An Algorihmic Approach for Transmission of Encrypted Image over Cloud System

Mr. Prabal Joshi, Dr. Shweta Pandey[2]

Research Scholar, Department of CSA, Desh Bhagat University,Mandi Gobindgarh, Punjab,[1]
Assit Professor, Department of CSA, Desh Bhagat University,Mandi Gobindgarh,, Punjab, India[2]

Abstract
Cryptography is the practice and study of hiding information. It is used from a thousand years ago. In the history of the Greeks are used to sending messages without an unauthorized person knowing. The Greek refugee Demeratus, according to the historian Herodotus, penned a message on two wooden tablets indicating that the Persian King Xerxes intended to attack Greece. He put wax on these tablets so that any Persian guards who happened to come across them would think they were blank. After receiving the tablets and removing the wax, the Greeks got ready to face Xerxes at the Bay of Salamis, where they triumphantly faced him brief history of cryptography. Methods and the key are the main factors of cryptography. Method is a process to encrypt the information by changing the word with other words and properties of methods are defined in the key. Encryption security mainly depends upon the number of keys that are generated by methods. It is very difficult for unofficial to decrypt the information if the large number of keys are used for encryption. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Until modern times cryptography referred almost exclusively to encryption.

Keywords-cloud computing; cryptography; encryption; decryption; AES algorithm; digital signature

Date of Submission: 12-12-2024 Date of acceptance: 25-12-2024

I. INTRODUCTION

Cryptography is a popular solution for video encryption. Using secret sharing concepts, the encryption procedure encrypts a secret video into the so-called shares which are noise-like secure videos which can be transmitted or distributed over an untrusted communication channel. Using the properties of the human system to force the recognition of a secret message from overlapping shares, the secret video is decrypted without additional computations and any knowledge of cryptograph. Cryptography deals with the encryption and decryption of the videos to protect the information related to them. The encryption requires certain levels of computation to divide the original video into several shares. This is done keeping in mind the fact that the resultant shares show no resemblance to the original video. As a new type of the technique of Cryptography, the shares are so manipulated that by looking at them one may extract some other information alone which would not be correct. Such a technique results into the formation of the innocent shares. After the formation of the shares, they are simply overlapped or better stated in terms of video processing are simply “and-end” to get the original video back. We can implement the Cryptography by using one of following access structure schemes. The field of Cryptography has been developed over the last several years. The original method was proposed by Naor and Shamir [1] for binary images. This provides a perfectly secure system where secret messages are contained in \shares". Individually these shares resemble random noise, but when they are stacked and aligned perfectly, their message is decrypted using only the human system. While this method gives security for text and binary images, the growth of digital media requires the expansion of this technique to provide security for gray and colour images. Several methods have been developed for securing gray and color images, including half toning [2], dithering [3], color sub pixel groupings [4], and meaningful image shares [5, 6]. Through this expansion of the original method, Cryptography provides a secure way to store and transmit text, binary images, gray images, and colour images.

II. LITERATURE REVIEW

2.1 CRYPTOGRAPHY IS THE SCIENCE OF INFORMATION SECURITY

Mohammed Abu Taha, MousaFarajallah, RadwanTahboub, Mohammad Odeh [14] Cryptography in the past was used in keeping military information, diplomatic correspondence secure and in protecting the national security. However, the use was limited. Nowadays, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage. Also, cryptography is a powerful mean in securing e-commerce. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one who has the decipher key, and data cannot be changed means the original information would not be changed or modified; this is done when the sender includes a cryptographic operation called a hash function in the original message. A hash function is a mathematical representation of the information, when any information arrives at its receiver; the receiver calculates the value of this hash function.

2.2 A NEW APPROACH TO CLASSICAL HILL CIPHER(2013)

M. Nordin A. Rahman, A. F. A. Abidin, MohdKamirYusof, N. S. M. Usop[19] the Hill cipher is the first polygraph cipher which has some advantages in symmetric data encryption. However, it is vulnerable to known plaintext attack. Another setback is that an invertible key matrix is needed for decryption and it is not suitable for encrypting a plaintext consisting of zeroes. The objective of this work is to modify the existing Hill cipher to overcome these three issues. Studies on previous results showed that the existing Hill algorithms are not yet sufficient. Some of these algorithms are still vulnerable to known plaintext attack. On the other hand, some of these algorithms have better randomization properties and as a result they are more resistant against known plaintext attack. Nevertheless, these enhanced Hill cipher algorithms still face the non-invertible key matrix problem. Moreover, neither of these algorithms are suitable for all zeroes plaintext block encryption. In this paper, a robust Hill algorithm (Hill++) is proposed. The algorithm is an extension of the Affine Hill cipher.

2.3 RajinderKaur, Er.Kanwalprit Singh [20] Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication and storage of images. Encryption is one of the ways to ensure high security images are used in many fields such as medical science; military. Modern cryptography provides essential techniques for securing information and protecting multimedia data. In recent years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from unauthorized access.

Tariq and Agarwal [1] it showed how the data can be accessed securely using the keyword which is stored in the cloud. This accessing is securely done using the fuzzy keyword searching wherein the keyword is one which is saved in the cloud during the file uploading. The fuzzy keyword search algorithm works efficiently by giving the results if there are minor spelling mistakes. Here during the data transfer from the client to the cloud the data is encrypted using AES symmetric algorithm with secret key. The encrypted file in the server is again encrypted using the asymmetric RSA providing double encryption and more security. During downloading the file from the server, the keyword is matched and then it is decrypted using RSA and AES decryption algorithms.

