IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 22, Issue 2, Ser. I (Mar - Apr 2020), PP 29-34
www.iosrjournals.org

Image Encryption for Secure Internet Transfer

Ashish Chauhan, CharviMinocha, Karan Bhandari, Akshara Pathak
Assistant Professor Department of Information Technology SRM Institute of Science and Technology
B.Tech Scholar Department of Information Technology SRM Institute of Science and Technology
B.Tech Scholar Department of Information Technology SRM Institute of Science and Technology
B.Tech Scholar Department of Information Technology SRM Institute of Science and Technology

***Abstract*:** *Encryption is a technique widely used in cryptography for the conversion of any readable information or message into a non-readable form, also known as encrypted form in order to protect our data from unauthorized entities. This increases the security of both, our system as well as the data. This mechanism is done via a finite set of instructions, known as algorithms and, set of characters for encryption know askeys.*
This project uses the combination of AES and RSA algorithms that are implemented on the system to make the process of hacking tougher. The ultimate objective is to maintain the confidentiality, integrity and privacy of the data that is being transferred over the channel, from the side of the sender to the side of the receiver. A technique of encrypting a colored image using random matrix key encoding is proposed to ensure the high security while transfer of data.

Keywords: *encryption, AES, RSA, decryption, security, keys, random matrix*

Date of Submission: 18-03-2020 Date of Acceptance: 03-04-2020

I. Introduction

In an organization, system security protocols are needed to ensure the protection of data and information in its networks and resources. Thus, data security is important for safeguarding the corporate asset. If the organizations fail to achieve the same, it could lead to major loss of information such as dipping of sales, discrepancy in the expected results, lack of monitory judgementsetc.

Security of data and information is very important especially when the data is required to be shared with other users. High level of integrity and confidentiality of data is supposed to be maintained when the sharing of data is done. The process of keeping our data safe and secured from other users is known as data security. Data security is implemented to protect our data from being accessed by unauthorized entities like hackers. A very common technique that is used to achieve the same is encryption. Encryption technique is used to convert the readable form of data into unreadable form by using the right set of encryption keys and algorithms. The key is used for encoding and decoding the data. The access to this key is only with the authorized users resulting in high security of data. Encrypting the data in form of text is comparatively easier than encrypting the images and videos. Encryption of images and videos require certain characteristics like mass data capacity and high dataredundancy.

The process of image encryption includes conversion of an image into another difficult image that is not easy to be recognized in order to maintain its confidentiality. In order to view the actual image, decryption of the image needs to be done using a decryption key. There are various methods that can be used for the purpose of conversion of the images however a continuous development of more techniques is done so as to achieve the best method of encryption. Thus, for the implementation of this technique we tend to use a set of important algorithms that effectively help in achieving a secure and desired output. RSA and AES are the two algorithms used in thisproject.

Data encryption methods can be distinguished under two categories i.e. substitution and transposition, based on their cryptographic algorithms. In substitution method, the data is replaced by some other symbol according to the algorithm and in transposition method the position of the data is interchanged or jumbled, following a specific algorithm.

Earlier, a new algorithm was introduced. According to that algorithm, the image was divided into small blocks, approximately of size 8x8. After that the blocks were shuffled and processed resulting in the generation of a random 2D image map. This algorithm makes the decryption more complicated and secure so that the unauthorized users cannot crack the algorithm easily and the confidentiality remains intact. In progress to this algorithm, another algorithm was proposed recently in which shuffling of the image pixels was carried out. This was done to generate a cipher image from a plain image which results into higher security and greater resistance to the attacks.

A lot of researches are carried out to achieve the maximum amount of security when it comes to the transfer of images in order to avoid the access of unauthorized users and increase thesecurity.

II. Literature survey

Extensive research has been conducted to find the most accurate image encryption technique that not only increases the level of security but also reduces the risks of attacks by hackers, crackersetc.

[1] 'A Highly Secure and Accurate Method for RGB Image Encryption'(2020)

This paper discusses the method of using RGB color image encryption-decryption which provides a higher level of security, accuracy and an accurate encryption-decryption technique which requires minimum hard work and software implementations.

[2] 'Image Encryption Using Elliptical Curve Cryptography' (2013)

This paper deals with Image encryption using a unique method called the Elliptical Curve Cryptography. This approach uses public key cryptography based on algebraic structure of elliptic curves over finitefields.

