection of his/her data in place without calling too much attention to the fact that the data is stored in electronic form. The combination of the concepts of encryption and image steganography leads to an examination of the possible application of both techniques together in the note-taking software [1].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2

B. Objectives

The objective behind the StegaVault project is to create a safe note-taking application using AES-GCM encryption and LSB image steganography in order to keep sensitive academic, personal and private data secure. The program functions by encrypting notes before hiding them into PNG images, which preserves their confidentiality and integrity. Only authorized people can retrieve and decrypt the original note by means of a key. This application has been designed to guarantee its usability and easy utilization thus it doesn't require users to have any technical skills.

II. RELATED WORK

Steganography and cryptography, which are parts of the sphere of information security today, have already been developed quite successfully. While encryption has a range of techniques for the security of information, steganography helps to conceal information that already exists. The combination of these two fields of knowledge enables the creation of various methods of securing information.

A. Image Steganography Techniques

A brief introduction to steganography is offered by Bandyopadhyay et al. [1]. An analysis of other types of information hiding methods is provided in this paper, including image, audio, and video and text steganography. The authors give an overview of several image-based techniques, such as LSB insertion, masking and filtering, redundancy pattern encoding, and encrypt-and-scatter method. Among other topics covered in this paper there are invisibility, capacity and robustness. The notions proposed in this paper are a starting point for researching image based information hiding techniques, which will be useful for the further analysis of StegaVault as this system is based on photographs. Digital Image Steganography. In their work, Mandal et al. [2] provide an overview of digital image-steganography techniques. They analyse the various techniques and difficulties encountered in concealing data in digital images. The most important aspects of any image-steganography system are the quality of the image, capacity of the data and the method used for embedding. These factors are significant in the case of StegaVault, which may influence the number of bits of information that can be stored in an image.

B. Authenticated Encryption

According to the National Institute of Standards and Technology (NIST), the Galois/Counter Mode (GCM) is one of the authenticated encryption modes for the block cipher [3]. The AES-GCM provides both the confidentiality and the authentication by using the technique of encryption that generates an authentication tag. In StegaVault, AES-GCM is used to encrypt notes and authenticate whether the encrypted data is genuine on retrieval.

III. RESEARCH GAP AND PROBLEM DEFINITION

The literature surveyed creates a solid foundation in terms of comprehending the image steganography, encryption and data security concepts which have been discussed in the current research. As regards the tutorial reference cited in the paper of Bandyopadhyay et al. [1], it touches upon the issues related to the basic data-hiding approaches but no information is given about how this technique could be used to hide confidential notes. There are certain practical aspects of image steganography, such as embedding capacity, image quality, extraction efficiency, which should be considered when the data encryption process is carried out within JPEG images as suggested by the authors [1], [2]. According to the literature reviewed in this paper, the current research is dedicated to the possibility of combining authenticated encryption and image steganography in order to develop the effective note management approach. In particular, the researchers face the problem of developing and testing the system aimed at providing the confidentiality of the note content via AES-GCM encryption and image steganography. The research study is aimed at answering the following research question

1. What is the approach to integrating image steganography with AES-GCM encryption in an efficient note-management system?
2. What is the effect on image quality and size of having encrypted data in a carrier image?
3. What is the relation between payload size and time taken to embed and extract it?

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2

4. How effective is AES-GCM authentication in revealing modified keys and encrypted payload?
5. To what degree is the system able to restore information in images which were not edited through unsupported methods?

IV. PROPOSED SYSTEM AND CONTRIBUTIONS

StegaVault is a system that gives a holistic solution for safe storage of notes. It consists of encryption methods, hiding information in images, and retrieving methods that are verified. The main contribution of this research is providing a framework for storing notes called StegaVault that brings together AES-GCM encryption with image steganography. The framework encrypts the notes with AES-GCM so that their content is protected during the retrieval step. The data that has been encrypted is hidden into the PNG file to hide its existence. The system has a retrieval technique that utilizes the data that is hidden and decrypts it. The current paper also introduces the trial examination of the system itself which relies on image characteristics.

V. PROPOSED METHODOLOGY

The StegaVault method comprises two fundamental actions. Storage is the first operation where a user's message is encrypted and hidden in a picture. Retrieval is the second operation where a secret message is recovered and decrypted.

A. Note Input

The procedure is initiated as soon as the user submits their sensitive data through the application interface. The note is taken into account and sent to the encryption module.

B. AES-GCM Encryption

The input note is AES-GCM encrypted using a cryptographic key that is unique and gives rise to the cipher text and an authentication tag. Encrypted information is sent to the image-steganography module, with the nonce and authentication tag remaining stored along with the data needed for decryption. AES-GCM provides confidentiality and authentication: the mechanism of authentication allows the system to detect whether any modifications were made to the authenticated encrypted data during decryption [3].