2.4 The data encryption is done using padding scheme which changes dynamically. Data manipulation access is given only for the authorized access service users. The taxonomy of the user gives a clear detail about each user who are allowed for which type of service access. Namasudra et al. [15] worked on deoxyribonucleic acid (DNA) computing to provide security for big data in cloud environment. Here 1024bit DNA based password is used as a key. The user after registration needs to login and then request for data access wherein the public key of the data owner is searched from the database and provide the public key for only those clients whose certificate and the secret key authenticity is confirmed. Post of which the data owner sends the generated DNA based secret key and certificate for the user which helps the user to access and store the data. In this method the results are calculated for number of users v/s key generation time and encryption and decryption time. Patel and Dadhania [16] proposed the article where the authors used both the symmetric and asymmetric algorithms such as AES and RSA. The MD5 Hash algorithm is also used for encryption. The given text or images is initially converted into a single vector from the formed row column matrix. This vector is divided into two blocks such as A and B, the block A is substituted to AES plus Hash for encryption and the block B is subjected to RSA plus Hash. The key obtained from both the blocks are XOR'ed and form a new key C which is again used for encryption. The same is used for decryption and continued obtaining plaintext by reverse process. Sivakumar et al. [17] used Heroku cloud as a cloud platform where data uploaded by the user is processed through advance encryption standard (AES) and the generated key is given for the user. Here majorly performance is calculated based on assess delay. The size of the text file used here are of 3, 5, 7, 10 and 15 MB which clearly shows that as there is increase in file size and hence the delay time is also increased simultaneously. Singh and Sharma [18] tried to enhance the cloud data security along with improving the efficiency by using various cryptographic techniques. Here the data is split into different modules and all the modules are stored in different cloud platforms where in applying AES and secure hash algorithm (SHA) for encryption. The comparison study is also made between the split algorithm and different standard symmetric algorithms for analyzing the security level, number of keys used and efficiency of the algorithms. The results are better for the split algorithm giving the highest efficiency using a single key resulting in high level of data security. Makkaoui et al. [19] worked on cloud data confidentiality and efficiency. Cloud-RSA and multiprime RSA are used to Encrypt the message whereas decryption is processed using multiprime RSA along with CRT to obtain high efficiency. The performance is calculated by comparing the results of encryption and decryption time for multiprime cloud RSA, cloud RSA and Cloud-ElGamal multiprime cloud RSA is also used for security analysis, it shows the good efficiency results compared to other methods. Lavanya and ThamizhThendral [20] presented the articles by the self-designing the algorithm known as deep substitution encryption method. Here the given plain text is passed through five different substitution technique i.e., each character has 6 cipher text. The plain text is first substituted with American Standard Code for Information Interchange (ASCII) code, after obtaining the ASCII codes the periodic elements of the periodic table are substituted. These periodic vales are further substituted with flower names. The 4th substitution phase i.e., hypertext markup language (HTML) color names given for the flower names of 3rd phase. This color names are finally substituted as HEXCODE which is considered as cipher text. The cipher text is decrypted back to the original plaintext by reversing all the five substitution phases in reverse order. To break this algorithm the hackers, need to have a vast knowledge about the entire periodic table and name of flowers. Miri and Rashid [21] proposed a method for data duplication, which is preserved from access of semi secured cloud service providers. The given plaintext is processed through Burrows wheeler transformation (BWT) encoding in which the block of plaintext is sorted using lexicographic sort which is further subjected to bzip2 function applying ‘move to front transformation and Huffman coding. The transformation created a L vector which is used to decompress the encoded text. To use this L vector the user is asked question for verification. Failing of verification will lead to access of only compressed file. The compressed files of the user are compared to avoid reduplication. Devi and Mani [22] applied double compression before encrypting the file to enhance the data security. Burrows wheeler transformation (BWT) technique is used for which move to front transformation is applied. The obtained results are further subjected to run length encoding (RLE) compression to reduce the complexity of redundancy. Which is finally dealt with modified RSA algorithm to encrypt the file, the RSA algorithm is modified by converting the obtained ‘n’ value into binary values which are further applied to find the cipher text. Singh et al. [23] tried to apply a simple and most secured encryption algorithm by using binary sequence for the given plain text. Firstly, the given plain text is converted into the binary bits and then it appended to make km/2 bits where Km is the mirror key and Kr is the rotational key. Applying mirroring to the appended sequence and then processed further for rotation leading to cipher text. The decryption process is carried out in reverser by rotational operation and then sequence mirroring and finally removing the right most bits which will generate the final original plain text. This algorithm is proved to be secure against the brute force attack also. Abdullah et al. [24] here the plain text is divided into 2 parts, in which for the first part of the plain text in encrypted using the AES algorithm of key size 128 bits. The encrypted text is followed by LempelZiv-Welch (LZW) compression. Then the second part of the plaintext is encrypted using 2,048 bits key of RSA which is also further subjected to LZW compression. Due to the use of both the AES and RSA algorithms the security level and robustness is high without comprising with the efficiency. The results of the proposed hybrid cryptographic algorithm (HCA) are compared with that of several other algorithms proving the results of HCA algorithms as best. Mani and Devi [25] could enhance the data security by applying pre-processing before encryption. The pre-processing involves encoding the given plain text by using Lucas and Fibonacci series obtaining first level of security and then the encoded text is further compressed with Huffman encoding resulting in second level of security and finally it is subjected to the RSA public key cryptographic algorithm resulting in cipher text which is third level of security. The cipher text is converted back to the plain text in reverse process by decrypting the cipher text then decompressed and finally decoded obtaining original plain text. Namasudra and Roy [26] in this scheme the cloud service provider maintains the separate table for storing the data. The table basically consists of four columns wherein the first column is the group number (Gp. No), second column is the data owners ID which is the ID number given for each data of cloud service provider. The third column is the data size column in which the data is moved to the particular group, i.e. the data owner sends the data to the cloud service provider and this data will be sent to particular group according to its size. This helps in reducing the access and search time of the data. During the process of file uploading, the data is first encrypted using the secret key and then it is again encrypted using the private key of the data owner. The data owners encrypt the data and the certificate using the cloud service providers public key and finally makes a bundle of encrypted data. The fourth column of the cloud service provider table consists of the date and time of the file which the data owner uploaded. While accessing the data the cloud service provider is trying to access and search the file only in that section. The data owners are also asked to register before sending any file to the cloud service provider. Mani and Devi [27] tried to enhance the data security by generating different key streams using Pythagorean triplets. Any two positive prime integers are used to find the triplets such that the gcd of the triplets is always 1. Barning tree is constructed using this triplet which are further used for used as a keystream. Out of the 8-bit keystream 1 bit is used for parity checking. DES algorithm is modified for encrypting the data file by using 8 characters from the primitive pythagorean triples (PPT) during first round of DES and is continued for all the 16 rounds of data encryption standard (DES). The modified DES results in good security and the generation of keystreams using PPT will enhance the security levels.

