Compressed Image Encryption for Secure Internet Transfer

Chaitanya Upadhyay[1], Stuti Vats [2]

[1] *Computer Science and Engineering SRM Institute of Science and Technology, Ghaziabad, India*

[2] *Computer Science and Engineering SRM Institute of Science and Technology, Ghaziabad, India*

***Abstract*—To protect personal data from unwanted parties, encryption is a commonly used cryptographic technology that transforms any readable information into an unreadable form, often known as encrypted form. As a result, both our system and the data are more secure. A finite number of instructions, known as algorithms, and a set of characters for encryption, known as keys, are used to implement this system. This project combines encryption of compressed images using AES and RSA algorithms and image compression method that are present on the device. Image compression is required to send large size images easily through this process without losing the actual picture quality of the image. The fundamental goal is to protect the image's privacy, confidentiality, and integrity of the data being sent across the channel from the sender's side to the receiver's side. This research paper aims to specify the process of compressing the image and implementing encryption and decryption on the compressed image, which can be transferred via different secure channel through internet.**

***Index Terms*—: AES, Decryption, Encryption, Image Compression, Random Matrix, Key Security**

I. INTRODUCTION

To guarantee the security of data and information in a company's networks and resources, system security protocols are required. Data security is crucial for protecting the organizational asset as a result. If the businesses are unable to accomplish this, it could result in a significant loss of information, including a decline in sales, a deviation from the anticipated outcomes, a lack of monitoring judgements, etc. Security of data and information is crucial, particularly when sharing with other users. Data security is the process of ensuring that our data is safe and protected from unauthorized users.

Encryption is a fairly popular method for achieving the same result. By utilizing the appropriate collection of encryption keys and algorithms, encryption techniques are utilized to transform the readable form of data into an unreadable form. The data is encoded and decoded using the key. Data is highly secure since only authorized people have access to this key.

Based on their cryptographic algorithms, data encryption techniques can be divided into two categories: substitution and transposition. In the substitution technique, the data is changed to another symbol in accordance with the algorithm whereas in the transposition method, the data's positions are switched about or mixed up in accordance with a certain algorithm. An updated algorithm was previously presented. The image was broken into roughly 8x8-inch-sized tiny blocks using that technique. A random 2D image map was created by processing and shuffling the blocks after that. In order to prevent unwanted users from quickly decrypting data and maintain confidentiality, this technique makes decryption more difficult and safer.

In order to safeguard the security of an image, image encryption involves converting it into another challenging image that is tough to identify. The image must be decrypted using a decryption key in order to be viewed as the actual image. There are a number of ways that can be applied to convert the images, but more are being developed in order to find the optimal encryption method. As a result, in order to accomplish this strategy, we frequently use a number of crucial algorithms that significantly aid in producing a secure and desired result. The two algorithms implemented in this project are RSA and AES.

Image compression is a technique through which we can change the size of an image into a compressed form of it with lower properties.

The encryption of large images was not an easy task because it took ample of time on transfer and the whole process of encryption slows down because of the large picture property of the image.

So, the large images are first compressed and then the encryption using these two algorithms was performed in this project due to which we were able to send a high-quality picture through the process of encryption via different channel of transfer.

Compression of image without losing its original picture quality is being implemented in this project and then encryption of that compressed image is being performed.

In order to prevent unauthorized people from accessing the photographs and to boost security, numerous studies are being conducted to reach the highest level of security.

II. LITERATURE SURVEY

Delavar Zareai et al. (2023) [1]: In association with the EGPIECLMAC system, this study proposes a new chaotic-based two-step encryption architecture for safe and efficient privacy image encryption. Arnold's Cat mapping and chaotic logistics are both used in the technique. The quality and superiority of the proposed algorithm are confirmed by standard evaluations of the encrypted and decoded privacy image with the EGPIECLMAC system and their comparison with related algorithms.

Nirmal Chaudhary et al. (2022) [2]: This article used various approaches including an advanced encryption standard (AES), block cypher encryption, an Arnold cat map, a hybrid chaotic map for encryption.

V Goutham Bharadwaja et al. (2021) [3]: The AES algorithm and the chaos sequence are combined to create a novel image encryption algorithm that is proposed in this research. AES will be used in the project to encrypt and decrypt the image transfer because it can solve issues that other algorithms are unable to. This uses the AES algorithm and the chaotic sequence to encrypt and decrypt images. Java coding is used for an effective implementation of the encryption and decryption process.

