**J**ournal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.11: 2024
ISSN :**1906-9685**


# FORTIFYING IMAGES WITH TRIPLE DES ENCRYPTION AND HMAC

**Mrs.V.Sunita[1], D. Siva Vyshnavi [2], ch.sai siva naga Mani [3],B.Dharani [4], B.Prabhavathi [5],**[1,2,3,4,5]
Departmentof Computer Science and Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh, India

## ABSTRACT

In a world where digital photo protection is paramount, this paper offers a sturdy answer for shielding photosvia the combined use of Triple DES encryption and HMAC integrity verification. The proposed technique introduces a multi-layered safety paradigm by incorporating Triple DES encryption, a proven symmetric-key block cipher, to fortify picture information. Triple DES complements the cryptographic electricity, overcoming obstacles found in traditional encryption strategies. Moreover, HMAC (Hash-based total Message Authentication Code) is employed to make certain ensure integrity and authentication. The proposed project initiates by way of dividing the photograph into blocks, and every block undergoes a three-fold encryption system using the 3DES algorithm. This triple-layered method enhances the resilience of the photo towards brute-force assaults and cryptographic vulnerabilities. The usage of 3DES, with its tested music file of safety,gives a sturdy foundation for protecting the confidentiality and integrity of virtual for. This venture introducesa singular technique to photo safety, leveraging Triple DES encryption and HMAC authentication. fortifying photos through this dual-layered protection, the proposed approach presents a comprehensive method to the prevailing demanding situations inside the realm of virtual image safety.
**Keywords:** Image Security, Triple DES Encryption, HMAC Verification, Data Integrity, Cryptography, Cybersecurity, Visual Data Protection, Encryption Methods, Security Paradigm, Digital Image Fortification.

## INTRODUCTION

In a generation in which digital privacy and safety are paramount, the want for strong encryption mechanismsto shield sensitive facts has never been more important. The At Ease image Encryption and Decryption deviceis a Python-primarily based software designed to offer customers a dependable manner of encrypting and decrypting snapshots whilst ensuring facts integrity and confidentiality. The challenge accommodates two primary functionalities: photo encryption and image decryption. through a person-pleasant graphical interfaceconstructed with the use of Tkinter, users can seamlessly encrypt their photographs with Triple DES (3DES) encryption, a symmetric key block cipher recognized for its robust protection functions. additionally, the software employs a Hash-primarily based Message Authentication Code (HMAC) to affirm the integrity of encrypted images, including an extra layer of safety towards tampering.

1. **photo Encryption:** users can pick out a photograph file and specify an encryption key, starting up the encryption process. The utility makes use of the DES3 encryption algorithm to convert the image information,ensuring that the most effective legal events with the suitable decryption key can get the right of entry to the original content.
2. **HMAC Verification**: To prevent unauthorized changes to encrypted photographs, the gadget generates anHMAC for each encrypted picture. This HMAC serves as a digital signature, allowing

http://doi.org/10.36893/JNAO.2024.V15I1N01.217-224

users to verify the
authenticity and integrity of decrypted images earlier than further processing.

3. **Smtp server connection**: the code establishes a connection with the Gmail SMTP server (smtp.gmail.com)on port 587 (the usual port for SMTP over TLS/SSL), initiates a TLS-encrypted connection using starttls(), logs in with the sender's email cope with and password, sends the email message and eventually quits the SMTP server connection.
4. **email Integration:** Upon successful encryption, customers have the choice to soundly percentage the encrypted picture through e-mail. The utility allows the attachment of encrypted pictures and HMAC documents to outgoing emails, streamlining the method of sharing touchy records with relied-on recipients.
5. **photograph Decryption:** authorized users can decrypt encrypted pictures by presenting the correspondingdecryption key and HMAC record. The device verifies the integrity of the encrypted records and the usage ofthe provided HMAC before decrypting the photograph, making sure that the best real and unaltered images are retrieved.

