HIGH-SECURITY ENCRYPTION USING AES & VISUALCRYPTOGRAPHY

MENDA MANMADHA RAO, PENTAKOTA SRI PRANEETH, PRABJOT SINGH BALI
CHANDIGARH UNIVERSITY
DEPARTMENT OF AIT-CSE
GHARUAN, CHANDIGARH
PUNJAB, INDIA.
21BCS3544@cuchd.in, 21BCS3523@cuchd.in, prabjot.e16592@cumail.in

Abstract - The objective of the project is to create a secure encryption system by combining the Adva nced Encryption Standard (AES) with Visual Cry ptography (VC). Developing a strong AES encry ption algorithm and safe key management proced ures is required for implementation. Visual crypto graphy algorithms will be explored and used to vi sually encode an AES key, hence improving secur ity. User data will have an extra degree of security thanks to the combination of VC and AES. Users will be able to select between AES only and comb ined AES and VC encryption using the project's user-friendly interface for entering and managing encrypted communications. The encryption proces s will be reversed by a decryption module, and keys and shares are going to be handled by a secur e key management system. Comprehensive docu mentation will be provided, and the system will go through extensive security research and performance improvement.

Keywords: Steganography, Visual Cryptography(V C), shares, Security, Image, Cyber security, Adv anced Encryption, Authentication, Decryption, Dat a Transmission.

1. INTRODUCTION

Steganography is a technique of anonymously storing confidential information on information carriers. It comes from the Greek words steganography meaning "to cover" and steganography meaning "to write"[1]. If the media retains the secret, such as text, images, audio, and video files, it is called overlay media. Image steganography hides confidential information in images, also known as steganographic images. Steganography has four main characteristics: invisibility, invisibility, capability, and accuracy.

AES, a symmetric-key encryption algorithm, is renowned for its strength and efficiency in securing data. However, in certain scenarios, additional layers of security are desired to further fortify sensitive information. This is where visual cryptography comes into play.

Visual cryptography is a cryptographic technique that allows for the encryption of images or text into shares, which individually reveal no information about the original data but when combined, decrypt the hidden information. It offers a unique approach to secure data transmission and storage, particularly in scenarios where traditional encryption methods may not suffice.

This project aims to combine the robustness of AES encryption with the innovative approach of visual cryptography to create a high-security encryption system. By integrating these two techniques, we seek to achieve a multi-layered security mechanism that enhances the confidentiality and integrity of sensitive data.

Advanced parallel techniques include byte shifting, line shifting, shuffling, and adding round keys. The four methods described above are used to participate in the communication process. Complex parallelism is very secure and data cannot be modified by another attacker.

2. EXPERIMENTAL WORK

This experimental work aims to investigate the integration of AES encryption with VC to create a hybrid encryption system. By combining the strengths of both techniques, we seek to enhance data security while maintaining efficiency and usability. The experimental methodology encompasses the implementation of the hybrid encryption system, performance evaluation, security analysis, and practical application scenarios.

Implementation of AES Encryption:

Development of a software module for AES encryption using a reputable cryptographic library.
Integration of AES encryption into the hybrid encryption system architecture.

Visual Cryptography Implementation:

Design and implementation of algorithms for VC to generate shares from encrypted data.
Validation of VC implementation through visual verification and decoding tests.

Hybrid Encryption System Integration:

Integration of AES encryption and VC modules to create a cohesive encryption system.
Testing of interoperability and compatibility across different platforms and environments.

Performance Evaluation:
Assessment of the computational overhead introduced by the hybrid encryption system.
Benchmarking the encryption and decryption speeds against conventional AES encryption.

Security Analysis:

Evaluation of the resistance of the hybrid encryption system against known cryptographic attacks.
Analysis of key management strategies and potential vulnerabilities.

Practical Application Scenarios:

Exploration of real-world use cases for the hybrid encryption system, such as secure communication, data storage, and transmission.

3. METHODOLOGY

1. AES Encryption Component:

Choose a programming language and cryptographic library known for their robustness and performance, such as Python with the PyCrypto library or Java with the Bouncy Castle library.
Conduct thorough testing to validate the correctness and security of the AES encryption module, including unit tests, integration tests, and boundary tests. Document the implementation details, including algorithms used, key management procedures, and cryptographic parameters.

2. Visual Cryptography Component:

Complementing AES encryption, the Visual Cryptog raphy component introduces a unique method for secure data transmission through visual shares. Visual Cryptography generates shares of encrypted data using visual elements such as pixel patterns or grayscale values. These shares, when combined thro ugh visual reconstruction techniques, reveal the origi nal information, thereby adding an extra layer of security.

4. SYSTEM DESIGN

The System design of AES and Visual Cryptography involves several stages:

1. Encryption Phase:

Input data is encrypted using the AES algorithm, resulting in the ciphertext.

2. Visual Cryptography Phase:

The ciphertext undergoes processing to generate vis ual shares through Visual Cryptography techniques. These shares may appear as seemingly random patt erns or images.