Prof. Ziad AlQadi (2020) [4]: this paper involves an approach of employing RGB color picture encryption-decryption on a three-dimensional matrix (DM) image. This technique provides a greater level of security and precision.

Priya Deshmukh (2016) [6]: The text and image in this article are encrypted using the AES technique to ensure their secure transport. It explains why utilising the AES algorithm has advantages over the DES algorithm. AES is comparatively faster than DES and employs 128-bit block sizes.

Mohamad M Al-Laham (2015) [7]: In this research, matrix multiplication is used to encrypt and decrypt images utilizing RGB color images. With matrix multiplication, the precise encryption matrix is created, which is then encrypted using the necessary key and afterwards decrypted at the receiver send.

Ashutosh Shukla et al. (2013) [8]: The Elliptical Curve Cryptography, a novel technique, is used in this research to encrypt images. Public key cryptography based on the algebraic structure of elliptic curves over finite fields is used in this method.

A. Subramanya (2001) [9]: An overview of the main picture compression methods is provided in this article. Most coding methods have fairly simple decoding processes that are often the opposite of the encoding steps.

III. METHODOLOGY

In this project we are using Python coding language for basic compression, encryption and decryption processes of the image that is sent over a secured medium of internet channel.

Firstly, the user has to Compress the image which appears to be large in size or will take a couple of minutes to send via internet channel selected from a folder or captured through webcam.

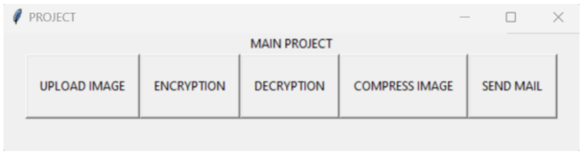
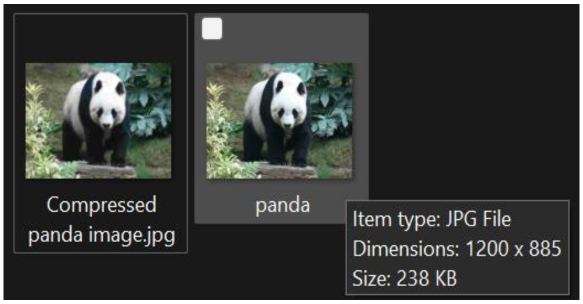


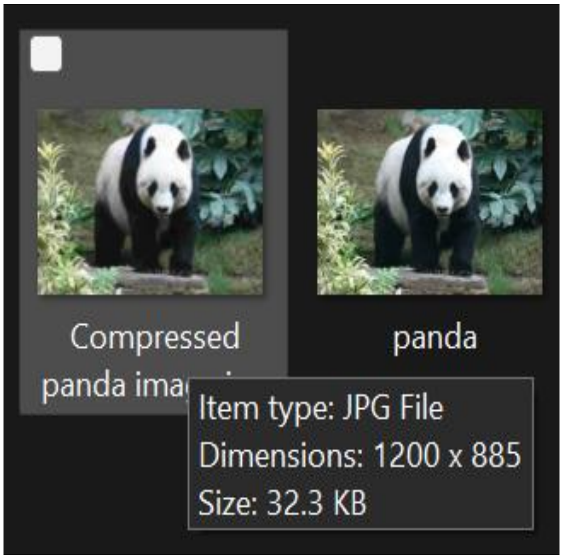
Fig.1 Main tab window open

Once the user receives the compressed image, they can upload it to perform further processes over it.



Item type: JPG File
Dimensions: 1200 x 885
Size: 238 KB

Fig.2 Actual Image size



Item type: JPG File
Dimensions: 1200 x 885
Size: 32.3 KB

Fig.3 Compressed Image size

The compressed image is now used for further processes.

The picture quality of image might get little blurry if high compression is performed.