C. Image Steganography

Following the encryption process, the cipher text along with necessary metadata is forwarded to the steganography module. The steganography module will embed the encrypted data in the given PNG file. The PNG image will function as the carrier image. The final obtained carrier image will have embedded the required hidden encrypted data and will be used for further extraction process. It is necessary to describe the embedding method used in practice. In case of using the least significant bit insertion method, the information on its functioning and disadvantages is provided in this subsection [1]

D. Secure Storage

The image that is produced is saved for future reference. The fact that the message was encrypted beforehand means that it should not be possible to find out what the note contains by simply decoding the hidden message

E. Data Extraction

When the person requires the note that has been saved, the image that was associated with that note will be given to the application. This image is then processed by the steganography module, which will extract the hidden message from the image.

F. AES-GCM Decryption and Verification

The payload that has been retrieved goes through AES-GCM decryption with the right key and nonce parameter. The authentication tag is checked during the authenticated decryption. If the key provided is right and the data has not been altered, the original message can be obtained. If authentication does not succeed because of the wrong key or modification of the authenticated data, the system must refuse the decryption rather than pass the message off as valid plaintext.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2

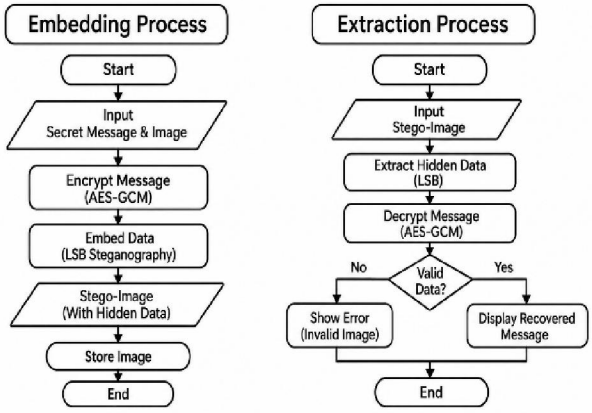


Fig. 1.Embedding and extraction process flowchart.

VI. SYSTEM

The StegaVault architecture envisaged involves a number of modules that work together to provide secure note storage and retrieval. This process is initiated by the submission of notes through the user interface, whereby the user enters confidential notes, chooses an image for performing storage and retrieval operations. In the encryption module, AES-GCM is applied to the entered notes, providing the user with encrypted data and required information for authentication [3]. This encrypted payload goes next to the steganography module, which hides it into some selected PNG image [1], [2]. The storage module saves the image generated for future access. Then on, the steganography module extracts the hidden encrypted content from within the stored image and passes it to the decryption and validation module. This module performs AES-GCM authenticated decryption with the right key to decrypt the hidden data [3]. If authentication succeeds, the original note is recovered; otherwise, the application declines the decryption operation. Together, these modules provide a complete process for protecting and retrieving confidential notes.

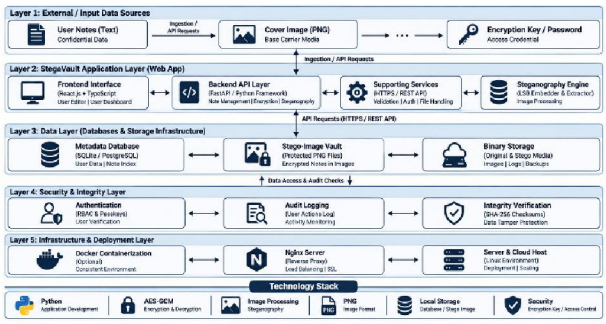


Fig.2.System Architecture.

A. Implementation Details

An operational model of StegaVault has been formulated to illustrate the suggested technique. Its realization has been divided into four main functions: encryption, insertion of image, extraction of image, and decryption.

B. Encryption Module

The encryption section takes the note from the user and encrypts it with AES-GCM. The cipher text, nonce and authenticate tag obtained are saved in the required format needed for its retrieval.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2

C. Embedding Module

The steganography system then takes the encrypted payload and embeds it into the chosen PNG image, producing the final image.

D. Extraction Module

The first step towards retrieving the payload is managing the image that was generated, thus revealing the embedded data.

E. Decryption Module

The decryption process requires utilizing the right cryptographic key along with the associated nonce to perform the AES-GCM authenticated decryption. If the verification process passes, then the original text message is recovered once more.