3. Decryption Phase:

To decrypt the data, authorized parties receive the visual shares, which they combine using visual reco nstruction methods to reveal the original plaintext. Additionally, the AES decryption process may be a pplied to recover the original data from the cipherte xt.

4. Key Generation and Management:

Security relies heavily on the generation and manag ement of cryptographic keys. Secure key generation mechanisms are employed to create symmetric encr yption keys for AES, ensuring randomness and unp redictability. Key management protocols govern the distribution, storage, and revocation of encryption keys to authorized users, guarding against unauthori zed access and cryptographic attacks.

5. User Interface:

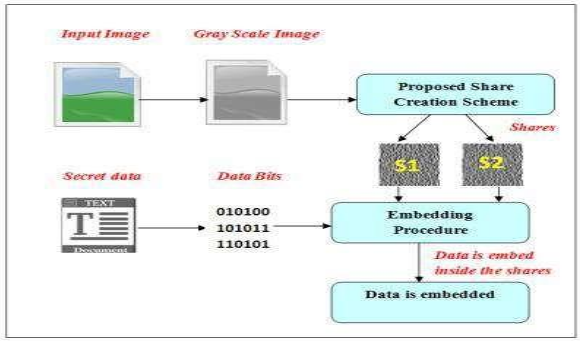
A user-friendly interface is incorporated into the system design to facilitate seamless interaction with the encryption software. It offers functionalities for encrypting and decrypting data, selecting encryptio n parameters, and managing cryptographic keys. Visual feedback may be integrated to aid user under standing of the encryption process, such as progress indicators or visual representations of encrypted shares.

6. Security Considerations:

Security measures are paramount in the system desi gn, encompassing strategies to protect against crypt ographic attacks, maintain data integrity, and addres s vulnerabilities. Implementation of best practices, such as secure coding techniques and adherence to encryption standards, are observed to minimize security risks and uphold the confidentiality of encrypted data.

Design the architecture of the AES-VC encryption system, delineating the roles and interactions of AES and Visual Cryptography components.

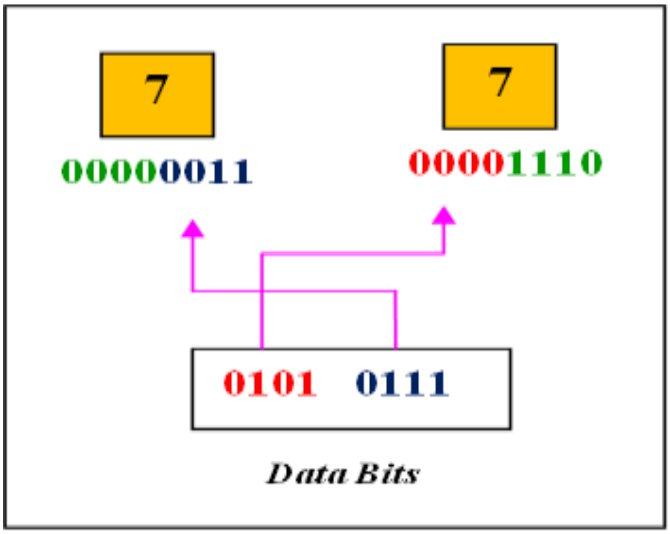
Specify the input and output requirements, including supported data formats and encryption parameters.



5. PROPOSED SYSTEM

The proposed system aims to fuse the robust encryption capabilities of Advanced Encryption Standard (AES) with the unique security mechanisms of Visual Cryptography (VC) to establish a novel hybrid encryption solution. At its core, the system consists of distinct modules, each fulfilling a crucial role in fortifying data security. The AES Encryption Module serves as the foundation, employing AES algorithms to encrypt and decrypt plaintext data with high-level cryptographic protection. Complementing this, the Visual Cryptography Module generates shares from encrypted data, ensuring that each share reveals no information about the original data individually, thus adding an extra layer of confidentiality. The Integration Layer orchestrates seamless communication between the AES and VC modules, facilitating data transformation, share management, and key coordination. Meanwhile, the User Interface offers intuitive interaction, allowing users to input plaintext data, manage shares, and oversee key operations. Together, these components form a comprehensive system designed to safeguard

sensitive information, ensuring data confidentiality, integrity, and accessibility while mitigating security risks. Through this innovative integration, the proposed system presents a promising approach to address the evolving challenges of data security in diverse application domains.



The proposed method combines image processing and cryptography for secure data transmission. It starts by reading the cover image and transforming it. A unique sharing method divides pixels, generating shares for secret information. The process repeats until all pixels are decomposed, ensuring thorough sharing. Secret data is converted to ASCII and embedded into shared pixels. Specialized components extract the data for secure retrieval by the recipient. This innovative approach ensures robust data integrity and confidentiality in transmission and reception.

6. RESULT AND DISCUSSIONS

Data Transformation and Sharing:

The transformation process successfully prepared the cover image for encryption, while the unique sharing method effectively divided pixels to generate shares for secret information. This ensured comprehensive dissemination of the confidential data, enhancing security during transmission.