III. OBJECTIVE

The proposed solution for cloud computing security is a novel method, where we are using image or part of image as encryption key to encrypt the data and information. The complete work flow of the method is as follow:
Step 1: Get the data or information which is going to be on cloud infrastructure.
Step 2: Now choose any image, and apply differential evolution algorithm. This will perform an intelligent segmentation process and will differentiate between objects and background of the image.
Step 3: Now the encryption key will be generate by using segmented objects of the image.
Step 4: Encryption will be process using the generate key. The pixels which value exist 100 to 255 are used for hiding data or image.
Step 6: Cloud computing infrastructure will communicate for the secure transaction of data and information over the network
Following are the key points that must be taken care of in this research work:

- The complete research work focuses on different Public/private image based cryptography.

IV. KEY LINK ALGORITHM

The link algorithm comprises the selection of a portionof c0(x), a binarization process, and the selection of L values to represent each key bit. The central 64x64 portion of c0(x) is extracted. This extraction is to provide translation invariance during subsequent verification attempts. Next, the real and imaginary components of the extracted portion are concatenated to form an enrolment template of dimension 128×64, i.e. an array with 128 columns and 64 rows [3, 4]. For example, if the element a+bi appears at position (x, y) of the 64×64 portion of c0(x), then, in the enrolment template, element a will appear at position (x, y) and element b will appear at position (x+64, y). This concatenation process converts a 64×64 complex-valued array into a 128×64 real-valued array. The enrolment template now contains 8192 real values, d, derived from either the real or imaginary components, a or b, respectively. Each value of the enrolment template is then binaries with respect to 0.0, i.e.:
$d \rightarrow 1$ if $d \geq 0.0$ $d \rightarrow 0$ if $d \leq 0.0$
This forms a 128×64 binaries enrolment template, which will be used to link with k0.

V. RESULT AND IMPLEMENTATION

5.1PROPOSED SYSTEM

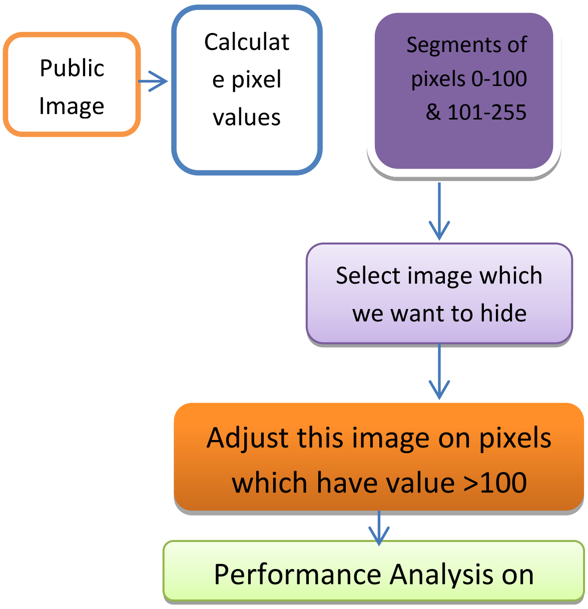

Public Image
Calculat e pixel values
Segments of pixels 0-100 & 101-255
Select image which we want to hide
Adjust this image on pixels which have value >100
Performance Analysis on

Figure 1 Flowchart used for Expected Results

5.2 DESIGNING TOOL FOR PROPOSED ALGORITHM

MATLAB platform used implementation of proposed work. It provides a good programming environment. The dataset which have taken also describe there on that dataset we implement our technique. Describe about the software and hardware required for implementation. By using snapshots describe what the steps which follow to get result are.

5.2.1 Basic of MATLAB

MATLAB (MATRIX LABORATORY) is providing an environment for computation in numerical form and we can say it a programming language of 4th generation. Math Works developed it, there is matrix manipulations, interaction with user, create functions, compatible with other languages as like C, C++ etc.By survey it found that near about one million users are available in market which follows MATLAB for programming and numerical computing. Students from any stream like engineering, science etc can use this tool for implementation of proposed algorithm. Many research institutes also use MATLAB as research platform tool.

