IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 3, Ser. I (May – June 2021), PP 58-69
www.iosrjournals.org

Software to increase Data Security using Cryptographic Algorithms

Ashish Chauhan, Aayush Mishra, Ayushi Vashist
Assistant Professor Department of Information Technology, SRM Institute of Science and Technology
B.Tech Scholar Department of Computer Science and Engineering, SRM Institute of Science and Technology
B.Tech Scholar Department of Computer Science and Engineering, SRM Institute of Science and Technology

Abstract: *Encryption is a technique used to convert readable data into an unreadable form it is widely used in securing data leaks and data integrity from unauthorized, malicious cyber-attacks. Encryption is achieved by passing the data through various steps which is called an encryption algorithm and changing the format of data from readable to unreadable format which can be accessed only with a specific key. For ensuring the confidentiality and the integrity of the data, this project uses various cryptographic algorithms that are strategically implemented throughout the software. The prime motive of this project is to provide users with a platform where an additional level of security can be added by using integrated encryption and decryption techniques to ensure data security of user data at a user level.*

Keywords*: Encryption, Algorithm, Decryption, Key, Visual Cryptography, Password Generator*

Date of Submission: 25-05-2021 Date of Acceptance: 09-06-2021

I. Introduction

As the world is moving forward more towards economy and technology. The primal instinct of security also needs to be updated to deal with the advancing threats. Whether it is an organization or a private entity, the confidentiality and the integrity of the information is a vital asset. Thus the necessity of data security arises for safeguarding personal or organizational or corporate assets. The failure in securing data leads to critical data leaks which may further inflict vital damage-causing financial loss, security breach, and can also breach the personal space of an individual. Security of data is more critical when the data is meant to be shared with multiple entities. Encryption and Decryption methods are used to cipher and decipher data which is done by using the right set of encryption keys and methods. The access to the key is with the authorized user to ensure data security.

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

Image encryption requires certain characteristics like mass data capacity and high data redundancy. For the image encryption, the input image is split up into small blocks, approximately of size 8x8. After that, the blocks are shuffled and processed resulting in the generation of a random 2D image map. This encryption makes the decryption more complicated and secure so that 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 in higher security and greater resistance to the attack.

The Confidentiality and the integrity of the data is at stake at two points-

1- When the data is stored in a system and an unauthorized user access the data

2- When the data is being transferred and the transmission is breached.

At a user level, a user uses a password as the only tool to ensure the security of the data.

This project provides an additional layer of security by Combining visual cryptography, cryptography, and password generating system into simple, user-friendly software to ensure secure transmission of data. This incorporates a combination of modern and classical cryptographic algorithms classified by the level of security that they provide which empowering the user with the tools to manage and advance their data security.

II. Literature Survey

Many research works have been carried out and several encryption and decryption methods have been developed to achieve the maximum level of security when it comes to ensuring data security to avoid the access of unauthorized users and making the data non-vulnerable to attacks.

[1] "A Symmetric key cryptographic Algorithm" (2010)
This paper discusses a comparative study of Symmetric Key and Asymmetric Key Cryptography methods and invented a new algorithm to encrypt small amount of data. It concludes that Asymmetric Key provides more security with less time efficiency. On the other hand, Symmetric method is efficient for encrypting bulk of data.
[2] "A Study of Encryption Algorithms AES, DES and RSA for Security" (2013)
This paper put emphasis on need of encryption for securing data. It comprises of three techniques-DES, AES and RSA along with their comparison based on time taken and efficiency of each one of these. Based on experimental results, AES is found to be better than DES and RSA.
[3] "Cryptography Algorithms: A Review" (2014)
This paper consists of analysis of various symmetric key algorithms like DES, Triple- DES, Blowfish, AES and asymmetric key algorithm like RSA. Blowfish has better performance and efficiency. RSA algorithm is most secure and widely used.
[4] **"**Alpha-Numerical Random Password Generator for Safeguarding the Data Assets" (2014)
This paper encourages the use of random numeric password that are less vulnerable to attacks .Passwords should be strong enough so that security is not compromised. Also, the passwords should be stored in encrypted form. It proposed a password generation mechanism that can be used in practice
[5] "A Secure and Fast Approach for Encryption and Decryption of Message Communication"(2017)
This paper discusses about various data security standards and parameters like flexibility, scalability, architecture used to evaluate it. It also proposed a approach foe encrypting and decrypting small amount of data with the purpose of reducing time and increasing effectiveness of the model.
[6] "Image Encryption for Secure Internet Transfer" (2020)
This paper involves the usage of combination of AES and RSA for image encryption and decryption. It focuses on need of method to increase image security by double encryption and transmission such that risks of attacks can be minimized. The decrypted output image is accurately colored image. Hence, the method is effective.