[3] 'Encryption-Decryption RGB Color Image Using Matrix Multiplication'(2015)

This paper deals with Image encryption and decryption using the RGB color image using matrix multiplication. The accurate matrix for encryption is generated using matrix multiplication and then it is encrypted via using the desired key and thus decrypted later at the receiver'send.

[4] 'An Image Encryption and Decryption method using AES Algorithm',(2016)

This paper involves the usage of Advance Encryption standard (AES) algorithm which provides a better method to perform encryption and decryption over the images, thereby increasing the security from unauthorized users.

III. Methodology

In this project, we are using Python for the basic encryption and decryption process of the image that has to be sent over a secure internetchannel.

Firstly, the user uploads the image which can be done either by desired path defined by used by the user or by capturing the image using awebcam.

Once the image is uploaded and the matrix of the image is generated. Then the user goes through the encryption process of the desired image. This step is used to convert the actual

image that has to be transferred into a cipher or encrypted image.

The encryption can be carried out via two methods; Single encryption technique and Dual encryption technique.

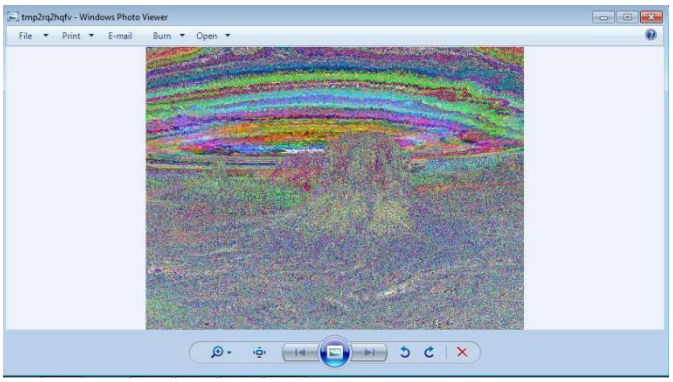
the actual image

Now, on selecting the desired option amongst the two mentioned above, the actual image is converted into an encrypted byte code format instantly via the AES algorithm. Which means that the image does not appear the same due to the application of the encryption algorithms.

the encrypted byte-code image

The generated encrypted byte-code image is taken as the input for the image that needs to be decrypted by the RSA algorithm.

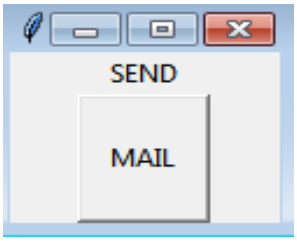
This encrypted byte-code is then converted into an encrypted image via the RSA algorithm.



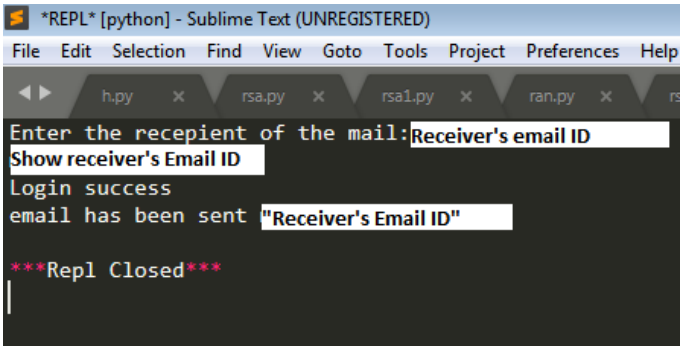
The encrypted image

It is now safe to be sent over the transfer channel from sender's end to the receiver's end.

This can be done via several techniques such as Email, Whatsapp, Message etc.