F. Technology Stack

The StegaVault prototype leverages different approaches in order to accomplish encryption, image steganography, and secure note storage. A list of technologies employed for components of the StegaVault is given in Table I

TABLE I. Technology Stack

Category	Technologies
Frontend	HTML5, CSS3, JavaScript
Mobile App	Android / iOS
Backend	Python, Flask, REST API
Database	SQLite, SQL
Encryption	AES-256-GCM, PBKDF2
Steganography	Pillow, LSB Steganography
AI/ML	PyTorch, U-Net

VII. EXPERIMENTAL SETUP AND EVALUATION

The evaluation of the StegaVault prototype system must be carried out through controlled experiments to assess its functionality and image-related performance.

A. Experimental Environment

StegaVault was evaluated in real-time by means of a web-based prototype using Python programming language. The prototype was run on a Windows operating system. AES-GCM implementation was done through PyCryptodome. Also, the Least Significant Bit (LSB) technique was used for the embedding of the encrypted information into PNG images. The focus was on testing the main operations of the system, namely encryption of notes, data embedding, and data storage into images, data extraction, and decryption.

B. Evaluation Approach

The present evaluation was conducted to check the performance of both the encryption module and the steganography module. For the encryption process, the plaintext is being converted into ciphertext by the AES-GCM encryption algorithm. The encrypted data is then embedded into the selected PNG image through the LSB technique. The original cover image was then compared with the new stego image to check for any changes resulted from the embedding process. For the extraction purpose, the data is usually retrieved from the stego image through the decryption process and decrypted to get the original note. The analysis of the proposed image-steganography technique took into account the impact of the quality of the image, its embedding capacity, and processing time on the efficiency of the new approach. Earlier studies have already indicated the importance of quality, capacity, and ability to hide messages [1], [2]. However, the current analysis cannot fully be described as quantitative, but rather qualitative in character (since only comparisons of PSNR and SSIM) have been made.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2



Fig. 3.Visual comparison of the original cover image and the generated stego-image.

A visual comparison was made between the cover image and the resulting stego-image to note the alterations made due to the LSB embedding process. The comparison offers a qualitative perspective on the process of image hiding. Since there are no quantitative measures like PSNR and SSIM taken into account, there is no claim made regarding the numerical improvement of the quality of an image.

C. Functional Testing

Functional testing was utilized to assess how StegaVault operates under different input parameters. The process of locking and embedding utilized valid notes inputs within a PNG format. The corresponding stego-image was compared against the respective cryptographic keys to verify the success of the extraction and decryption. The application was tested against a wrong key test to assess the functioning of the authentication mechanism of AES-GCM. A modified-payload test was performed to check if any alteration in the authenticated encrypted data affected the process of decryption. Additionally, tests were performed on invalid images to analyse how the software operated with images which are invalid or unsupported. The right-key retrieval test demonstrated that the note could be properly retrieved after decrypting the note successfully using the private key. The tests with the wrong keys and the altered payload revealed how AES-GCM fails during the authentication verification stage. The comparison between the cover image and the stego-image represented a preliminary means to evaluate the process of LSB embedding. Thus, the connections between the key StegaVault modules were established.

TABLE II. Functional Testing of StegaVault

Test ID	Test performed	Expected outcome
T1	Note encryption	Encrypted
T2	Payload embedding	Embedded
T3	Correct-key retrieval	Recovered
T4	Incorrect-key test	Rejected
T5	Modified-payload test	Rejected
T6	Invalid-image test	Rejected
T7	Visual image comparison	Compared

VIII. RESULTS AND DISCUSSION

The StegaVault prototype showcased how AES-GCM encryption and image steganography are integrated into a note-management application with security functions. The prototype displayed different stages involved in receiving confidential notes from users, encrypting the notes, hiding the resulting encrypted data in a PNG file, and recovering the hidden notes through decryption. Thus, the solution puts together cryptography and hiding of information using images [1], [2].The AES-GCM algorithm is used as a part of the encryption module for securing the content of user notes. During recovery, the hidden encrypted data undergoes decryption using the key for decryption. The AES-GCM encryption process helps to identify the incorrect keys and corruption of the encrypted information [3]. Thus, the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2

recovery of the original note is possible due to the key and information being correct. The image-steganography module showed how PNG images could be used as carrier files for encrypted data. The stego-image allowed the hiding of the existence of an encrypted payload in an image without attracting attention. There are important aspects to consider in image steganography, such as visual quality, embedding capacity, and extraction reliability. The prototype was effective in demonstrating how encryption and steganography could be combined into a single document processing system, but the current evaluation was mainly focused on implementation and demonstration of functionality. Quantitative measures such as PSNR, SSIM, payload capacity, embedding time, and extraction time were not part of the present study. In general, StegaVault applies a comprehensive method of storing private notes by amalgamating AES-GCM encryption with image steganography. The system gives rise to the essential performance of the system and sets the basis for the next development, namely performance assessment, image quality assessment, management of keys, and safe information transfer.