III. Methodology

In this project, we have used java to provide a platform for this software for the basic encryption and decryption process of the text as well as the image that has to be encrypted/decrypted for secure transmission.
At first, the user can choose any of the four options as per the need-

1.Text Cipher
2.Text Decipher
3.Image Encryption/Decryption
4.Password Generator

- **Text Encryption**- To change the data from Plain text to Cipher-text using a key.

For this, select Text Cipher option from the main menu-

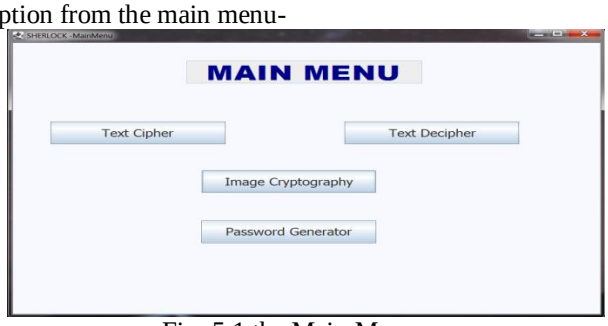

Fig: 5.1 the Main Menu

Then, select the level of security needed-

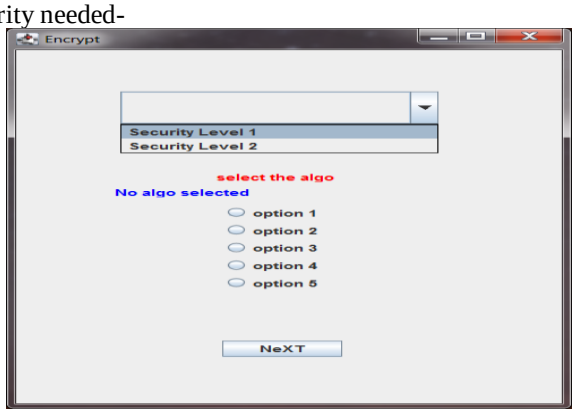

Fig: 5.2 Main Menu-Text Encrypt

Then, select the appropriate algorithm as per requirement from Security Level 1 Cipher-

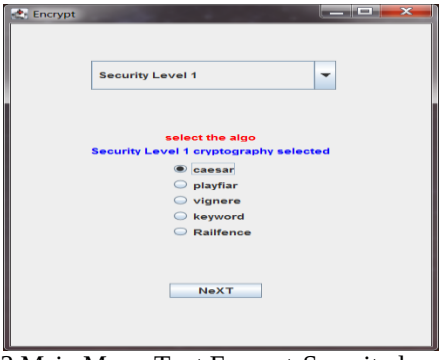

Fig: 5.3 Main Menu-Text Encrypt-Security level 1

Fig: 5.4 Main Menu-Text Encrypt-Security level 1

Now, Enter the plain text and the key then press ENCRYPT Button.