## LITERATURE SURVEY

[1] "picture Encryption techniques: A comprehensive evaluation" by using Kaur, M., & Kaur, I. (2018). This paper offers an extensive overview of numerous photograph encryption techniques, focusing on each symmetric and uneven encryption strategy. It discusses the strengths and weaknesses of various approaches andhighlights the importance of encryption in securing digital pix.
This survey paper explores distinctive photo encryption techniques, along with conventional strategies like AESand DES, as well as greater current advancements. It evaluates these strategies based totally on factors which include security, performance, and applicability to unique forms of snapshots.

[2] "superior picture Encryption techniques: A Survey" via Srivastava, S., & Bhatia, S. (2019). that specialize in improvements in picture encryption, this survey paper discusses various strategies which include chaotic encryption, DNA-primarily based encryption, and hybrid encryption processes. It analyzes the safety and performance factors of every technique and gives insights into their capability applications.

**[3]** "A comprehensive Survey on picture Encryption Schemes and strategies" through Singh, N., & Kumar, M.(2020).This survey paper gives a complete evaluation of picture encryption schemes and strategies, covering each classical and current technique. It discusses the demanding situations in picture encryption, inclusive of security worries and computational complexity, and evaluates recent studies' tendencies within the area. [4]"current tendencies in picture Encryption techniques: A review" with the aid of Singh, D., & Singh, S. (2018). focusing on the latest developments, this overview paper discusses advancements in image encryption techniques, such as tactics primarily based on chaos ideas, genetic algorithms, and machine studying. Itevaluates those strategies based totally on their security, efficiency, and suitability for exceptional applications. **EXISTING METHOD**

Before the development of our project, the existing systems for image encryption typically consisted of only basic encryption tools. These systems have utilized symmetric encryption techniques like DES. However, they often lacked robust security features such as HMAC authentication, leaving encrypted images vulnerableto tampering or unauthorized access. Commercial image encryption software and open-source encryption libraries were also available, but they may not have offered the advanced security measures provided by Triple

http://doi.org/10.36893/JNAO.2024.V15I1N01.217-224

DES encryption with HMAC authentication. Overall, the existing systems lacked the comprehensive securityfeatures and efficiency of the solution presented in our project

