IMAGE ENCRYPTION AND DECRYPTION USING AES

Prof. Vijay Mane, Shantanu Pawar, Nagesh Pujari, Ruturaj Patil

Department of Electronics & Telecommunication
Vishwakarma Institute of Technology, Pune, 411037, Maharashtra, India

Abstract — **An "Image Encryption and Decryption" project aims to enhance the security of digital images by applying cryptographic techniques. It involves encrypting the image using algorithms like AES , converting it to unreadable text format which is impossible to open without the proper decryption key. This protects sensitive visual data from unauthorized access or tampering. Decryption, when required, restores the image to its original form. The decrypted image is not tampered or altered. This project contributes to data security, privacy, and confidentiality, making it ideal for applications like secure image transmission and storage in various domains, including healthcare, military, and multimedia communications.**

Keywords — **Cryptography, AES, Digital Security, Encryption.**

I. INTRODUCTION

This project is a user-friendly program that improves the security of digital photos, using cryptographic techniques. The project has a graphical user interface, which allows users to choose image files, encrypt them, and then decrypt them as needed. They can choose their own encryption key according to their choices. Advanced Encryption Standard (AES) technique is used to encrypt the images. With the goal of protecting the integrity and confidentiality of sensitive visual data, it is appropriate for use in a variety of fields where data security and privacy are essential, including multimedia communications, the military, and the healthcare industry. Users can choose picture files for encryption and decryption with ease because of this application's attractive and user-friendly interface. It creates distinct encryption keys for every operation and secures specific photos using the powerful AES encryption technique. It will provide an important feature which can be further implemented while sharing media over social media accounts.

Once they have the decryption key, users may easily decrypt previously encrypted photos.
In order to preserve the original image and grant authorized users safe access, the project also oversees the storage of encrypted and decrypted files. To further improve the user experience, the design elements have also been added, including unique typefaces, button styling, and a background image. All things considered, this project is a useful tool for protecting image data in applications where data security and privacy are important. It gives users the ability to protect their visual material from various malicious sources. In case a visual data gets in the hand of the wrong person it may cause problems.

II. METHODOLOGY/EXPERIMENTAL

The "Image Encryption and Decryption" project is being developed using a process that includes multiple important stages. Project planning is the first step in the process, during which the requirements, goals, and scope are established. Identifying the correct requirements is also while working on the project.

AES Algorithm Working
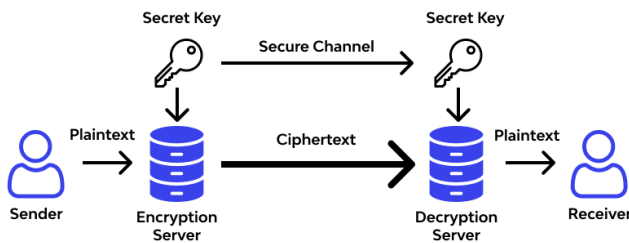
Fig 1.1

Fig 1.1 explains the working of the AES encryption method. It gives the glimpse of how an image will get encrypted and decrypted as per the user. AES is a widely used symmetric encryption algorithm. It operates on fixed-size blocks of data and employs a secret key for both encryption and decryption. AES is highly secure, with key lengths of 128, 192, or 256 bits, making it suitable for protecting sensitive data in various applications, including digital communication and file encryption.

The application's structure, which includes the primary frame and layout, is planned, and custom UI elements, such as buttons and labels, are designed. The selection and placement of components are chosen to guarantee a user-friendly interface. The user can also customize the interface according to his choice if intended to. But for that some internal changes in the code are required.

The main encryption and decryption logic is put into practice, along with techniques for working with AES-encrypted image files. In order to handle data securely, it is essential to generate and manage encryption keys. Additionally, file actions like reading, writing, and deleting must be properly controlled to avoid data loss.The project heavily relies on user input, and button-associated functions including file selection, encryption, and decryption are implemented. The process is made accessible and user-friendly by helpful labels and messages that lead consumers through it.

III. RESULTS AND DISCUSSIONS

The project gives the desired result to that user. It successfully encrypted and decrypted the image whenever the command was given to it. It efficiently encrypts and decrypts picture files using the AES algorithm, guaranteeing the security and privacy of critical visual data. Within the application, users can pick photographs to encrypt (making them unreadable without the decryption key) and then decrypt (using the supplied key). This encryption feature contributes to data privacy and security through a variety of wide-ranging uses, including safeguarding medical records and sensitive visual data in military settings.Another standout feature is the user interface design, which provides a fun and intuitive experience. Selecting picture files, entering encryption keys, and starting the encryption and decryption operations are all done with ease by users.


Fig 1.2

Fig 1.2 shows the user interface on which the user can choose the encryption key according to his choice. To further improve reliability and usability, the project includes strong error-handling systems that handle exceptions and any problems during file operations and cryptographic processes. This feature lowers the chance of data loss or corruption, which is especially important when working with sensitive data.