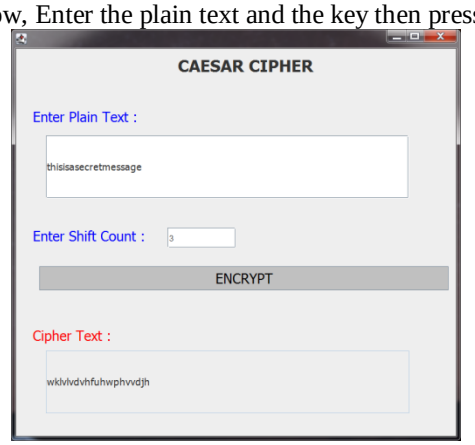

Fig: 5.5 Text Encrypt-Security level 1-Caesar Cipher

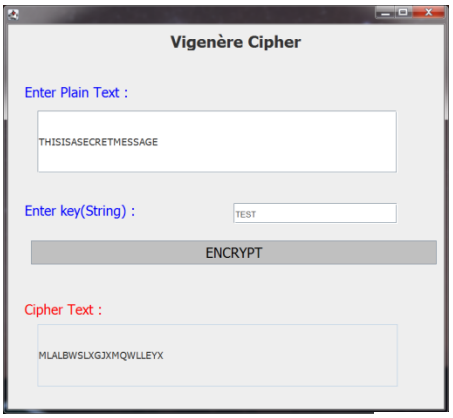

Fig:5.6 Text Encrypt-Security level 1-Vigenère Cipher

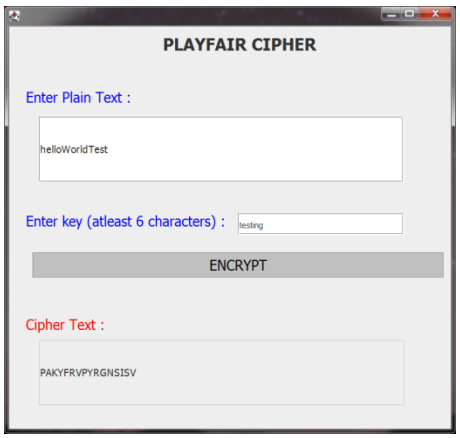

Fig: 5.7 Text Encrypt-Security level 1-Playfair Cipher

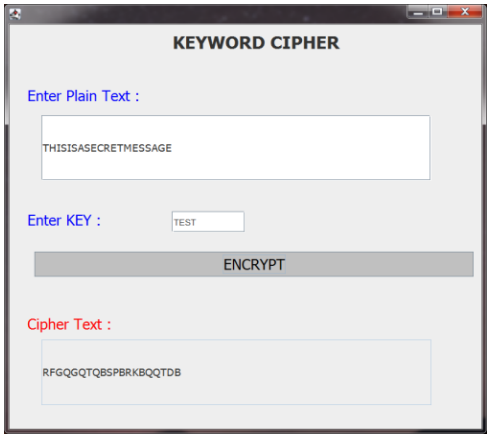

Fig: 5.8 Text Encrypt-Security level 1-Keyword Cipher

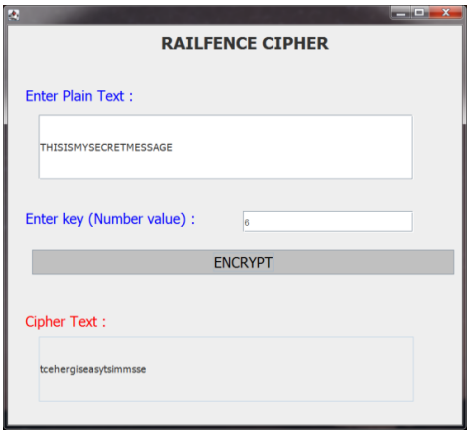

Fig: 5.9 Text Encrypt-Security level 1-Rail Fence Cipher

Following algorithms are used for enabling Level 1 of Security:

1. Caesar Cipher- It is a kind of Substitution cipher method in which plain text is simply shifted by a particular shift-count (key) to give the ciphertext.
2. Vigenère Cipher- It falls under the category of polyalphabetic substitution Cipher method. The User inputs a keyword, which is then repeated in a circular manner to match plain text length. Then corresponding Characters of plain text and keyword are added and the sum is modulus by 26 to get the required ciphertext.
3. Playfair Cipher-It is a digraph Substitution Cipher method. It uses the key to generate a table of 5*5 in which initial entries are unique key alphabets followed by remaining letters in order. Plain text is divided into pairs which then are converted to ciphertext with help of the Key table.
4. Keyword Cipher- It falls under the category of monoalphabetic substitution Cipher method. In this substitution alphabet corresponding to the plain text is found with help of a given keyword, which results in ciphertext.
5. Rail Fence Cipher-It is the kind of transposition cipher i.e. it jumbles up the given plain text. It uses the key to determine the number of levels of zigzag. Then, it generates a table that contains plain text written in zigzag form along with a path. The Cipher Text is read row-wise.

Fig: 5.9 Text Encrypt-Blowfish Cipher

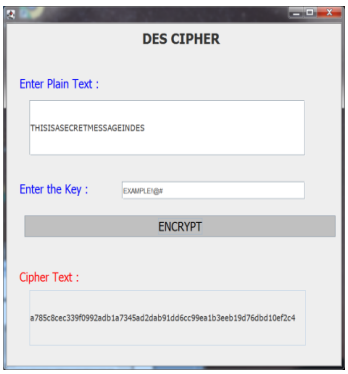

Fig: 5.10 Text Encrypt-DES Cipher

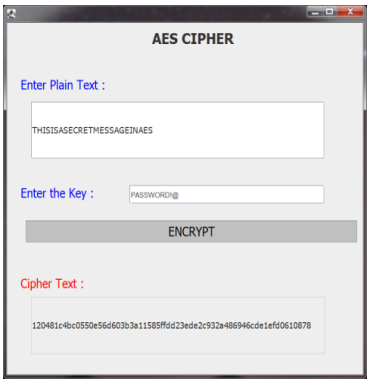

Fig: 5.11 Text Encrypt-AES Cipher

Fig: 5.12 SHA-512 Hashing

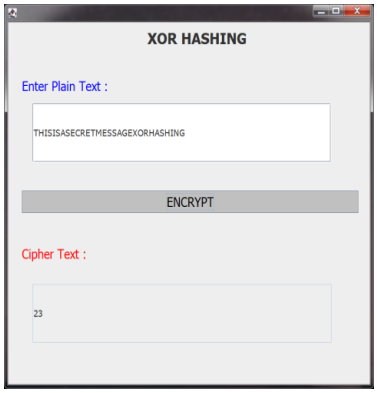

Fig: 5.13 XOR Hashing

Following algorithms are used for enabling Security Level 2:

1. Blowfish Cipher -Blowfish is a Symmetric cryptography algorithm. It has 16 rounds and a 64-bit block size. It makes use of two sub-arrays- the P-array and S-boxes for key broadening and encryption process. The S-box generates a 32-bit output value. One value from the P-array is used in every round. Blowfish's algorithm divides the 32-bit input into four parts and uses them as input to the S-boxes.
2. DES Cipher- Data Encryption Standard is a Symmetric block Cipher technique, which implies that one key is employed for both encryption and decryption process. It takes plaintext in the block size of 64 bits and converts to ciphertext blocks of the same size with help of keys of 56 bits. Firstly, initial permutation is carried out on the plain text, which gives two parts of the permuted block, which undergoes 16 rounds of the encryption and both are recombined and final permutation is performed. The result is 64-bit ciphertext blocks.

3. AES Cipher- Advanced Encryption Standard is drawn on the network of Substitution-Permutation. It ensures efficient performance compared to DES or 3DES. Its block size is of 128 bits. It has 10 rounds for a key size 128-bit. Key size can vary as 128,192,256 bits. Each round enforces the same function to the given block. Each round includes the following steps- substitution, shift rows, column-mixing, and round key addition.

4. XOR Hashing- it is an 8 -bit checksum that XOR on all bytes. XOR "exclusive or" is a bitwise (and logical) operation that outputs 1 (true) if the two inputs are not the same and output 0 (false) if the two inputs are the same. a numerical output is generated which can be used to verify data integrity. It can be called the digital signature of the data.

5. SHA-512 Hashing- The Secure Hash Algorithm - 512 -encryption is based on the previous version SHA-256, except the fact that it produces a 512-bit numeric output- 128 hexadecimal characters. Block size is 1024 bits. The number of rounds in the process is 80. This hash algorithm is dependent on a non-linear function, to prevent any decryption method to crack it. It is diversely used nowadays such as in internet security, digital certificates, and even blockchains.

- **Text Decryption-** Converting cipher text back to plain text (readable form)
  Select the Text Decipher option from the main menu
  Select the level of security -1 or 2.
  Select algorithm to decipher
  Enter ciphertext to decipher