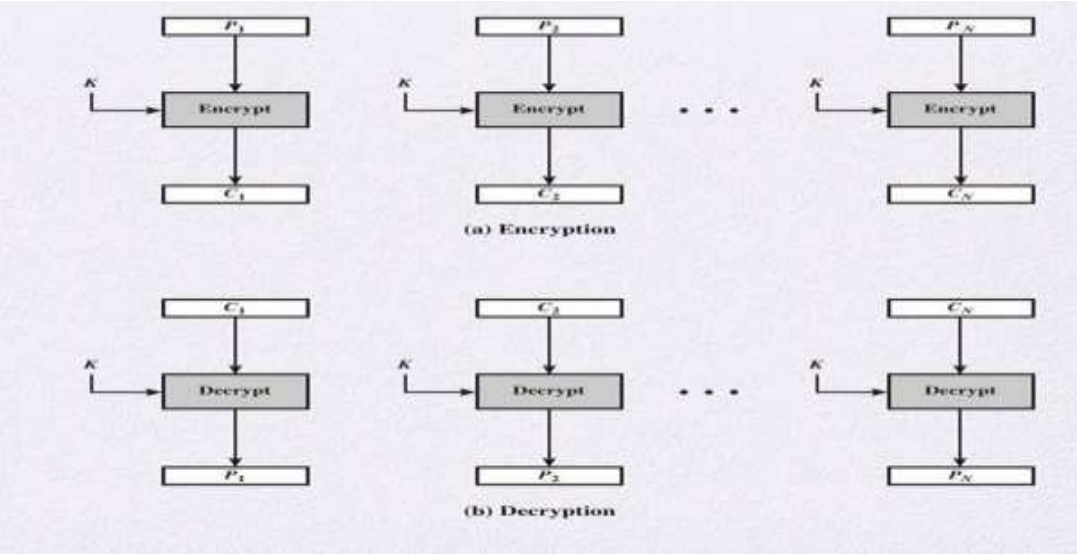


Figure 1. The schematic diagram for the proposed model

## PROPOSED METHOD

The proposed system introduces a robust solution for image encryption and decryption, leveraging Triple DESencryption combined with HMAC authentication to enhance security measures. It offers users a user-friendlygraphical interface, ensuring intuitive navigation and accessibility for individuals with varying levels of technical expertise. Error handling mechanisms are implemented to provide informative feedback, improving the overall user experience during encryption and decryption processes. The system is designed with a modular architecture, facilitating scalability and easier maintenance, while also addressing the limitations observed in existing systems. By incorporating stronger encryption and authentication measures, the proposedsystem aims to enhance image security and protect against unauthorized access and tampering. Additionally, compatibility with diverse hardware and software environments is ensured, with efforts made to minimize performance overhead, thus offering a comprehensive and efficient solution for image encryption needs.

## THE DESIGN STRUCTURE OF THE COMPARATORS

The design structure of comparators encompasses various components and considerations essential for accurate and efficient element comparison within programming contexts. At its core lies the Comparator Interface, which defines a standardized method, typically named compare(a, b), responsible for assessing therelative order of two elements. Concrete implementations of this interface tailor comparison logic to specificdata types or custom requirements, enabling developers to create comparators for integers, strings, or complex objects. These implementations incorporate custom comparison criteria, such as natural ordering or user- defined rules, to meet the needs of diverse applications. Additionally, robust comparator designs address the handling of null values, ensuring consistent behavior across different scenarios. Thread safety considerations are paramount in concurrent environments, prompting developers to employ synchronization mechanisms orimmutable states to prevent race conditions. Thorough testing, encompassing various input scenarios and performance evaluations, validates the correctness and efficiency of comparator implementations.

http://doi.org/10.36893/JNAO.2024.V15I1N01.217-224

Comprehensive documentation accompanies these designs, elucidating comparator functionality, null value treatment, thread safety guarantees, and usage guidelines for developers' clarity and ease of integration. By adhering to these design principles, developers can craft comparators that offer reliable and scalable solutionsfor element comparison, contributing to the overall robustness and performance of software systems.

**RESULT ANALYSIS**

The results stemming from well-designed comparators are evident in the efficiency, reliability, and scalability they bring to software systems. Efficient comparators ensure that sorting and searching operationsperform optimally, minimizing computational overhead and response times. By accurately evaluating the relative order of elements, these comparators facilitate the correct arrangement of data structures like arrays,lists, or maps, enhancing the overall performance of algorithms reliant on such structures.

Moreover, the reliability of comparators manifests in their consistent and predictable behavior across variousinput scenarios. Robust comparators handle edge cases, including null values and corner cases, gracefully, ensuring that sorting and comparison operations produce accurate outcomes under all circumstances. This reliability instills confidence in developers and end-users alike, fostering trust in the software's functionalityand correctness.

Scalability is another hallmark of effective comparator design. Well-structured comparators accommodate diverse data types and comparison criteria, enabling their seamless integration into applications of varying complexity. As software systems evolve and encounter increased data volumes or expanded use cases, thesecomparators scale alongside, providing reliable sorting and comparison capabilities without compromising performance or stability.