In technical computing MATLAB perform a vital role. It provides a integration of three environment as like computation, ization, and programming. There many in built data types and functions that are very useful for developer and make it easy to perform. This also support object oriented programming. Due to these types of tools MATLAB is point of attraction for all researchers. We also choose the MATLAB tool as programing of our proposed work. MATLAB is short form of Matrix Laboratory.The following windows are common in starting of Matlab platform:

*Desktop: Desktop represents the basic windows and folders that are open and ready to use for user. Current folder, Command window, Workspace etc comes in desktop.
*Figure Window: when a programmer run the program then some outputs generated that are represented in figure window. The color of this window is gray and background is white.
*Editor Window: all files written and edited in this window which have extension .m.

6. MODULES OF THE PROPOSED SYSTEM

Module 1: Create GUI to make easy interfere with clients

```
functionvarargout = ImageEncryptionGui(varargin)
gui_Singleton = 1;
gui_State = struct('gui_Name',       mfilename, ...
                   'gui_Singleton',  gui_Singleton, ...
                   'gui_OpeningFcn', @ImageEncryptionGui_OpeningFcn, ...
                   'gui_OutputFcn',  @ImageEncryptionGui_OutputFcn, ...
                   'gui_LayoutFcn',  [] , ...
                   'gui_Callback',   []);
ifnargin&&ischar(varargin{1})
gui_State.gui_Callback = str2func(varargin{1});
end

ifnargout
    [varargout{1:nargout}] = gui_mainfcn(gui_State, varargin{:});
else
gui_mainfcn(gui_State, varargin{:});
end
```

Module 2: Generation of key

```
function [key] = keyGen(n)
n = n*8;
% n = 2048*2048*16;
% n = 24 * 24 * 8;
bin_x = zeros(n,1,'uint8');
r = 3.9999998;
bin_x_N_Minus_1 =  0.300001;
x_N = 0;
tic
```

Module 3: Processing Image

```
function [proImageOut] = imageProcess(ImgInp,key)
 [n m k] = size(ImgInp);
```

Module 4: Decoder at other side

```
EncImg=getimage(handles.axes1);
globalImg;
global key;
DecImg = imageProcess(EncImg,key);
Img = imageProcess(EncImg,key);
axes(handles.axes2);
imshow(DecImg);
imwrite(DecImg,'Decoded.jpg','jpg');
guidata(hObject, handles);
```

7. RESULTS OBSERVED

We create a GUI to make it user friendly. GUI attracts the all functions and features of model at a single platform. So we initial our project with GUI interface.