Following are snippets of Level 1 Decipher option -

Fig: 5.14 Text Decrypt-Caesar Decipher

Fig: 5.15 Text Decrypt- Playfair Decipher

Fig: 5.16 Text Decrypt-Vigenère Decipher

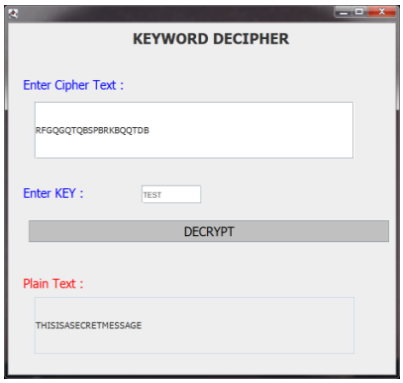

Fig: 5.17 Text Decrypt-Keyword Decipher

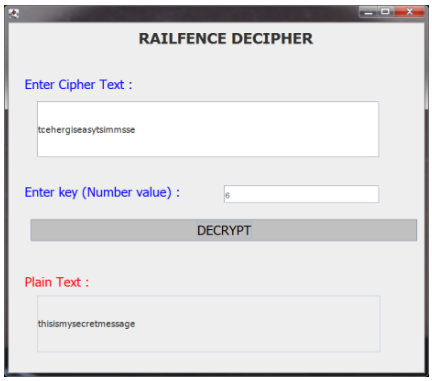

Fig: 5.18 Text Decrypt- Railfence Decipher

Following are snippets of Level 2 Decipher option -

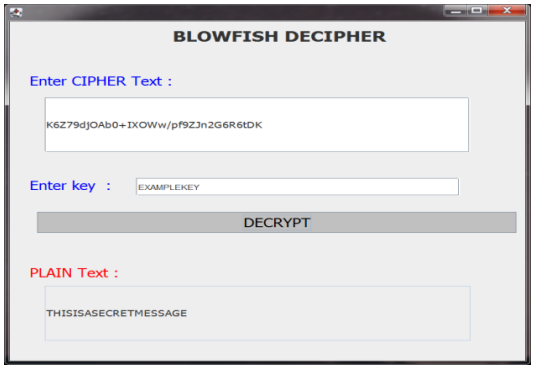

Fig: 5.19 Text Decrypt-Blowfish Decipher

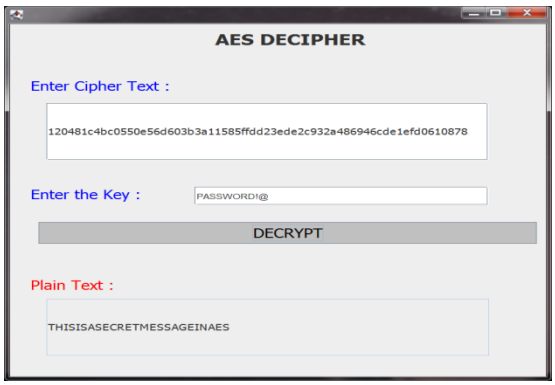

Fig: 5.20 Text Decrypt-AES Decipher

Fig: 5.21 Text Decrypt-AES Decipher

- **Image Encryption/Decryption**- Converting input image to an encrypted image to secure contents of the original image.

Select Image Encryption/Decryption from the main menu

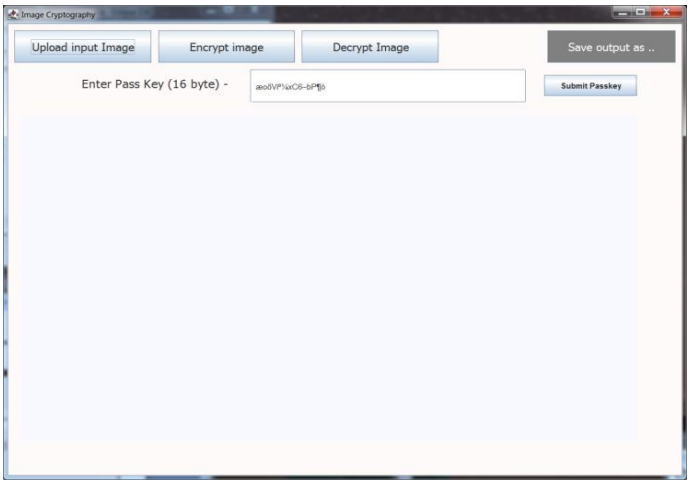

Fig: 5.21 Main Menu-Image Encryption/Decryption

Upload the image

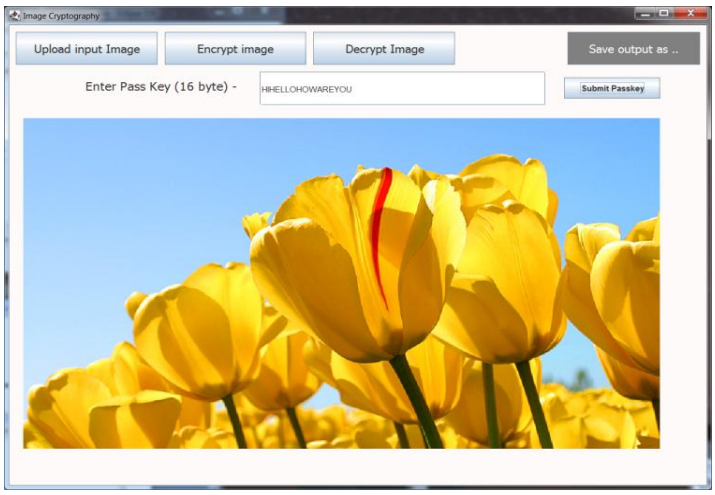

Fig: 5.22 Image Upload

Select Encrypt image/Decrypt image by clicking on respective buttons.
Single encryption

Fig: 5.23 Single Encryption of image

Fig: 5.24 Triple Encryption of image

Multiple encryption: multiple layers of encryption process i.e. Encrypting the cipherimage again by treating it as original image to make sure higher level of security.