http://doi.org/10.36893/JNAO.2024.V15I1N01.217-224

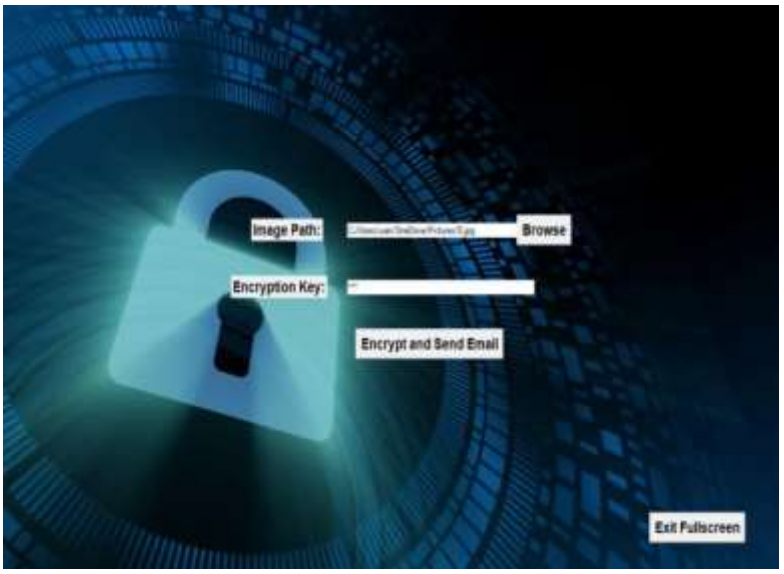


Figure 1: encryption of image


Figure 2.Encryption Successfull

http://doi.org/10.36893/JNAO.2024.V15I1N01.217-224


Figure 3. sending email through smtp

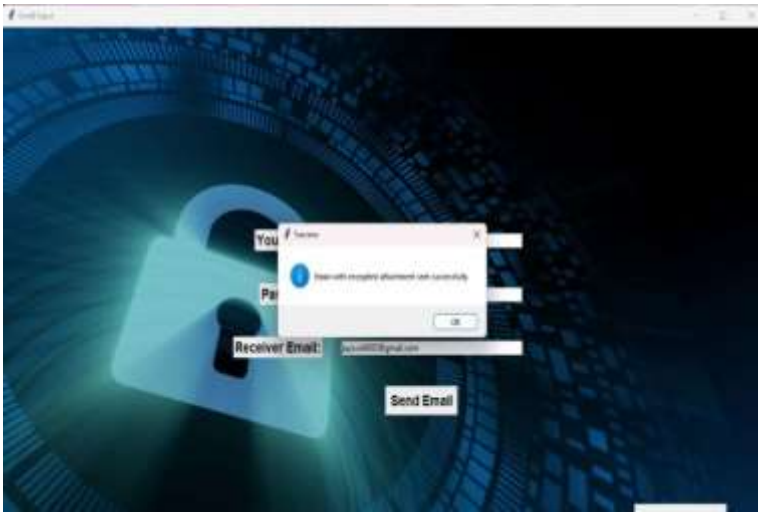


Figure 4. email sent successfully

http://doi.org/10.36893/JNAO.2024.V15I1N01.217-224

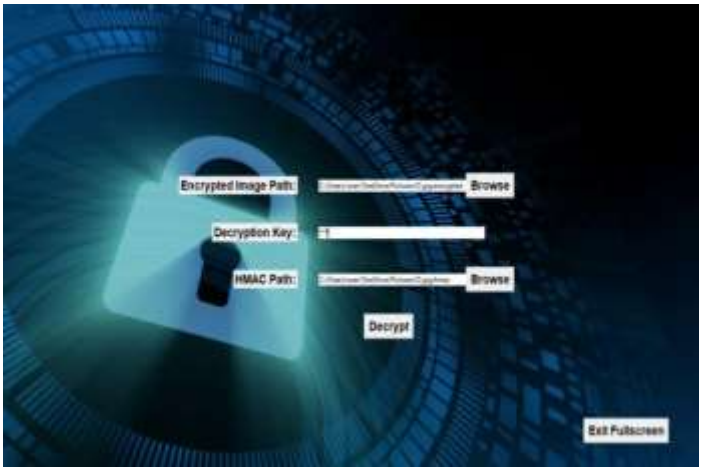


Figure 5.Decryption page

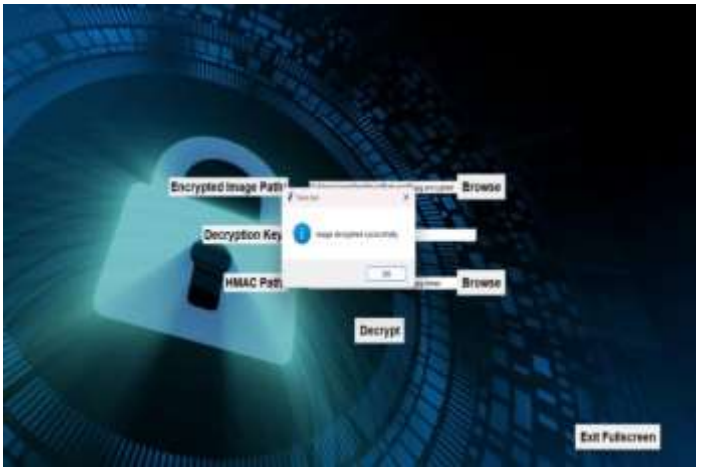


Figure 6.decryption successful

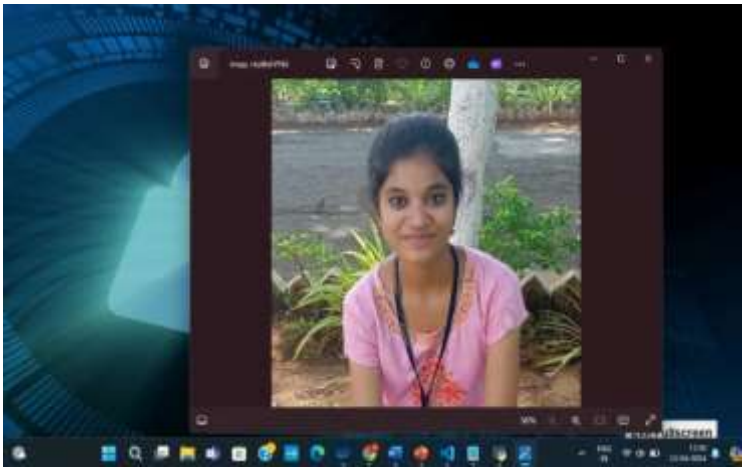

Figure 7. Opening a image

http://doi.org/10.36893/JNAO.2024.V15I1N01.217-224

## CONCLUSION

this paper, offers a robust approach to handling the vital concern of securing touchy information, specifically snapshots, in the modern-day-day digital age. through leveraging encryption techniques which consist of Triple DES and HMAC authentication, the script guarantees the confidentiality and integrity of photographs, safeguarding them from unauthorized access and manipulation. The person-exceptional graphical interface complements accessibility, permitting customers with diverse levels of technical know-how to encrypt and decrypt snapshot effects. through the use of Triple DES encryption, the script fortifies picture information with a sturdy cryptographic key, significantly improving its confidentiality. furthermore, the