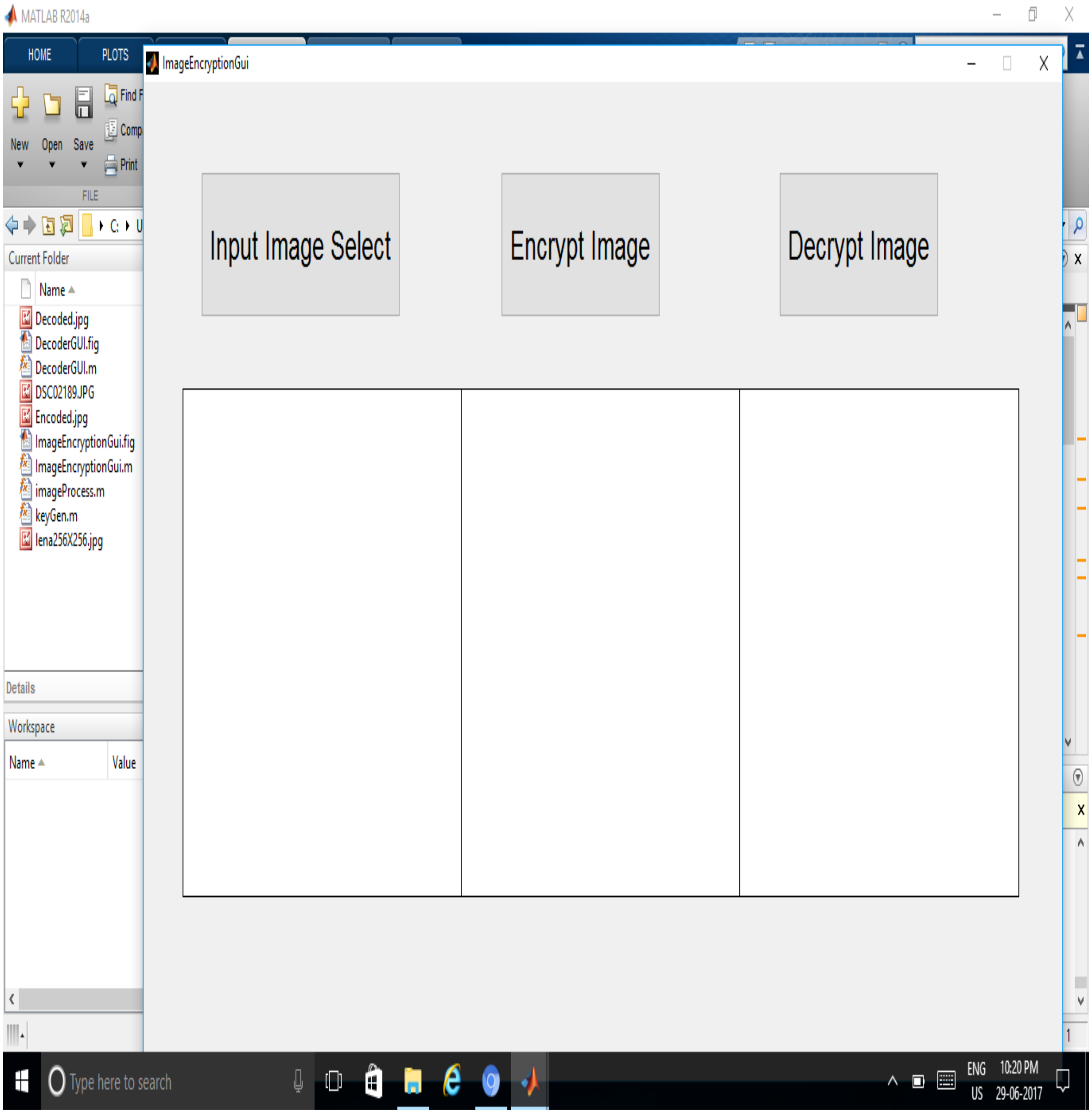


Figure 2. GUI interface of model

Description7.1 This figure shows that initate our project with GUI interface.

Now we need a image which want to encrypt. So we browse it as shown in following figure by pressing the button ‘Input Image Select’.

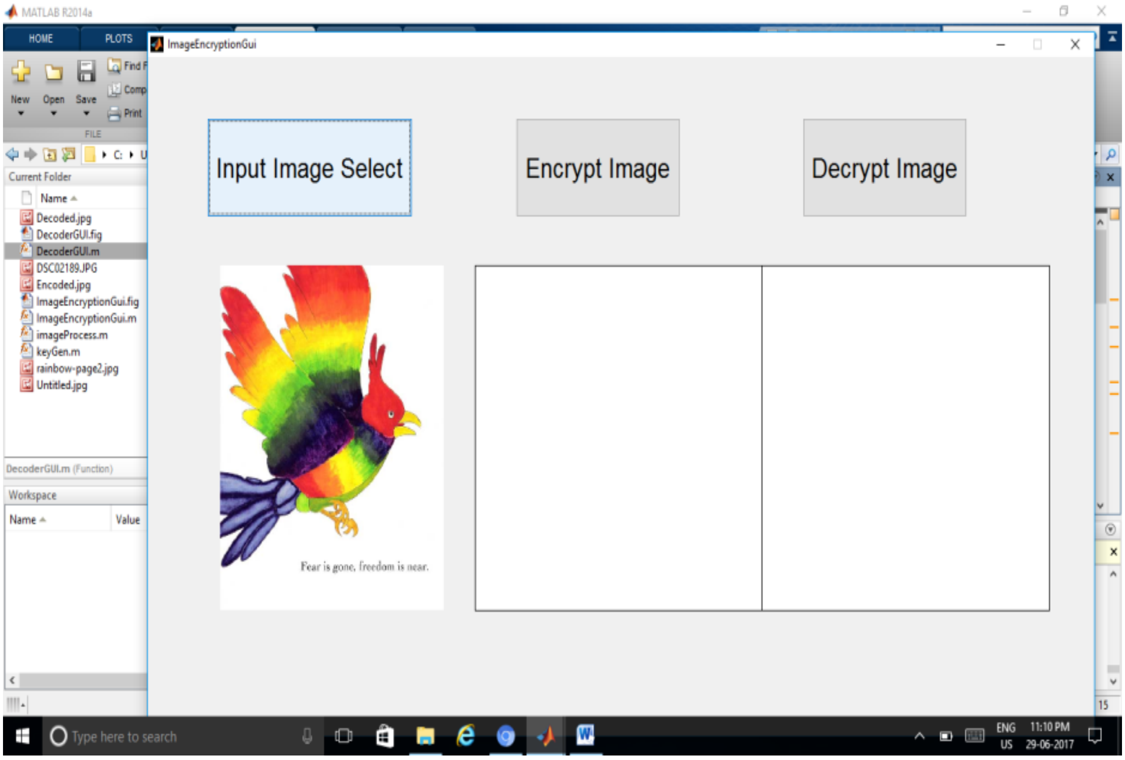


Figure 3. Access of input image for Encryption

Description 7.2 This figure shows that the Selection of image those we want to encrypt. The output comes from this process is work as like input of proceeding step. The encoded image is shown in middle box. We get this image by pressing the button 'Encrypt image'.