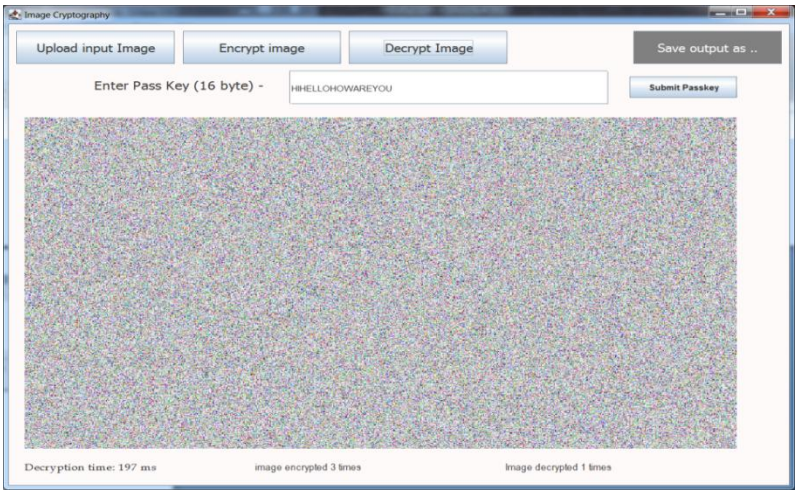

Fig: 5.25 Single Decryption of image

Image decryption

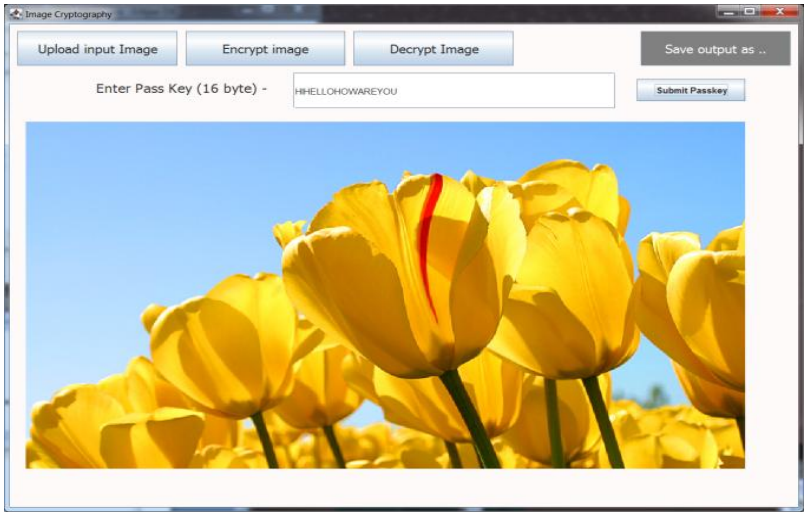

Fig: 5.26 Output image after Decryption

Image decryption output

- **Password generator-**

Select password generator option from the main menu.