IX. SECURITY ANALYSIS

StegaVault's reliability is dependent on proper encryption mechanisms, secure key management, and sound image-steganography. AES-GCM is responsible for confidentiality by ensuring encryption of notes before embedding them into an image. Hence, getting the encrypted content does not necessarily mean a person can have access to the original note. Moreover, AES-GCM provides authentication by means of an authentication tag which must be verified during decryption. If an incorrect key is used or the encrypted message is altered, authentication fails. Image steganography makes it impossible to detect whether there is any encrypted message within the carrier image but there is still a possibility of detecting the presence of hidden data. Another aspect of security is key management. In particular, it is important to protect the cryptographic key from being revealed in source code and from being stored in an insecure way with the carrier image. Besides, proper implementation of AES-GCM requires proper handling of nonce, which plays a crucial role in the encryption security [3]. The integrity of the carrier image influences the extraction process, as certain modifications that include image conversion, resizing, cropping, and compression may harm or change the payload [1], [2].

X. LIMITATIONS

While StegaVault successfully showcases the incorporation of AES-GCM encryption and the idea of image steganography based on LSB, its current version has some drawbacks. Its evaluation stresses functional testing that includes encryption and decryption processes, embedding, extraction, correct-key discovery, rejected keys, modified payload technique and invalid images procedure. The project did not yet result in conclusions on its quantitative performance features such as PSNR, SSIM, and embedding and extraction duration of time. The system also applies only PNG images for embedding the data that may affect the retrieval process in case the photo's property changes. Hence, it is necessary to conduct more tests of the current breakthrough in order to improve its performance level related to image quality and payload. The contemporary process for LSB-based systems may be subject to image processing operations like compression, resizing and filtering thus causing failures with hidden-data recovery.

XI. FUTURE SCOPE

In the near future, StegaVault can be enhanced with additional state-of-the-art image-steganography solutions to boost its performance in terms of information hiding, images' quality, and resilience to changes. The effectiveness of the system can be measured with the help of such measures as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), embedding time, and payload. These values may dramatically influence performance indicators during various implementation processes. Moreover, the technology can be applied in different image types and formats as well as cases when larger note payloads are used. It is possible to use the more reliable systems of key management, including the secure systems of key storage and creation. The further testing would show how well the new technology works when it comes to the compression of images, resizing of images, filtering, etc., which can eventually influence the retrieving of hidden information. In addition, it is possible to think of the user identifying

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, November 2026
Impact Factor: 8.2

process, encrypted cloud storage, and backup systems for data proper management. Furthermore, a mobile version of the program can be created, making it possible for people to use StegaVault.

XII. CONCLUSION

The authors introduce StegaVault, a secure system for handling notes that combines AES-GCM cryptography with steganography in images. By using this technology, notes will go through the process of encryption in advance of being included in a PNG image. When the notes are retrieved, the extraction of the information and the process of decrypting will allow for obtaining the original note content. The combination of the two technologies resolves two challenges with respect to information protection. Image steganography aims to conceal the presence of embedded information within a carrier image. However, the possibility of detecting hidden data cannot be completely eliminated. A working prototype illustrates how storage and retrieval work. Further experiments are needed for verification of image quality, capacity for embedding, time for processing, and reliability during retrieval. Improvement in terms of the management of keys, ways of sharing, and robustness is bound to improve the system.

ACKNOWLEDGEMENT

The authors wish to convey their heartfelt appreciation to the project guide as well as the faculty members for their unwavering support, encouragement, and wisdom throughout the StegaVault project. Moreover, the authors wish to extend their gratitude to the MIT Art, Design, and Technology University's Department of Computer Engineering and Technology for providing the necessary materials. Lastly, the authors wish to thank all those who helped in the successful realization of the project.

REFERENCES

1. S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
2. J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
3. S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
4. M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in Proc. ECOC'00, 2000, paper 11.3.4, p. 109.
5. M. H. Kombrink, Z. J. M. H. Geradts, and M. Worring, "Image steganography approaches and their detection strategies: A survey," ACM Comput. Surv., vol. 57, no. 2, Art. no. 33, 2024, doi: 10.1145/3694965.
6. S. Rahman et al., "A novel and efficient digital image steganography technique using least significant bit substitution," Scientific Reports, vol. 15, Art. no. 107, 2025, doi: 10.1038/s41598-024-83147-3.
7. M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image steganography using LSB and hybrid encryption algorithms," Applied Sciences, vol. 13, no. 21, Art. no. 11771, 2023, doi: 10.3390/app132111771.
8. E. J. G., H. M. A., and F. H. M. S., "Enhanced security: Implementation of hybrid image steganography technique using low-contrast LSB and AES-CBC cryptography," Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 8, 2022, doi: 10.14569/IJACSA.2022.01308104.