2023 6th International Conference on Advances in Science and Technology (ICAST)

Review: Converging Encryption, Hashing and Steganography for Data Fortification

Devansh Vora
Department of Computer Engineering
K J Somaiya Institute of Technology, Mumbai
Mumbai, India - 400022
dav@somaiya.edu

Harshala Ubhare
Department of Computer Engineering
K J Somaiya Institute of Technology, Mumbai
Mumbai, India - 400022
harshala.u@somaiya.edu

Yash Chheda
Department of Computer Engineering
K J Somaiya Institute of Technology, Mumbai
Mumbai, India - 400022
yash.bc@somaiya.edu

Pradnya Bhangale
Department of Computer Engineering
K J Somaiya Institute of Technology, Mumbai
Mumbai, India - 400022
pyb@somaiya.edu

2023 6th International Conference on Advances in Science and Technology (ICAST) | 979-8-3503-5981-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAST59062.2023.10455052

***Abstract* –In today's digital world, storing and transmitting sensitive data electronically is common but risky due to the potential for unauthorized access, disclosure, modification, or destruction. To tackle this challenge, our proposed system offers a comprehensive solution focusing on secure data transmission. AES-GCM or Advanced Encryption Standard in Galois/Counter Mode, is a type of encryption. with flip and rotational LSB (Least Significant Bit) steganography techniques to ensure secure data transmission and covert concealment within digital images This integrated approach offers a single, robust platform that not only guarantees the confidentiality of data but also verifies its integrity and enables covert communication within image files. The goal of our proposed system is to increase data confidentiality by allowing secret data transfers inside seemingly benign pictures.**

Keywords: steganography, AES-GCM, HMAC, cryptography, hashing, encryption.

I. INTRODUCTION

In the era of surging internet-based communication and escalating data transfer volumes, safeguarding data integrity is paramount. Intrusion techniques by hacker groups constantly evolve, presenting growing challenges to protect sensitive information. While traditional cryptographic methods transform data into an unreadable form, AES-GCM, emerges as a valuable ally. It encrypts and verifies data authenticity, combining AES encryption with Galois Message Authentication Code (GMAC). AES-GCM ensures data remains secure and tamper-evident, even if intercepted during transmission. In this ever-higher stakes landscape of data security, encryption systems, like AES-GCM, continuously evolve with robust algorithms and stronger encryption keys.

Additionally, steganography plays a unique and pivotal role. Unlike cryptography, steganography conceals communication parties by embedding hidden messages within cover media, making detection exceedingly challenging. This technique offers invaluable protection for data, conceals critical information on computers, secures communication contents in messages or documents, and ensures that sensitive data remains accessible only to its intended recipient. Steganography can also enable discreet, secret communication, allowing individuals to exchange information without arousing suspicion or detection by unauthorized parties. In tandem with encryption methods like AES-GCM, steganography forms a powerful arsenal in the ongoing battle to safeguard data and communications in the digital age.

As data security takes precedence, encryption, through methods like AES-GCM, remains a vital shield, ensuring that intercepted data remains indecipherable without the proper decryption key. In response to rising security risks, encryption systems persistently innovate and enhance their defenses, while steganography continues to be a valuable asset in the realm of covert communication and data protection.

II. LITERATURE SURVEY

The following part summarizes important studies on information security systems and methods using cryptography and steganography.

In [3], Lalit Negi and Lokesh Negi suggested a new way to protect data that uses both coverless image steganography and cryptography. This new method is faster and safer than the previous system they made by combining cryptography and steganography, which was an Android-based security system called Steg! In [1] the suggested method focuses on using picture steganography without a cover. The suggested method employs a steganographic program that sends the secret message through an OMR sheet, since these sheets are less likely to be read. For the cryptography part, we used a 128-bit version of the Advanced Encryption Standard method. The existing methods, DES and 3-DES, are not as safe as AES.

The author of [4] describes a steganography image application that offers safe data sharing, as well as security and privacy. This is because steganography uses the AES and random bit methods to hide messages in multimedia data that isn't expected.In [6], In this study, protected pictures, we offer a simple, quick, and proven way to secure data. On document files,an integration of AES and LSB methods may be utilized to ensure that extremely sensitive corporate documents are kept secure both when they are delivered and when they are received. There are no bugs in the way the application works when the paper is saved[2].while putting secret information in a cover photo using a strong main idea a way to hide information by replacing random pixels in a cover image with bits of a secret message that can only be read with a secret key and a stego picture. Change the pixels on the main picture to binary 24-bit, with three sets of 8-bit values.