IV. CONCLUSION

This project has efficiently used and integrated the power of the AES encryption technology, allowing users to safely safeguard their private image data. The project gives users the ability to easily encrypt and decode photos, giving them the means to protect their important data. The user can now

freely share their digital images through platforms if they have used this encryption feature. It provides a tool to be intertwined with multiple social media accounts which have a daily vast amount of digital media transactions. The application's smart design elements and user-friendly interface enable a broad spectrum of users to utilize it, regardless of their level of technical expertise. This accessibility adds to a dependable and seamless user experience, together with the project's strong error-handling features.
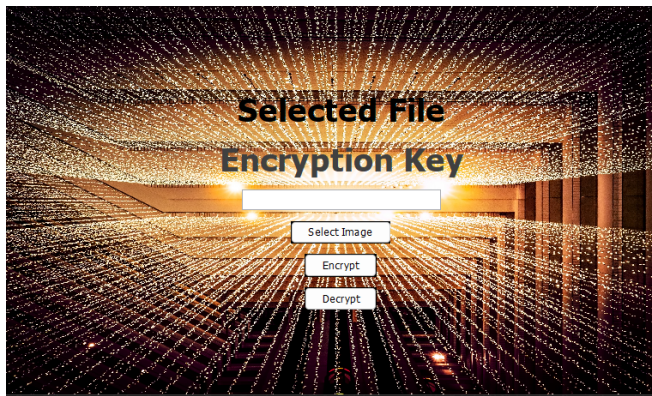
Fig 1.3

Fig 1.3 shows the user interface from which the user can select the operation which he wants to perform. This project offers a flexible and useful solution with applications in the healthcare, military, and multimedia communications areas, among other fields. It ensures the privacy and security of digital images in a world where data protection is of paramount importance. The successful implementation of this project underscores its potential to enhance data security and confidentiality, making it a significant contribution to the field of image encryption and decryption.

V . Acknowledgment

VI. References

[1] Yu, Gan, Yongjun Shen, Guidong Zhang, and Yanhua Yang. "A chaos-based color image encryption algorithm." In 2013 Sixth international symposium on computational intelligence and design, vol. 2, pp. 92-95. IEEE, 2013.

[2] Gao, Tiegang, and Zengqiang Chen. "A new image encryption algorithm based on hyper-chaos." Physics letters A 372, no. 4 (2008): 394-400.

[3] Rasras, Rashad J., Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, and Qazem Jaber. "Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation." International Journal of Computer Science and Mobile Computing 8, no. 3 (2019): 14-26.

[4] Wan, Nan, and Yi Zhang. "Digital image encryption and decryption algorithm based on optimization and fusion strategy." In 2020 13th International Symposium on Computational Intelligence and Design (ISCID), pp. 244-248. IEEE, 2020.

[5] Li, Xiaofeng, and Yinhui Zhang. "Digital image encryption and decryption algorithm based on wavelet transform and chaos system." In 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), pp. 253-257. IEEE, 2016.

[6] Yousif, Bedir, Fahmi Khalifa, Ahmed Makram, and Ali Takieldeen. "A novel image encryption/decryption scheme based on integrating multiple chaotic maps." AIP Advances 10, no. 7 (2020).

[7] El Sawda, Rami, Ayman Al Falou, Gilles Keryer, and Ammar Assoum. "Image encryption and decryption by means of an optical phase mask." In 2006 2nd International Conference on Information & Communication

Technologies, vol. 1, pp. 1474-1477. IEEE, 2006.

[8] Farajallah, Mousa, Zeinab Fawaz, Safwan El Assad, and Olivier Deforges. "Efficient image encryption and authentication scheme based on chaotic sequences." The 7th International Conference on Emerging Security Information, Systems and Technologies, 2013.

[9] Chowdhary, Chiranji Lal, Pushpam Virenbhai Patel, Krupal Jaysukhbhai Kathrotia, Muhammad Attique, Kumaresan Perumal, and Muhammad Fazal Ijaz. "Analytical study of hybrid techniques for image encryption and decryption." Sensors 20, no. 18 (2020): 5162.

[10] Joshi, Madhusudan, and Kehar Singh. "Color image encryption and decryption using fractional Fourier transform." Optics communications 279, no. 1 (2007): 35-42.

[11] Younes, Mohammad Ali Bani. "A SURVEY OF THE MOST CURRENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES." International Journal of Advanced Research in Computer Science 10, no. 1 (2019)..

[12] Zhang, Yong, and Yingjun Tang. "A plaintext-related image encryption algorithm based on chaos." Multimedia Tools and Applications 77, no. 6 (2018): 6647-6669.

[13] Bigdeli, Nooshin, Yousef Farid, and Karim Afshar. "A novel image encryption/decryption scheme based on chaotic neural networks." Engineering Applications of Artificial Intelligence 25, no. 4 (2012): 753-765.

[14] Samhita, Poluri, Prateek Prasad, K. Abhimanyu Kumar Patro, and Bibhudendra Acharya. "A secure chaos-based image encryption and decryption using crossover and mutation operator." Int J Control Theory Appl 9, no. 34 (2016): 17-28.

[15] Singh, Amandeep, Praveen Agarwal, and Mehar Chand. "Image encryption and analysis using dynamic AES." In 2019 5th international conference on optimization and applications (ICOA), pp. 1-6. IEEE, 2019.