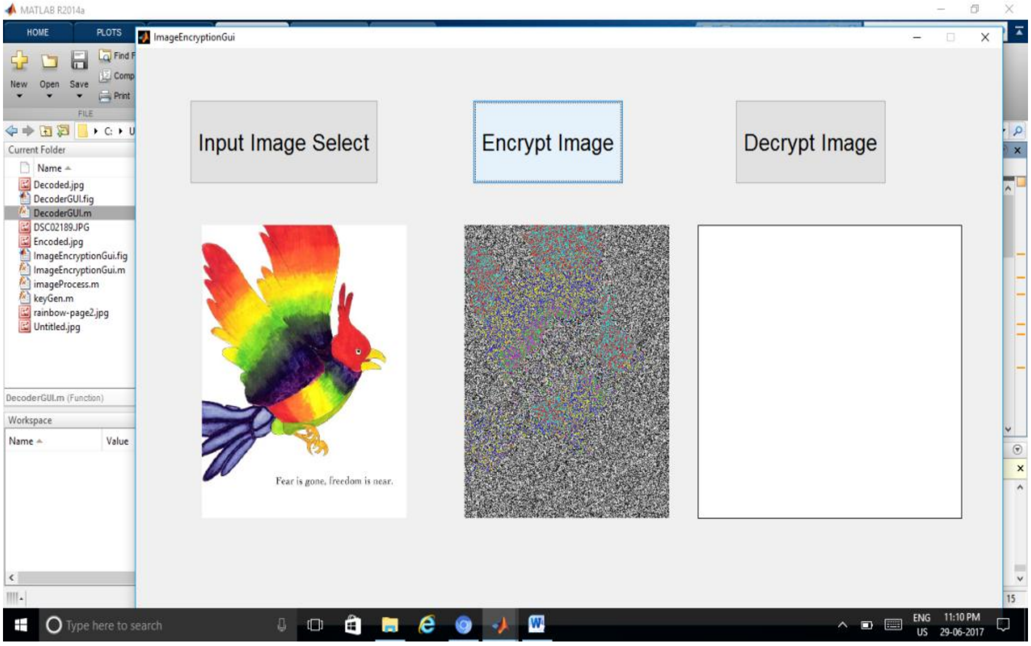


Figure 4 Encoded image after Encryption

Description 7.3 This figure shows that the conversion of plain image into an encrypted image.

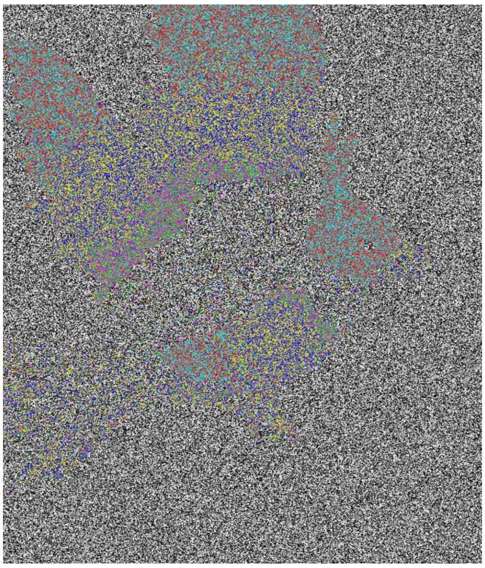


Figure 5 Encoded image save in folder

Description 7.4 Now we save decoded image in folder for further transmission over cloud or any social site.

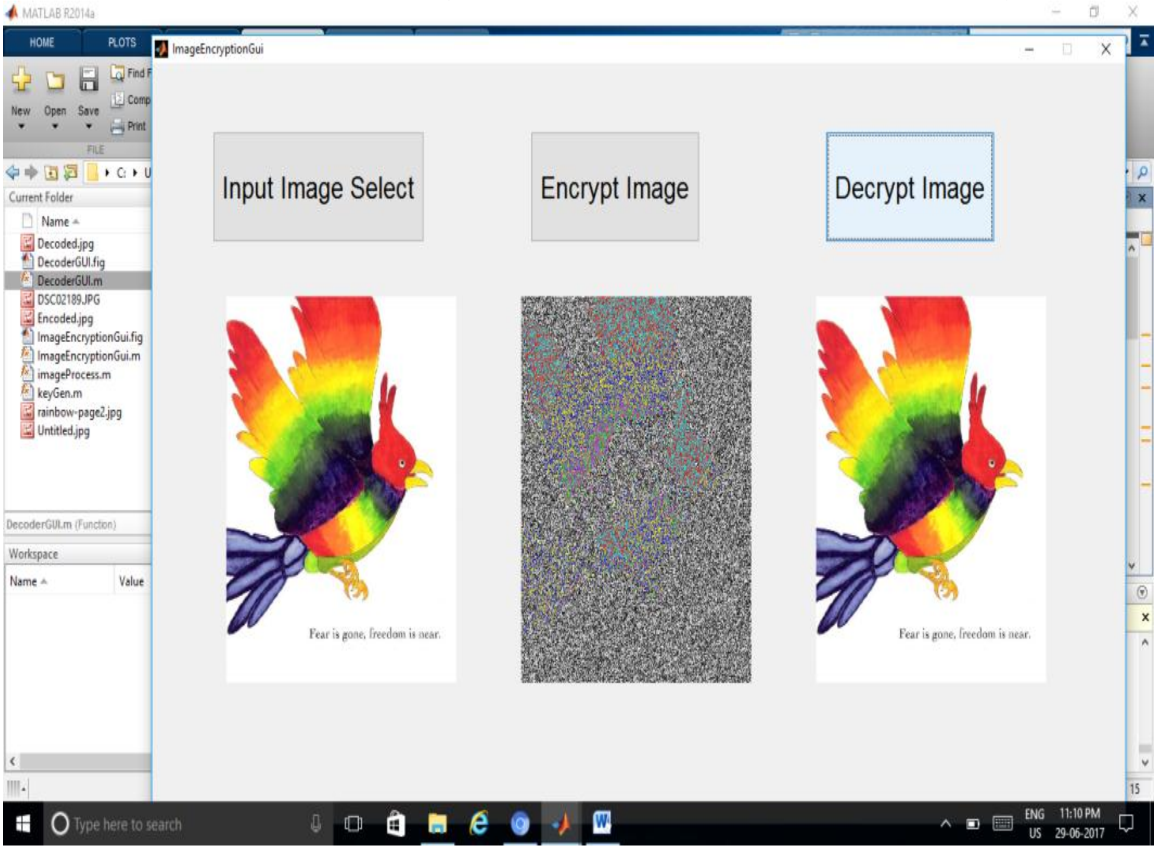
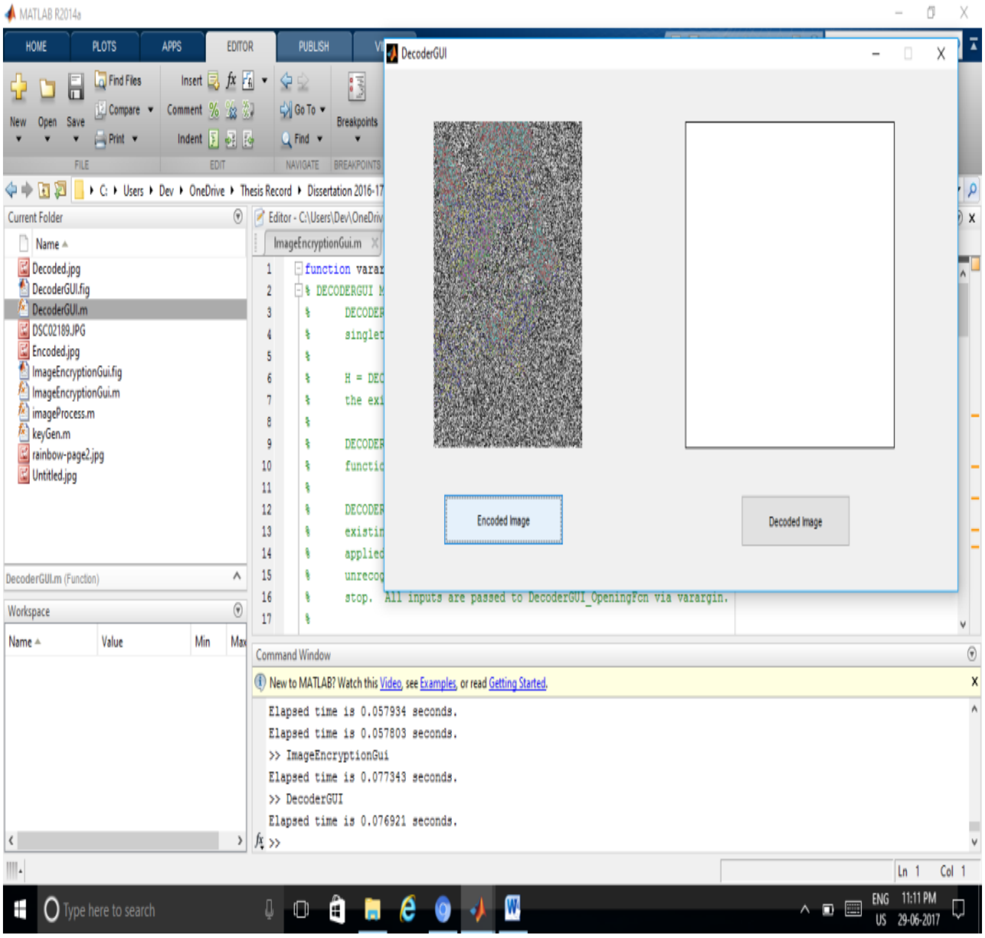


