A Review on Image-text Encryption Decryption

Abhishek Dhokale, Dhairyasheel Jadhav, Maharudra Gapat, Swarada Badekar,

Prof. Mr. S.P. Gunjal

[1,2,3,4]Students, [5]Professor, Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Kusgaon(BK), Lonavala, Pune, India.

[1]abhishekdhokale.sknsits.comp@gmail.com, [2]dhairyasheeljadhav.sknsits.comp@gmail.com,

[3]maharudragapat.sknsits.comp@gmail.com, [4]swaradabadekar.sknsits.comp@gmail.com,

[5]cplachake.sknsits@sinhgad.edu

Abstract - In the digital age, secure communication and data protection are paramount. Image-text encryption and decryption, a fusion of cryptography and steganography, provides an innovative solution to safeguard sensitive information. This technique involves encrypting textual data using advanced cryptographic algorithms and embedding it within images using steganographic methods. This paper delves into the principles, methodologies, and applications of image-text encryption and decryption. This paper provides a comprehensive overview of the methodologies and considerations involved, underscoring the significance of this technique in contemporary digital security paradigms.

Keywords – Feature Extraction, AES, Classification, Model-training

I. INTRODUCTION

Image-text encryption and decryption are techniques used to secure both textual and visual information in digital communication and storage. These methods involve encoding text or images in such a way that unauthorized users cannot access or understand the content without the proper decryption key or algorithm.

Image encryption is the process of transforming the pixel data of an image into a scrambled or encrypted form to protect its confidentiality and integrity.

Methods of Image encryption:

Symmetric Key Encryption : This approach uses a single secret key for both encryption and decryption. Common symmetric encryption algorithms like Advanced Encryption Standard (AES) can be applied to image data.

Asymmetric Key Encryption : In this method, a pair of keys, a public key and a private key, is used. The public key is used for encryption, while the private key is used for decryption. RSA and Elliptic Curve Cryptography (ECC) are examples of asymmetric encryption applied to images.

Substitution Ciphers : Substitution ciphers replace each character in the plaintext with another character according to a predefined rule. Example : Caesar cipher and Vigenère cipher.

Transposition Ciphers: Transposition ciphers rearrange the characters of the plaintext without changing them. An example is the Rail Fence cipher.

AES Algorithm :The AES algorithm (also known as the Rijndael algorithm) is a symmetrical block cipher algorithm that takes plain text in blocks of 128 bits and converts them to ciphertext using keys of 256 bits. Since the AES algorithm is considered secure, it is in the worldwide standard.The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware to encrypt sensitive data. It is essential for government computer security.

MD5 Algorithm :The MD5 message-digest algorithm is a cryptographically broken but still widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function.

The increasing need for privacy, security, and data integrity in various applications and sectors. Implementing robust encryption methods ensures that sensitive information remains confidential, secure, and trustworthy in the digital realm.

To protect sensitive information by converting images and text in to unreadable formats that can only be deciphered by authorized users with the appropriate decryption key.

To safeguard the privacy of individuals and organizations by ensuring that their personal and confidential data remains inaccessible to unauthorized parties.

To ensure that the content of images and text remains

 DOI : 10.35291/2454-9150.2024.0202

unchanged during transmission or storage. Detect and prevent unauthorized modifications or tampering.

II. ACKNOWLEDGMENTS

I would like to thank Prof. S.P.Gunjal for helping me out in selecting the topic and contents, giving valuable suggestions in preparation of Seminar report and presentation **'IMAGE – TEXT ENCRYPTION DECRYPTION.'**

I am grateful to Dr. S. M. Patil, for providing healthy environment and facilities in the department. He allowed us to raise our concern and worked to solve it by extending his co-operation time to time..

Goal makes us to do work. Vision is more important than goal which makes us to do work in the best way to make work equally the best. Thanks to Principal, Dr.M.S Rohokale for his support and vision.

Consistent achievement requires boost on consistent interval basis. Management has given full support and boosted us to be consistent and achieve the target. Thanks to management for their support.

Thanks to all the colleagues for their extended support and valuable guidance. I would like to be grateful to all my friends for their consistent support, help and guidance.

III. LITERATURE SURVEY

1. **Ghebleh M, et.al (2014):**

-Title: "An image encryption scheme based on chaotic maps."

- Description: This work presents an image encryption scheme that utilizes irregularly decimated chaotic maps as a key component for securing digital images.

2. **Sivakumar T, et.al (2015):**

- Title: "A novel image encryption using calligraphy based scan method and random number."

-Description: This paper introduces a novel image encryption method that combines calligraphy-based scanning techniques and random number generation for enhanced security.

3. **Forouzan BA, et.al (2011):**

- Title: "Cryptography and network security (Sie)."

- Description: This work is likely a textbook or academic publication on the subject of cryptography and network security.

4. **Li XW, et.al (2013):**

- Title: "Optical 3D watermark based digital image watermarking for telemedicine."

- Description: This paper presents a digital image watermarking method that uses optical 3D watermarks specifically designed for applications in telemedicine.