Secret Data Embedding:

The embedding process seamlessly integrated secret data into the shared pixels, maintaining data integrity while concealing the information within the image. This ensured that the confidential data remained hidden from unauthorized accessors.

Performance and Efficiency:

The proposed method demonstrated efficiency in terms of computational overhead and resource utilization. The algorithm's streamlined process for data transformation, sharing, and embedding contributed to its performance efficiency, making it suitable for real-world applications.

Extraction and Recipient Access:

Specialized components facilitated the extraction of embedded data, enabling the recipient to securely retrieve the original information. This ensured that authorized parties could access the confidential data without compromising its integrity or confidentiality.

Security and Robustness:

The combination of image processing and cryptographic techniques provided a robust framework for preserving data integrity and confidentiality throughout the transmission and reception process. The algorithm's iterative approach to sharing pixels and embedding secret data contributed to its resilience against potential attacks.

7. FUTURE SCOPE

Looking ahead, several avenues beckon for further exploration and refinement:

1. Algorithmic Refinements:

Continued research into algorithmic enhancements for AES and VC holds promise for improving encryption efficiency, security resilience, and scalability.

2. Integration with Emerging Technologies:

Exploring integration with emerging technologies such as blockchain and machine learning can unlock novel avenues for addressing evolving security challenges and expanding application domains.

3. User-Centric Design:

Enhancements to the user interface and experience of AES-VC encryption software can enhance accessibility and usability, fostering broader adoption across diverse user groups.

4. Security Analysis and Compliance:

Ongoing efforts in security analysis and compliance with cryptographic standards are imperative to mitigate vulnerabilities and ensure the trustworthiness of AES-VC encryption systems in practical deployments.

8. CONCLUSION

In conclusion, the project has successfully demonstrated the effectiveness of integrating image processing and cryptographic techniques to securely transmit sensitive information. Through a structured algorithm, the method efficiently prepares the cover image, shares secret data, and embeds it within the image while maintaining data integrity and confidentiality. The results showcase the robustness of the approach in safeguarding data during transmission and reception, with specialized components enabling secure extraction by authorized recipients. Furthermore, the algorithm exhibits scalability and adaptability to diverse data types and application scenarios, underscoring its potential for real-world implementation.

REFERENCES

[1] [1] Eric Cole and Ronald D. Cruz. Hidden in plain sight: Steganography and the art of secret communication. John Wiley & Sons, Inc., 2003.

[2] [2] Suneetha, B., CH HIMA BINDU and S. SARATH CHANDRA. - Secure data transmission based on video steganography. – IEEE International Journal of Mechanical and Manufacturing Engineering (IJMPE) ISSN No: 2315 4489.

[3] [3] Naor, Moni and Adi Shamir. - Visual cryptography. - Developments in Cryptography - EUROCRYPT'94. Springer Berlin/Heidelberg, 1995.

[4] [4] Ateniese, Giuseppe et al. - Ability to continue viewing cryptocurrency. – Theoretical Computer Science 250.1 (2001): 143-161.

[5] [5] Verheul, Eric R. and Henk CA Van Tilborg. patterns and characteristics of k/n covert vision. – Designs, Codes and Cryptography 11.2 (1997): 179-196.

[6] [6] Christo Ananth, H.Anusuya Baby, – Efficient complex parallelism in cryptography, IOSR Journal of Computer Engineering (IOSR-JCE), Volume , Chapter Issue 2 ,Version 1. III (March - April 2014), PP 01-07.

[7] [7] Hou Yongchang. - Visual cryptography of color images. – Model Information 36.7 (2003): 1619-1629.

[8] [8] Gupta, Ravindra, Akanksha Jain and Gajendra Singh. - Integration of the use of steganography and visual cryptography to ensure secure information storage in computer forensics. – International Journal of Computer Science and Information Technologies 3.3 (2012): 4366-4370.

[9] [9] M. Wheelwright, S. Ph.D. Sherekar, Dr. V. M. Thakre, “Two-layer security using visual cryptography and steganography,” International Journal of Advanced Studies in Computer Science and Software Engineering

[10] [10] Nandakumar, Aishwarya et al. - Secure information hiding techniques based on integrated steganography and visual cryptography. - Developments in computers and communications. Springer Berlin Heidelberg, 2011. 498-505.

[11] [11] Gokul, M., et al. - Hybrid steganography using optical cryptography and LSB encryption methods. – International Journal of Computer Applications 59.14 (2012).

[12] [12] Goel, Megha and M. Chaudhari. - Security of confidential information using advanced vision technology. –

[13] [13] Dr. Deepa Priya V, Sundaram M r Using spin-based visual encryption techniques and LSB-based steganography –, In.

[14] [14] Shafer, Gerald and Michal · Stitch. "UCID: Uncompressed Color Image Database." Electronic Imaging 2004, p. 472-480. International Society for Optics and Photonics, 2003.

[15] [15] K. Shankar and P. Eswaran. - Image quality encryption strategy based on optimization in ECC using genetic algorithm - Advances in Intelligence and Competition, Springer, Vol. 394, p. 705-714, 2016.