[5] The suggested method is safer than usual LSB ways since it encrypts the data with a security key before adding it to the picture. The method has been tried out on different pictures and has been shown to hide data without changing the quality of the image.

[7] proposes a performance-oriented architecture for the Galois/Counter Mode (GCM) algorithm, which ensures confidentiality and authenticity. The proposed architecture is based on a pipelined implementation of GCM, which allows for parallel processing of the data. It is also optimized for high throughput and low latency. Experimental results show that the proposed architecture outperforms existing architectures by up to 17%. In [8], a parallel implementation of the AES-GCM algorithm is suggested, resulting in substantial throughput and low energy usage. The suggested method decouples the connections between authentication and encryption by using a pipelined layout and a lock-free coordination technique. In [9], It is proposed to use an FPGA to build the GHASH core for the AES-GCM cryptosystem. The suggested GHASH core is based on a pipelined design and a parallel implementation of the multiplication operation, and it reaches 1.2 Gbps at 100 MHz clock frequency.

The paper [10] presents an inventive approach to concealing data in JPEG images while preserving visual quality and evading detection. It leverages JPEG compression's quantization tables for this purpose. Additionally, the author improves key management and evaluates the method's robustness, acknowledging its strengths but also pointing out potential weaknesses and capacity limitations. Apart from this, the paper [11] provides a fresh steganographic technique that is explored, involving color space conversions to hide data in images with minimal visual impact. This method relies on careful data embedding in channels with varying perceptual sensitivity, such as RGB to YCbCr. It's resilient against steganalysis but could potentially introduce color artifacts and susceptibility to attacks targeting specific channels. The paper showcases its potential for practical data concealment with minimal visual disruption.

The paper [12] suggests an innovative coverless image steganography technique that is explored, utilizing DWT approximation and pixel intensity averaging for secure data concealment while reducing detection risks. This approach relies on DWT to capture image structure, enhancing security by eliminating a distinct cover image. However, potential capacity limitations and susceptibility to advanced steganalysis techniques should be considered for practical application and robustness. In advancement, paper [13] proposes a hybrid steganographic technique, merging both Discrete Wavelet Transform and Discrete Cosine Transform to hide encrypted secret images within cover images. This method prioritizes security and robustness, leveraging DCT's energy compaction property. However, it might impact visual quality and involve a complex encryption process, as demonstrated in the results for covert communication with encrypted secret images. Table I shows the comparison of existing technologies.

III. PROPOSED SOLUTION

The proposed system is a comprehensive solution that integrates AES-GCM encryption with flip and rotational LSB (Least Significant Bit) steganography techniques to ensure secure data transmission and covert concealment within digital images as shown in figure 1.

Initially, a strong AES encryption key of 256 bits is generated along with a 96-bit initialization vector known as IV. The AES-GCM technique is then utilized for encoding data that needs to be protected. This process involves dividing the data into blocks and encrypting each block individually. During encryption, a counter (CTR) value is initialized, which ensures that each block is encrypted with a unique value to prevent nonce reuse and enhance security. As part of the encryption process, additional authenticated data (AAD) can also be included, which serves as supplementary information to be authenticated but not encrypted. An authentication tag (AT) is calculated using the encryption key, the encrypted text, and the AAD.