5. **Bi N, et.al (2007):**

- Title: "Robust image watermarking based on multiband wavelets and empirical mode decomposition."

- Description: This research focuses on robustly watermarking digital images using techniques based on multiband wavelets and empirical mode decomposition.

IV. PROPOSED SYSTEM

In the recommended system, we employ the AES method for encryption and decryption, as well as data protection and secure access control. The MD 5 technique should be used to prevent duplication of data.

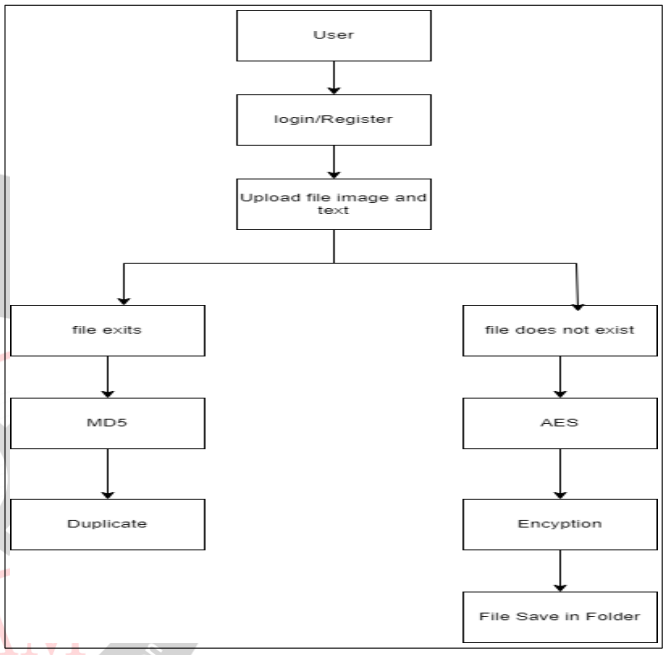


Figure 1 :System Architecture

WATERFALL MODEL DIGRAM :-

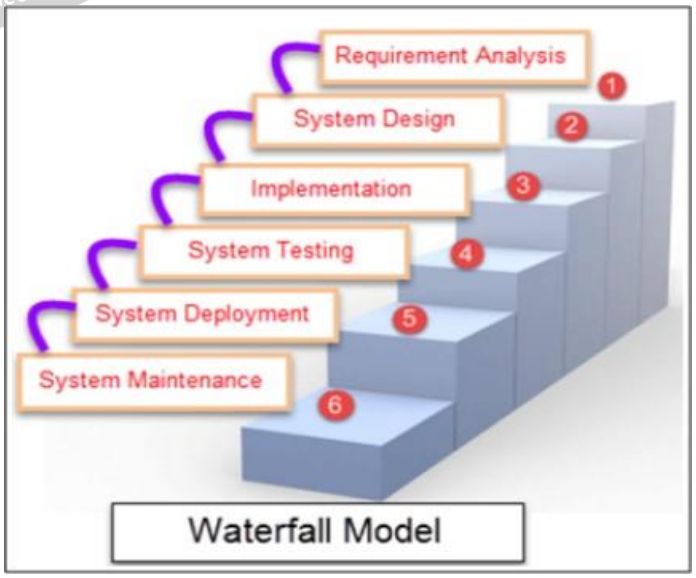


Figure 2 :Waterfall Model Diagram

 DOI : 10.35291/2454-9150.2024.0202

V. ALGORITHM

AES :

AES is asymmetric encryption algorithm that is widely used to secure sensitive data. It is a block cipher, meaning it processes data in fixed-size blocks. AES operates on blocks of 128 bits and supports key sizes of 128, 192, or 256 bits. The same key is used for both encryption and decryption algorithm.

MD5 :

MD5 initializes four 32-bit variables, often referred to as A, B, C, and D, with spe- cific constant values. The input data is processed in blocks of 512 bits (64 bytes). If necessary, the input data is padded to fit the last block.

VI. WORKING MODULES

Python:

Python is an interpreted, high-level and general-purpose programming language. Python's design philosophy emphasizes code. Its language constructs and object-oriented approach aim to help programmers. Python is dynamically-typed and garbage-collected. It supports multiple programming paradigms, including structured, object-oriented and functional programming. Python is often described as a "batteries included" language due to its comprehensive standard library.

Spyder:

Spyder is an open-source cross-platform for scientific programming in the Python language. Spyder integrates with a number of prominent packages in the scientific Python stack, including NumPy, SciPy, Matplotlib, pandas. It is released under the MIT license. Spyder is extensible with first-party and third-party plugins,includes support for interactive tools for data inspection. Python-specific code quality assurance such as Pyflakes, Pylint and Rope.

FUTURE SCOPE

The future of image text encryption and decryption is likely to see a convergence of these advancements, leading to more secure, versatile, and tamper-proof methods for hiding and transmitting sensitive information within digital images. his advanced technique allows computations on encrypted data without decryption, enabling secure analysis of hidden text. Hiding the text data within seemingly random parts of the image itself.

System Design: In this system design phase we design the system which is easilyunderstood for end user i.e. user friendly. We design some UML diagrams and data flow diagram to understand the system flow and sequence of execution.