Then the image uploaded by the user go through an Encryption process which converts the actual compressed image into a Cipher image or encrypted image

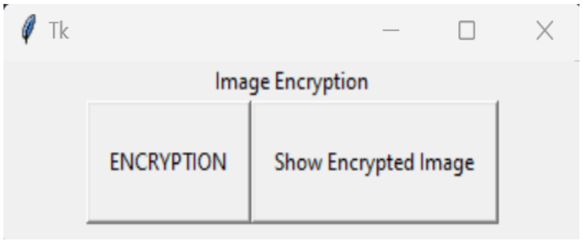
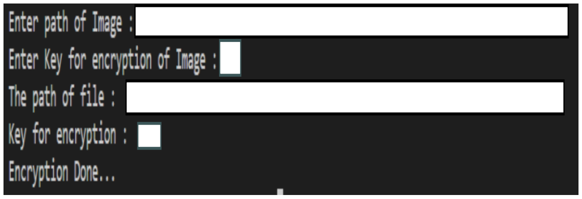


Fig.4 Encryption tab open

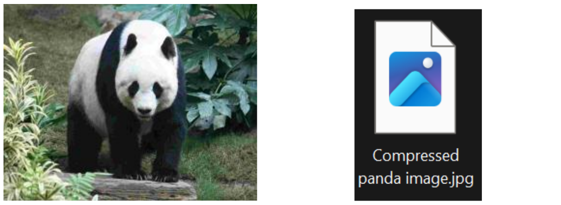
The user will have to enter the path of the compressed image they want to encrypt very carefully and enter the encryption key which they must remember at the time of decryption to decrypted the image.



```
Enter path of Image :
Enter Key for encryption of Image :
The path of file :
Key for encryption :
Encryption Done...
```

Fig.5 Encryption done Successfully

After implementing encryption technique, the compressed image is converted into an encrypted byte code. Now our uploaded image is no more same as the original image



Compressed Image before encryption

Image after encryption is performed

Fig.6 Actual image not visible after encryption

Next the encrypted byte code is converted into a decrypted image using RSA algorithm.

The encrypted image is given as an input to RSA algorithm which is required to decrypt the image.

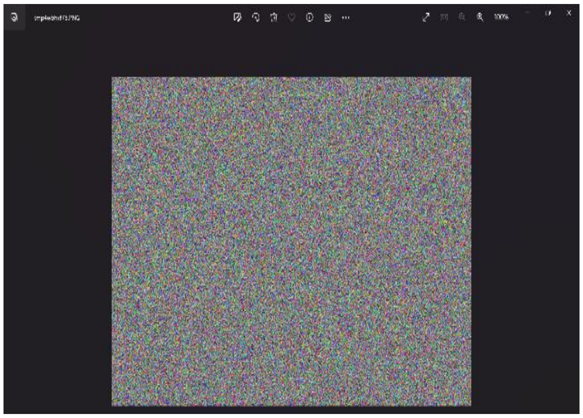


Fig.7 Encrypted Image

This image is now secure and encrypted to send over internet via any secure medium from one user to another.

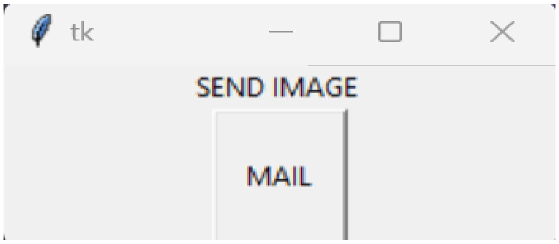
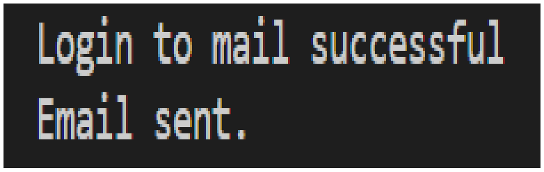


Fig.8 User click on mail to send the mail

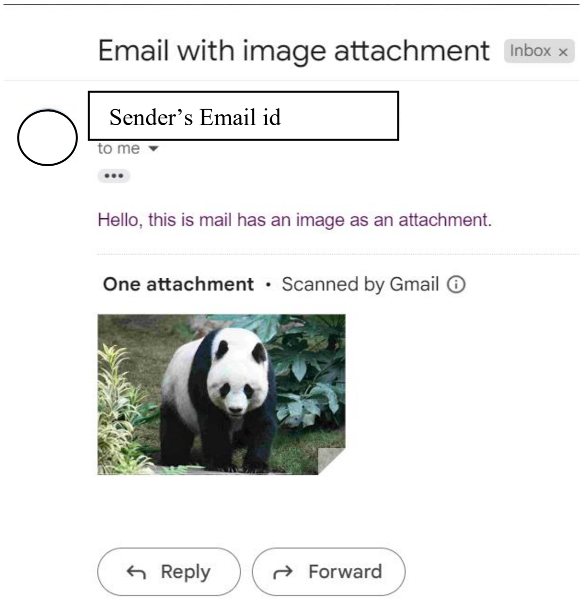


```
Login to mail successful
Email sent.
```

Fig.9 Email sent confirmation

After entering the sender's address and receiver's email address the user will get this email sent prompt in console.