Figure 6. Decrypted image received at same side

Description 7.5 In this figure performs decoding process and the image got as original at same side.
Now we upload the image on any social site that is visible to publically and anyone can download. The client or user only can decrypt it to which we sent decoder code. After receiving the code the following GUI open at receiver side:

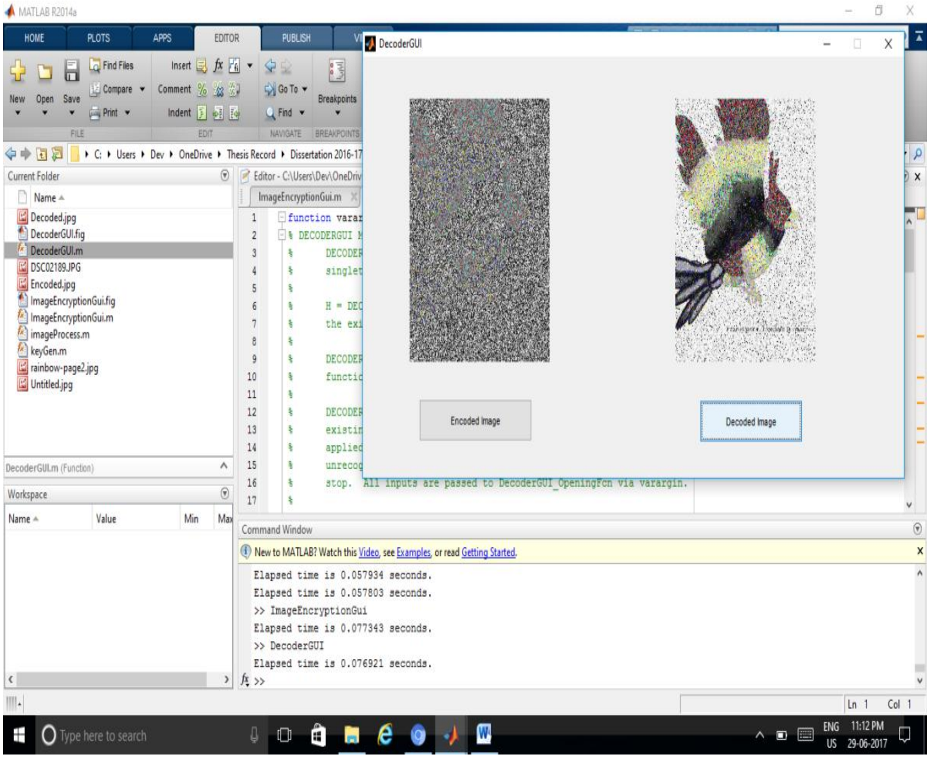


```
function varar
% DECODERGUI M
%      DECODER
%      singlet
%
%      H = DEC
%      the exi
%
%      DECODER
%      functic
%
%      DECODER
%      existin
%      applied
%      unrecog
%      stop.  All inputs are passed to DecoderGUI_OpeningFcn via varargin.
%
```

```
Elapsed time is 0.057934 seconds.
Elapsed time is 0.057803 seconds.
>> ImageEncryptionGui
Elapsed time is 0.077343 seconds.
>> DecoderGUI
Elapsed time is 0.076921 seconds.
fx >>
```