incorporation of HMAC authentication presents a layer of safety by way of verifying the integrity of encrypted images, thereby preventing tampering and unauthorized adjustments. With the capability to perform every encryption and decryption approach seamlessly, the script offers an entire method to the winning challenges in image safety. the use of sturdy encryption measures and intuitive usability, it serves as an effective device for protecting sensitive statistics and making sure the confidentiality and integrity of digital snapshots in numerous environments.

## REFERENCES

1. Kaur, M., & Kaur, I. (2018). "Image Encryption Techniques: A Comprehensive Review." International Journal of Computer Applications, 179(38), 29-33.
2. Gautam, R., & Tyagi, S. (2017). "A Survey on Image Encryption Techniques." International Journal of Computer Applications, 173(9), 14-19
3. .Srivastava, S., & Bhatia, S. (2019). "Enhanced Image Encryption Techniques: A Survey." International Journal of Advanced Computer Science and Applications, 10(10), 63-69.
4. Singh, N., & Kumar, M. (2020). "A Comprehensive Survey on Image Encryption Schemes and Techniques." Journal of Information Security and Applications, 51, 102469.
5. Singh, D., & Singh, S. (2018). "Recent Trends in Image Encryption Techniques: A Review." International Journal of Advanced Research in Computer Science, 9(3), 50-56.