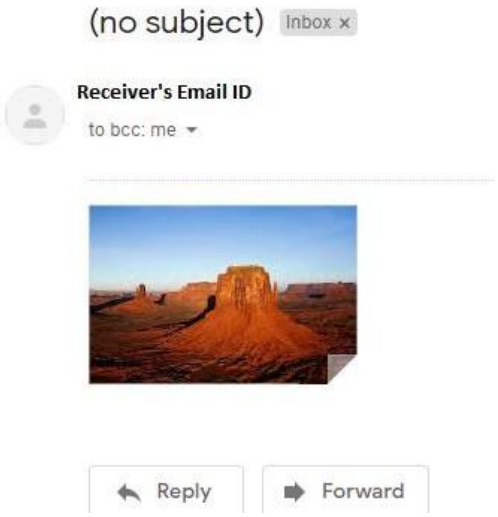


user clicks on mail



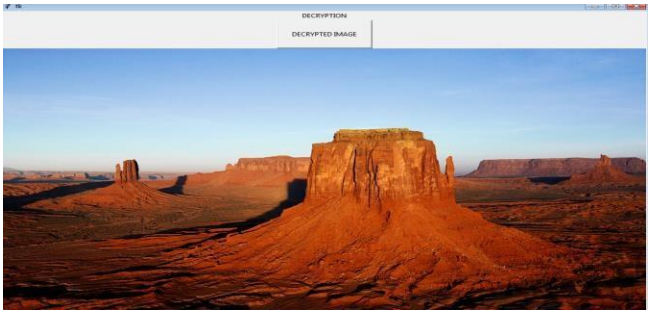
input the Recipient's email ID

The user is asked to provide the Recipient's Email address over which the sender is required to send the Decrypted image securely.



the received mail

The recipient receives the Decrypted image eventually through this secure Internet transfer technology.



the decrypted image

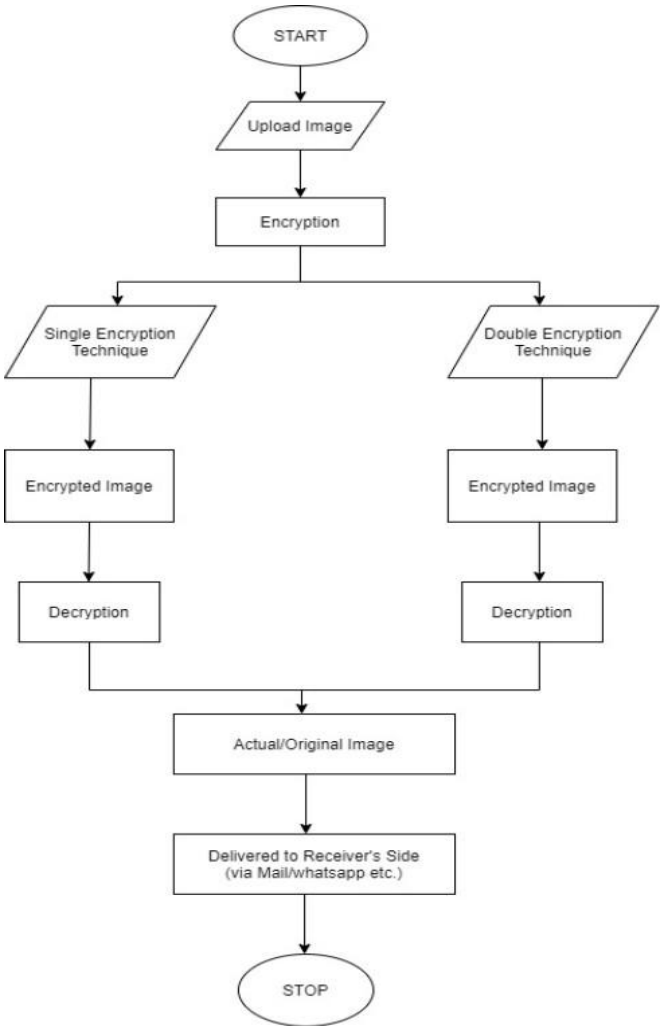
IV. Technique Description

Various technologies and techniques are used for the purpose of implementing the following:

1. Encryption: The process of converting the actual image into another image that is difficult to process orunderstand.
2. Decryption: It is the process of fetching the original contents from the unreadable form ofdata.
3. Encryption Time: The time that is taken for the purpose of implementingencryption.
4. Decryption Time: The time that is taken for the purpose of converting the image from encrypted form to actual form.
5. Double random matrix key: It is a 2D matrix that is generated with random values in order to reduce the probability of the hacking ofkey.

In order to achieve image encryption, a method was suggested according to which the image color should be converted to grey before encryption to achieve greater confidentiality. However, this method had some disadvantages as well. The disadvantages are asfollowed:

1. The components in this process requires greater memoryspace.
2. The components in this process also require extra time for the transmission ondata.
3. The red and greens components in this process are usually not secure.