Implementation: In implementation phase of our project we have implemented various module required of successfully getting expected outcome at the different module levels. With inputs from system design, the system is developed in small programs called units, which are integrated in the next 10 phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.

Testing: The different test cases are performed to test whether the project module are giving expected outcome in assumed time. All the units developed in the implementation phase are integrated into a system. the entire system is tested for any faults and failures.

Deployment of System: Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market.

Maintenance: There are issues which come in the client environment. To fix those issues patches are released. Maintenance is done to deliver these changes in the environment. All these phases are cascaded to each other.

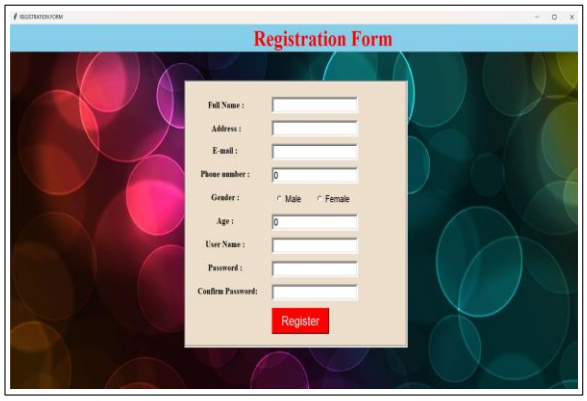
RESULT

The image which has to be encrypted is chosen from the folder and the encrypt button is clicked. The original input image taken in the form of .GIF file as shown in fig 3. Once the image is encrypted successfully then the message is displayed fig 4. and when the image is viewed. For decryption of the image which has been encrypted then the encrypted image has to be select and then decrypted button is clicked, then the successful decryption. When the image is viewed then it shows the original image shown in fig 5.

Login Page

Figure 3 :Login Page

 DOI : 10.35291/2454-9150.2024.0202



Registration Page

Figure 4: Registration Page

GUI Main

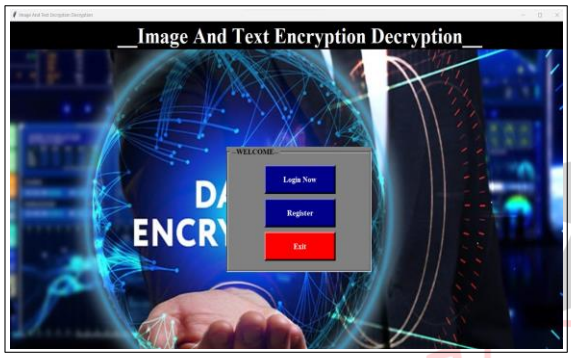


Figure 5 :GUI Main

CONCLUSION

In this paper we discussed that to avoid the duplication using the Encryption And decryption method. And for the text uploading we are using three algorithm., For the uploading in the cloud system we are using the Structural Similarity AES Algorithm and the main purpose of the similarity index is to check the image quality such as luminance, contrast and structure, then it measures the similarity of two image. To store large amount of data with efficiency, to avoid the duplicate text and image we are using the encryption method . The journey toward securing image-text data is ongoing and dynamic. By addressing the challenges identified in this study and fostering collaborative efforts among researchers, industry professionals, and policymakers, we can develop encryption and decryption solutions that not only meet the demands of today but also anticipate and prepare for the challenges of tomorrow. The ultimate goal is to create a digital environment where individuals and organizations can communicate and share information freely, securely, and with confidence in the privacy and integrity of their data.

VII. REFERENCES

[1] Ghebleh M, Kanso A, Noura H (2014) An image encryption scheme based on irregularly decimated chaotic maps. Signal Process Image Commun 29(5):618–627

[2] Sivakumar T, Venkatesan R (2015) A novel image encryption using calligraphy based scan method and random number. KSII Trans Internet Inf Syst 9(6):2317–2337.

[3] Forouzan BA, Mukhopadhyay D (2011) Cryptography and network security (Sie). McGraw-Hill Education, New York.

[4] Bi N, Sun Q, Huang D, Yang Z, Huang J (2007) Robust image watermarking based on multiband wavelets and empirical mode decomposition. IEEE Trans Image Process 16(8):1956–1966.

[5] Li XW, Kim ST (2013) Optical 3D watermark based digital image watermarking for telemedicine. Opt Lasers Eng 51(12):1310–1320

[6] Belazi A, El-Latif AAA, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170

[7] Chai X, Chen Y, Broyde L (2017) A novel chaos-based image encryption algorithm using DNA sequence operations. Opt Lasers Eng 88:197–213.

[8] Zhao G, Chen G, Fang J, Xu G (2011) Block cipher design: generalized single-use-algorithm based on chaos. Tsinghua Sci Technol 16(2):194–206.

[9] El-Samie FEA, Ahmed HEH, Elashry IF, Shahieen MH, Faragallah OS, El-Rabaie E-SM, Alshebeili SA (2013) Image encryption: a communication perspective. CRC Press, Boca Raton

 DOI : 10.35291/2454-9150.2024.0202