The Recipient receive the decrypted image via this secure channel of internet transfer.



Email with image attachment

Sender's Email id

to me

Hello, this is mail has an image as an attachment.

One attachment • Scanned by Gmail

Fig.10 Received mail via this secure channel

The user can now decrypt the image and see the decrypted image after entering the right path of the image and the correct key which was generated at the time of image encryption.

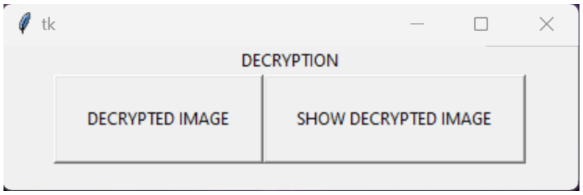
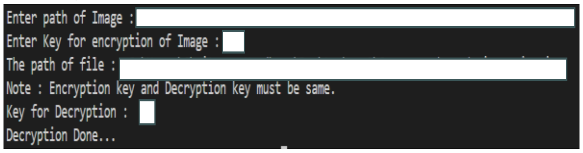


Fig.11 Decryption Tab

Decrypt the image by giving correct path of the image and key.



```
Enter path of Image :
Enter Key for encryption of Image :
The path of file :
Note : Encryption key and Decryption key must be same.
Key for Decryption :
Decryption Done...
```

Fig.12 Decryption Successfully done

The Encryption and decryption key must be same to carry out the process correctly.

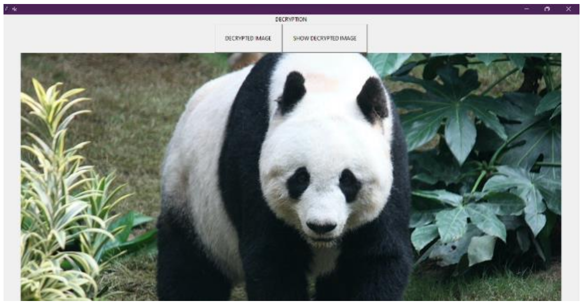


Fig.13 Decrypted Image

IV. TECHNIQUE DESCRIPTION

Several technologies and methods are implemented in order to achieve the output as following:

1.Encryption: The conversion of normal image into a non-understandable image which is hard to guess or understand.

2.Decryption: The conversion of non-understandable image into normal actual image which is easy to understand.

3.Encryption Time: The time taken by the encryption process to convert the image into non-understandable image.

4.Decryption Time: The time taken by the decryption process to convert encrypted image into actual image which is easy to understand.

5.Image Compression: The conversion of actual image into an image with lower picture quality and size.

6.Lossless Image Compression: The conversion of actual image into a compressed image with lesser size than actual image without losing its actual picture quality.

In order to achieve image encryption with less time lossless compression technique was implemented before encryption, this enabled large sized images to be encrypted in less time and consume less space. Then encryption was performed using AES algorithm and decrypted using RSA.

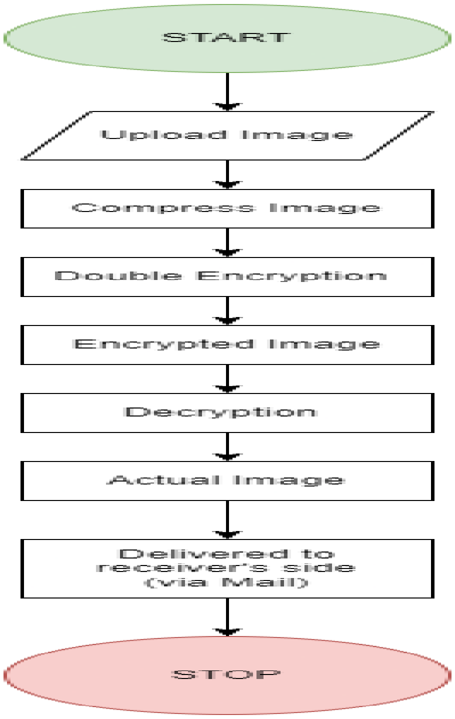


Fig.14 Data Flow Chart

V. TECHNIQUE IMPLEMENTATION

For more clarification process let’s look at the implementation process:

•First choose the image you want to encrypt.