Figure 7. Browse downloaded decoded image for apply Decryption process

Description 7.6 This figure shows that the encrypted image is uploading on social site. Now we get the original image by click on “Decrypted Image” button shown in following figure.



```
function varar
% DECODERGUI M
%      DECODER
%      singlet
%
%      H = DEC
%      the exi
%
%      DECODER
%      functic
%
%      DECODER
%      existin
%      applied
%      unrecog
%      stop.  All inputs are passed to DecoderGUI_OpeningFcn via varargin.
%
```

```
Elapsed time is 0.057934 seconds.
Elapsed time is 0.057803 seconds.
>> ImageEncryptionGui
Elapsed time is 0.077343 seconds.
>> DecoderGUI
Elapsed time is 0.076921 seconds.
fx >>
```

Figure 8.Image received after Decryption

Description 7.7 This figure shows to get original image by click on “Decrypted Image” button.

VIII. CONCLUSION

Image Encryption is an algorithm for the linking and retrieval of digital keys, which can be used as a method for the secure management of cryptographic keys. In this paper, a cryptography and steganography methods have proposed for providing better security of data in a network environment. With system that we have proposed data can be transferred between sender and receiver via unsecured network environment. Obviously, in a network environment this system is one of the best ways of hiding the secret of message from intruders. The main focus of the paper is to develop a system with extra security features. The convenience and security provided by Image Encryption will undoubtedly help to promote more widespread use of cryptographic systems.

FUTURE SCOPE

The research work did on the surface of racing tracking can be further modifying in different ways as following:

- The dataset can be changed in future for other encryption.
- The technique used for this work can be enhanced as other encryption technique.
- This work can be used to make cipher text for any other type of data other than image.

REFERENCES

[1]. S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, “Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications,” Vehicular Communications, vol. 28, no. 1, Article ID 100306, 2021. View at: Publisher Site | Google Scholar

[2]. G. M. Kiran and N. Nalini, “Enhanced security-aware technique and ontology data access control in cloud computing,” International Journal of Communication Systems, vol. 33, no. 23, Article ID e4554, 2020. View at: Publisher Site | Google Scholar

[3]. A. Ramamoorthy and P. Jayagowri, “A secure public key cryptosystem based medical records using non-commutative group,” Journal of Physics: Conference Series, vol. 1964, no. 2, Article ID 022011, 2021.View at: Publisher Site | Google Scholar

[4]. F. Ramzan, S. Klees, A. O. Schmitt, D. Cavero, and M. Gultas, “Identification of age-specific and common key regulatory mechanisms governing eggshell strength in chicken using random forests,” Genes, vol. 11, no. 4, p. 464, 2020. View at: Publisher Site | Google Scholar

[5]. G. Qiu, C. Wang, S. Luo, and W. Xu, “A Dual Dynamic Key Chaotic Encryption System for Industrial Cyber-Physical Systems,” IEICE Electronics Express, vol. 17, no. 24, 2020. View at: Google Scholar

[6]. M. Arun, S. Praveenkumar, P. S. Rajakumar, and P. Thamizhikkavi, “Cbca: consignment based communal authentication and encryption scheme for internet of things using digital signature algorithm,” IOP Conference Series: Materials Science and Engineering, vol. 1074, no. 1, Article ID 012003, p. 16, 2021. View at: Publisher Site | Google Scholar

[7]. Iwase, L. Pusztai, K. Blenman et al., “Validation of an immunomodulatory gene signature algorithm to predict response to neoadjuvant immunochemotherapy in patients with primary triple-negative breast cancer,” Journal of Clinical Oncology, vol. 38, no. 15, p. 3117, 2020.

[8]. Pia Singh et al "Image Encryption and Decryption Using Blowfish Algorithm in Matlab," International Journal of Scientific & Engineering Research, vol. 4, Issue. 7, July 2013

[9]. Vishwagupta, Gajendra Singh ,Ravindra Gupta,–Advance cryptography algorithm for improving data security‖, International Journal of Advanced Research in Computer Scienceand Software Engineering, Volume 2, Issue 1, January 2012

[10]. P. S. Ghode, –A Keyless approach to Lossless Image Encryption‖, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE.), vol. 4, Issue. 5, pp. 1459- 1467, May 2014.

[11]. D. Reshetnikova and P. D. Dunaev, “Academician andrei dmitrievich ado and the kazan scientific research institute of epidemiology and microbiology,” Kazan medical journal, vol. 102, no. 1, pp. 115–122, 2021. View at: Publisher Site | Google Scholar

[12]. P. Amudha, J. Jayapriya, and J. Gowri, “An algorithmic approach for encryption using graph labeling,” Journal of Physics: Conference Series, vol. 1770, no. 1, Article ID 012072, p. 9, 2021. View at: Publisher Site | Google Scholar

[13]. R. E. Christenson and M. J. Harris, “Real-time hybrid simulation using analogue electronic computer technology,” International Journal of Lifecycle Performance Engineering, vol. 4, no. 1/2/3, p. 25, 2020. View at: Publisher Site | Google Scholar