TABLE I. Comparison Between the Existing Technologies

Ref. of paper	Methodology	Advantages	Limitations
[1]	For LSB steganography, AES 128 is used to secure and recover the message and hide the hidden message inside it.	The suggested method is easy for people to use and can grow easily.	The system does not address all types of attacks.
[2]	Information, LSB steganography, AES Cryptography and an MP3 file.	Conceal a big quantity of info in a digital picture	Slightly reduce the quality of the image
[3]	AES algorithm for coverless image steganography.	More secure than available systems.	The steganalysis attack can be used against this system because it uses old-fashioned picture steganography.
[4]	The AES and random bit method are used in this application.	Steganography is a safe way to send data that can be used on many types of data, like voice, video, and pictures.	Still vulnerable to some attacks and may reduce image quality.
[5]	LSB Steganography, Masking and Filtering, Fingerprinting and Watermarking Algorithm	There are many ways that the system can be used to send private information. It's simple to use the method.	There are some bugs in the system that can still be found by AI and ML algorithms. The method can slightly lower the brightness of the picture.
[6]	Traditional techniques, generic Adversarial Network-Based techniques, and CNN-based methods.	Protection, accuracy, and safety of the data	This restricts their use for transmitting large volumes of information.
[7]	Pipeline the AES algorithm, use a parallel architecture for the GHASH function, and combine the AES and GHASH functions in a pipelined manner	High throughput, Low latency, Efficiency	High Complexity, high cost, vulnerable to attacks, not scalable, high power consumption
[8]	Partition the AES-GCM algorithm into multiple tasks, Execute the tasks in parallel on multiple cores, Use a lock-free synchronization mechanism	Ease of implementation, Energy efficient, High throughput, highly Scalable	complex, vulnerable to attacks, It may have some overhead associated with the thread pool and the lock-free synchronization mechanism
[9]	Pipeline the GHASH algorithm, use a parallel architecture for the multiplication operation, Use a redundant register method to resolve the bit-parallel multiplier's huge fan-out problem	Security Enhancement, Efficient AES-GCM, Resolution of Fan-Out Problem, High Throughput, Versatile	Hardware Overhead, high Complexity , Limited Application Scope
[10]	Create robust DCT set, combine with steganographic costs, use lattice embedding, and perform 64 recompressions	Robust steganography, difficult detection, and higher payload	Complex calculations for optimal hiding and may reduce image quality
[11]	Select blank image, split into channels, initialize ASCII message, embed codes, add security, and iterate pixels	Secure, Easy Implementation, Greater Control, and Optimized Data Hiding	Relies on HSV and YCbCr color spaces, compatibility issues are possible. Limited data size due to blank image size.
[12]	Decompose cover image, approximate coefficients, embed message, divide blocks, and reconstruct steganography image	Capacity, Robustness, Security and resistance to common image processing operations	Limited capacity, embedded in approximation coefficients, less robust to geometric attacks
[13]	Embed secret in subbands, inverse DWT to get steganography. Extract secret and inverse DWT for encrypted image	Secure, imperceptible, efficient, fast, and easy implementation	It requires a large secret image matching cover size and is not robust to attacks

This tag acts as a digital signature for the encrypted data, ensuring that it has not been tampered with during transmission or storage.

Parallel to encryption, the system integrates a flip and rotational LSB steganography module. This component allows the encrypted data to be surreptitiously embedded within digital images. The selection of appropriate cover images is facilitated by the user or the system itself. Flip LSB steganography involves flipping particular bits into an image's pixel values by substituting them with concealed information bits. This subtle alteration aims to encode the hidden data within the image's LSBs while minimizing changes that can be seen. On the other hand, rotational LSB steganography rotates pictures in a predetermined number of positions to the left or right. This "shifts" the secret information into these bits. Through small changes in image values, this method tries to hide the existence of hidden data.

In order to reduce visual artifacts, LSB steganography hides the previously created ciphertext within the cover image's pixels' least significant bits during the data embedding process. After that, The prepared picture is resized, aligned, and planned as before. The AT created by AES-GCM and securely transmitted to the receiving end inspired the name of this stego-image, which is loaded with concealed encrypted data.

The final phase of the system encompasses decryption and authentication. Upon receipt of a stego-image, the receiving end, hidden data, comprising the ciphertext, is meticulously extracted from the LSBs. Subsequently, the system verifies the authenticity of the data by generating the AT at the receiving end and verifies it by matching it with the previously generated AT. The authentication tag is an essential component for verifying data integrity towards the recipient's side. If the communication is verified to be genuine, the AES-GCM decryption module is used to decrypt the ciphertext using the encryption key.