V. Technique implementation

For illustrating the concept let's take a look at the following steps:

- Upload the image that has to be encrypted before itstransmission.
- Generate the matrix corresponding to the uploadedimage.

```
  ...
  [ 74 129 211]
  [ 73 130 211]
  [ 69 132 211]]

 [[ 47 124 206]
  [ 51 123 205]
  [ 53 126 205]
  ...
  [ 75 130 212]
  [ 73 130 211]
  [ 69 130 210]]

 [[ 49 126 206]
  [ 53 125 207]
  [ 54 127 206]
  ...
  [ 74 131 210]
  [ 73 130 211]
  [ 70 131 211]]

 ...

 [[  2   3   0]
  [ 35   7   3]
  [ 56   8   4]
  ...
  [  9   4   1]
  [ 14   4   2]
  [ 20   5   0]]

 [[ 33   3   1]
  [ 30   4   3]
  [ 37   6   4]
  ...
  [  9   3   3]
  [ 15   5   4]
  [ 18   6   6]]
```

- Click on the "Encryption"button.
- Select the desired encryption technique, i.e. Single or Dual.
- After selecting the desired option, click on the Technique via which you want to send the image to the Receiver'sside.
- The decrypted image is sent to the receiver at the receiver'send.

VI. Experimental results

The python code was written, executed and tested several times in order to find the correctness and the experimental results were analyzed several times to remove thebugs.

The python code was tested using various images of different sizes, and it was found out to be exactly matching as the original image.

EncryptionandDecryptionrateneedtobeappropriatefrom the point of good image aspect. Time taken by the encryption and decryption for different sized and colouredimage was measured. Depending on the size of the image, the time taken for the same may vary accordingly. If the path given by the user is invalid or does noexist then the process cannot be achieved.

VII. Results Discussion

The experimental results revealed during this study are as follows:

1) The proposed technique is a successful amalgamation of two techniques and RSAalgorithm.
2) The proposed technique enhances the security of the systemeffectively.
3) The proposed technique successfully sends the decrypted image at the Receiver'sside.
4) The proposed Technique is accurate and efficient to a greatextent.
5) The decrypted image is coloredimage.

VIII. Conclusion

The security of digital images has become an important part of cyber security since a lot of transfer occurs over the internet in the form of images very frequently. This new technique of image encryption and decryption uses combination of two encryption algorithms namely AES and RSA. According to our experiments the image transmission has rapidly been increased and has become much more secure. The user sends the decrypted image to the receiver and dynamically takes the input of the receiver's email id so that the image is always sent to the desired person enhancing the security during transmission. Usually, the process of decryption of the image produces a black and white image but, in our project, we have ensured that the decrypted image is a colouredimage.

References

[1]. Prof ZiadAlQadi,(2020),'A Highly Secure And Accurate Method for RGB ImageEncryption'.
[2]. AshutoshShukla,JayShah,NikhilPrabhu(2013),'Image Encryption Using Elliptical CurveCryptography'
[3]. Mohamad M Al-Laham,(2015),'Encryption-Decryption RGB Color Image Using MatrixMultiplication'
[4]. PriyaDeshmukh,(2016),'An Image Encryption and Decryption method using AESAlgorithm'.
[5]. G A.Sathishkumar, K. Bhoopathybagan and N. Sriraam, (2011) "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network Security & its Applications, Vol. 3, No. 2, pp181-194.
[6]. Jamil Al Azzeh, Hussein Alhatamleh, ZiadA. Alqadi, Mohammad Khalil Abuzalata : Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications (0975 – 8887).Volume 153 – No2, November2016.
[7]. Ziadalqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, v. 2, issue 4, pp. 288-298,2007.
[8]. Mohammed Abuzalata Jamil Al-Azzeh, ZiadAlqadi; Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February-2019.
[9].] Jamil Al Azzeh, ZiadAlqadiQazem, M. Jabber: Statistical Analysis of Methods Used to enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24- 26,2017.
[10]. Bilal Zahran, Jamil Al-Azzeh, ZiadAlqadi, and Mohd- Ashraf Al Zoghoul: A Modified Lbp Method To Extract Features From Color Images: Journal of Theoretical and Applied Information Technology May2018.
[11]. J Al-Azzeh M Abuzalata, ZiadAlqadi, Modified Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing, v, 8, issue 2, pp. 93-103,2019..
[12]. KundankumarRameshwarSaraf, Vishal Prakash Jagtap, Amit Kumar Mishra, (2014, May-June)."Text and Image Encryption Decryption Using Advance Encryption Standard", International Journal of Emerging Trends and Technology in computer science(IJETTCS) volume-3, issue-3,pp.118-126.

Ashish Chauhan,etal. "Image Encryption for Secure Internet Transfer." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 22.2 (2020), pp. 29-34.