•Compress the image if its larger in size and take a lot of time in process.

•Take the compressed image and upload it for further process.

•Generate the matrix of the Compressed image.

```
[[[199 146  96]
  [199 146  96]
  [199 145  98]
...[105  99 137]
  [105  99 137]
  [105  99 137]]
```

•Click on the Encryption button to encrypt the image.

•Enter the correct path of the image you want to encrypt and generate a key for encryption.

•If you want to see how the encrypted image is going to look , click on the show encrypted button.

•After the encryption process, send the image via your desired application like email to send the image to receiver.

•The decrypted image is now sent to the receiver’s end by this process.

•To see the decrypted image the user, need to enter the correct path and key for the encrypted image to see the actual image.

VI. EXPERIMENTAL RESULTS

The code was written in python programming language and tested for several times in order to remove bugs and match the correctness and other experimental results were continuously analyzed.

The python code was tested with several images of various sizes. After techniques of compression, encryption and decryption the image was found to retain the quality and exactly same to the original image.

The compression of an image was done on several images of different size and the quality of the compressed images was matched to the original images several times.

The size of the compressed image was found out to be lesser than the original image.

Both encryption and decryption need to be performed in the correct order in order to achieve needful results on image encryption decryption. The time taken for processing the image might vary according to the size and quality of the image. If the path of the image is not correct or does not exist in the system then the process cannot be achieved as desired.

VII. CONCLUSION

In today’s world cyber security is becoming one of the most basic and important need. So, in order to provide this security to share images through internet channel this paper specify a technique of Compressed image encryption decryption using two algorithm of encryption AES and RSA. Previously images of large size could not be easily compressed and lost its picture quality .In this research paper a lossless image compression technique has been applied to reduce the size and then encryption is being performed .Now user can easily encrypt and decrypt large images and send the decrypted ,compressed image to user at the other end through mail or any means of media transfer.

REFERENCE

[1] Zareai, D., Balafar, M. & FeiziDerakhshi, M. EGPIECLMAC: efficient grayscale privacy image encryption with chaos logistics maps and Arnold Cat. Evolving Systems (2023)

[2] Chaudhary, Nirmal, Tej Bahadur Shahi, and Arjun Neupane. 2022. "Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach" Journal of Imaging 8, no. 6: 167

[3] Bharadwaja, V Goutham, Yashas M S, Yathendra Yadav T V and Gelvesh G. “IMAGE ENCRYPTION FOR SECURE INTERNET TRANSFER.” International Journal of Engineering Applied Sciences and Technology (2021): n. page

[4] Prof. Ziad AlQadi, ‘A Highly Secure and Accurate Method for RGB Image Encryption’ International Journal of Computer Science and Mobile Computing, Vol.9 Issue.1, January- 2020, pg. 12-21

[5] Rani, Nisha, A. Noble Mary Juliet and K. Renuka Devi. “An Image Encryption & Decryption and comparison with text - AES algorithm.” International Journal of Scientific & Technology Research 8 (2019): 668-673

[6] Deshmukh, Priya. “An image encryption and decryption using AES algorithm.” (2016)

[7] Al-Laham, Mohamad. (2015). Encryption-Decryption RGB Color Image Using Matrix

Multiplication. International Journal of Computer Science and Information Technology. 7. 109-119

[8] Shukla A, Shah J, Prabhu N. Image encryption using elliptic curve cryptography. International Journal of Students' Research in Technology & Management. 2015; 1(2):115-7

[9] A. Subramanya, "Image compression technique," in IEEE Potentials, vol. 20, no. 1, pp. 19-23, Feb-March 2001, doi: 10.1109/45.913206

[10] Abuzalata, Mohammed & Alqadi, Ziad & Al-Azzeh, Jamil & Jaber, Qazem. (2019). Modified Inverse LSB Method for Highly Secure Message Hiding. 8. 93-103

[11] Zahran, Bilal & Al Azzeh, Jamil & Alqadi, Ziad & Zoghoul, Mohd Ashraf & Khawatreh, Saleh. (2018). A modified LBP method to extract features from color images. Journal of Theoretical and Applied Information Technology. 96. 3014-3024

[12] Meghashree B. S, B. R Sujatha, 2018, AES based Image Encryption and Decryption using Matlab, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCESC – 2018 (Volume 6 – Issue 13)