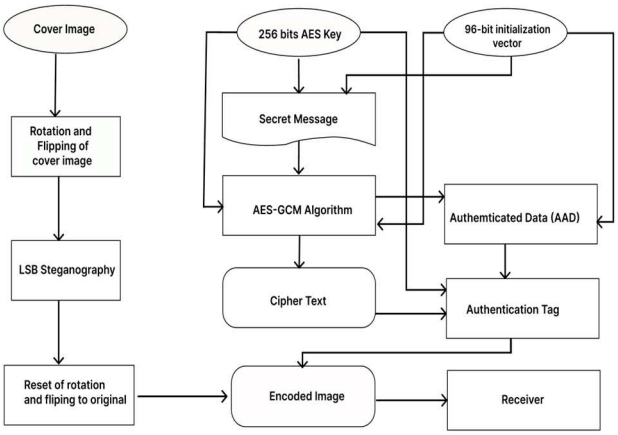

Fig. 1. Proposed System Architecture

IV. CONCLUSION

In conclusion, this paper explored AES-GCM encryption and Flip and Rotational LSB steganography, two vital components of information security. AES-GCM offers robust data protection through a combination of AES encryption and GCM mode, safeguarding against various threats. Meanwhile, Flip and Rotational LSB steganography enable discrete data embedding in images. These techniques, though distinct, can work together to enhance digital security and privacy in an increasingly vulnerable landscape. AES-GCM encryption is a very secure encryption algorithm, and Flip and Rotational LSB steganography is a relatively simple but effective steganography technique. When used together, these two techniques can be useful to embed messages to be sent in pictures without degrading the image's quality and with a heightened security.

However, it's crucial to note that none of the steganography technique is perfect, an attacker who knows about AES-GCM encryption and Flip and Rotational LSB steganography may be able to extract the secret message from a steganography image. Therefore, it's crucial to combine these methods with other security precautions like two-factor authentication and secure passwords.

REFERENCES

[1] L. Negi and L. Negi, "Image Steganography Using Steg with AES and LSB," 2021 IEEE 7th International Conference on Computing, Engineering and Design (ICCED), Sukabumi, Indonesia, 2021, pp. 1-6, doi: 10.1109/ICCED53389.2021.9664834.

[2] A. Ahyuna, S. Syamsuddin, H. Hasriani, A. Ardimansyah, I. Irmawati and S. Wahyuni, "The Application Of LSB Steganography For Secure Text and Hiding Confidential Information Using AES Cryptography," 2021 3rd International Conference on Cybernetics and Intelligent System (ICORIS), Makasar, Indonesia, 2021, pp. 1-5, doi: 10.1109/ICORIS52787.2021.9649497.

[3] L. Negi and L. Negi, "Hybrid approach for Data Security using Coverless Image Steganography with AES," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1077-1083, doi: 10.1109/ICCES51350.2021.9489260

[4] A. Harika, S. Anamalamudi, S. Humayra and M. K. Enduri, "Application of Steganography Imaging by AES and Random Bit," 2021 13th International Conference on Computational Intelligence and Communication Networks (CICN), Lima, Peru, 2021, pp. 177-182, doi: 10.1109/CICN51697.2021.9574676.

[5] N. P. Angel, J. A. M. Rexie and M. Mythily, "Security Key-Based Steganography for Images," 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichirappalli, India, 2023, pp. 1-7, doi: 10.1109/ICEEICT56924.2023.10157853.

[6] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Image Steganography: A Review of the Recent Advances," in IEEE Access, vol. 9, pp. 23409-23423, 2021, doi: 10.1109/ACCESS.2021.3053998.

[7] Mohanraj, V., Sakthivel, R., Paul, A., & Rho, S. (2017). “High performance GCM architecture for the security of high speed network. International Journal of Parallel Programming”. https://doi.org/10.1007/s10766-017-0545-7

[8] J. Su, N. Gu, Q. Bai and C. Lin, "Parallel Implementation of AES-GCM with High Throughput and Energy Efficiency," 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, 2018, pp. 251-256, doi: 10.1109/NANA.2018.8648719.

[9] T. Chen, W. Huo and Z. Liu, "Design and Efficient FPGA Implementation of Ghash Core for AES-GCM," 2010 International Conference on Computational Intelligence and Software Engineering, Wuhan, China, 2010, pp. 1-4, doi: 10.1109/CISE.2010.5676905.

[10] J. Butora, P. Puteaux and P. Bas, "Errorless Robust JPEG Steganography using Outputs of JPEG Coders," in IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2023.3306379.

[11] K. Vhito and V. Chouvatut, "Steganography with Adaptable Separate Encrypted Code of Hidden Confidential Information," 2023 20th International Joint Conference on Computer Science and Software Engineering (JCSSE), Phitsanulok, Thailand, 2023, pp. 523-528, doi: 10.1109/JCSSE58229.2023.10202145.

[12] S. Biswas, S. Debnath and R. K. Mohapatra, "Coverless image steganography based on DWT approximation and pixel intensity averaging," 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 1554-1561, doi: 10.1109/ICOEI56765.2023.10125935.

[13] A. O. vyas and S. V. Dudul, "Hybrid DWT- DCT image steganography for encrypted secret image," 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC), Nagercoil, India, 2019, pp. 1-7, doi: 10.1109/ICRAECC43874.2019.8995111