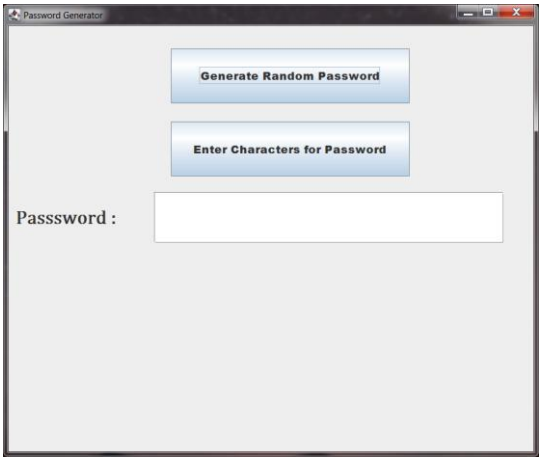

Fig: 5.27 Password Generator

Select "Generate Random Password" for Auto password generator

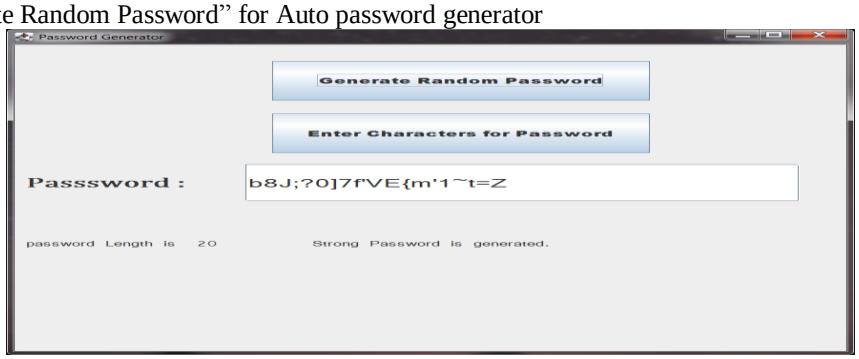

Fig: 5.28 Generate random password

Select "Enter Character For Password" for user specific password

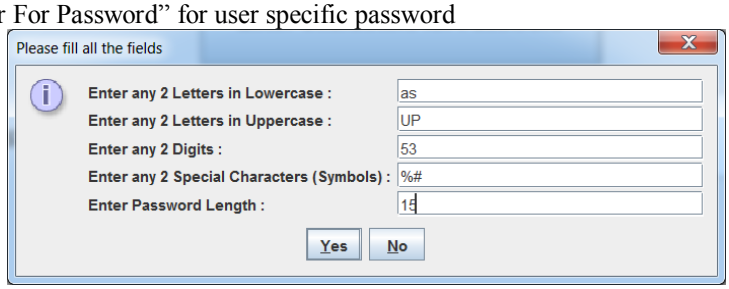

Fig: 5.29 Enter Characters for password

Accept the confirmation and the Output is-

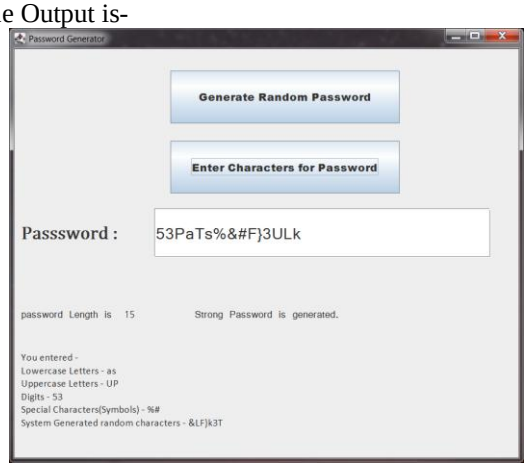

Fig: 5.30 User password generated

IV. Technique Description

- Cryptography

1. Encryption- The process of converting Plain Text into ciphertext using cryptographic Algorithms
2. Decryption- The process of decoding the ciphertext back to Plain Text with an authorized key.

- Visual Cryptography

1. Image Encryption- Converting the input image into a different image by changing the pattern of the pixels
2. Image Decryption- Fetching the actual image from the encrypted image.

- Password Generator

It generates a Random Password using - uppercase/lowercase/Numeric value/Special Characters based on user preferences and the level of difficulty. It can also generate random passwords. This Combination will make the password strong and less susceptible to Brute Force techniques.

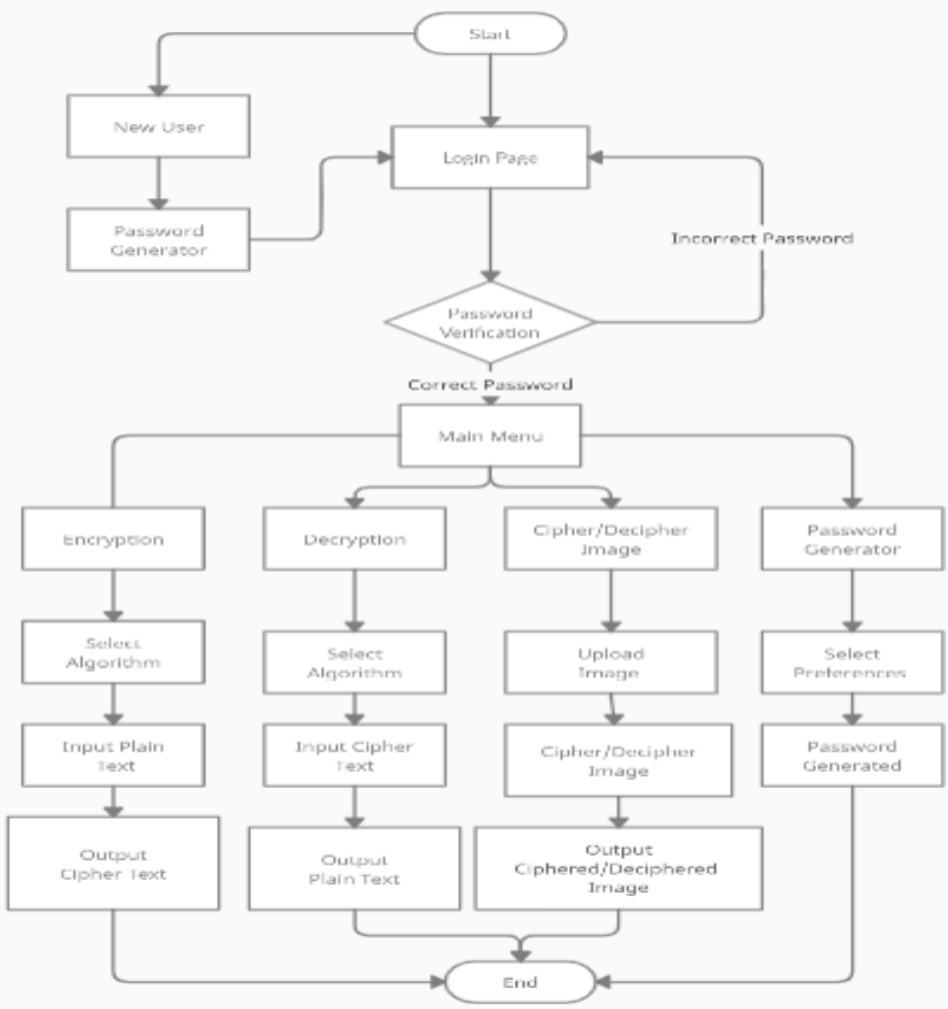

Fig: 5.30 Flowchart of the System

V. Technique Implementation

Illustration of the Steps:

- **Encryption/Decryption**

1. Login
2. Enter the main menu
3. Select Encryption/Decryption
4. Select the required algorithm
5. Input plain Text/ Input cipher Text
6. Enter the key
7. Output plain/Cipher text is displayed.

- **Image Encryption/Decryption**

1. Login
2. Enter the main menu
3. Upload Original/Cipher Image
4. Select Image Encryption/Decryption
5. Enter the key
6. Save the Cipher/Original image

- **Password Generator**

1. Login
2. Enter the main menu
3. Enter Password Generator
4. Input preferred Characters from the provided options
5. Get strong random generated password as output.

VI. Experimental results

The java code was written, executed ,and tested several times in to find the correct result and the experimental results were analyzed several times to remove the bugs.

The java code was tested using various images/texts of different sizes, and it was found out to be exactly matching the original input image. Time taken by the encryption and decryption for different sizes of the image was measured. Depending on the size of the image, the time taken for the same may vary accordingly.

Multiple image Encryption i.e. Taking the cipher image of the Encrypted image and Encrypting it 'n' number of times" to make it more secure was tested and the result was found to be accurate and the original image can be decrypted after decrypting 'n' number of times.

VII. Results Discussion

The results of the experimental tests that were done are

1. The results of the encryption/decryption process of text/image are accurate and efficient.
2. Encryption/Decryption of images can be done n-number of times and it gives appropriate output.
3. The integrity of the results were checked and found to be accurate.
4. Password generator provides the desired output as a strong password.
5. The proposed technique will exponentially increase the data security.

VIII. Conclusion

With the increasing growth of technology the means of securing our assets needs to be up to date to avoid any unauthorized access or invasion of privacy. This software gives excellent results in this purpose, alongside it is capable to enforce another further level of security to the user data. The multiple-image encryption method yields a higher level of security. The main purpose of empowering a user with tools of cryptography to ensure the user has the means to add desired security to their data –text, as well as image, can be achieved with this software.

References

[1]. Prof ZiadAlQadi,"A Highly Secure And Accurate Method for RGB ImageEncryption",2020.
[2]. AshutoshShukla,JayShah,NikhilPrabhu,"Image Encryption Using Elliptical CurveCryptography",2013.
[3]. Mohamad M Al-Laham,"Encryption-Decryption RGB Color Image Using MatrixMultiplication,2015.
[4]. A.Sathishkumar, K. Bhoopathybagan and N. Sriraam "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network Security & its Applications, Vol. 3, No. 2, pp181-194,2011.
[5].]. G A.Sathishkumar, K. Bhoopathybagan and N. Sriraam "Image encryption based on diffusion and multiple chaotic maps", International Journal of Network Security & its Applications, Vol. 3, No. 2, pp181-194, 2011.
[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, November,2016.
[7]. Ziadalqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, v. 2, issue 4, pp. 288-298,2007.
[8]. Mohammed AbuzalataJamil 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]. 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 May,2018.
[10]. KundankumarRameshwarSaraf,VishalPrakashJagtap, 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.
[11]. William Stallings "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011.
[12]. Ayushi "A Symmetric Key Cryptographic Algorithm" ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15

[13]. Dr. Prerna Mahajan & Abhishek Sachdeva" A Study of Encryption Algorithms AES, DES and RSA for Security" Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc. (USA) Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

[14]. Anjula Gupta & Navpreet Kaur Walia "Cryptography Algorithms: A Review" © 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939

[15]. Sandanasamy &. D. Muthulakshmi "Alpha-Numerical Random Password Generator for Safeguarding the Data Assets" International Journal of Engineering Research & Technology (IJERT) IJERT ISSN: 2278-0181 IJERTV3IS120404 www.ijert.org Vol. 3 Issue 12, December-2014

[16]. Ekta Agrawal , Dr. Parashu Ram Pal "A Secure and Fast Approach for Encryption and Decryption of Message Communication" Volume 7 Issue No.5 ISSN 2321 3361 © 2017 IJESC

[17]. Ashish Chauhan, CharviMinocha, Karan Bhandari, Akshara Pathak "Image Encryption for Secure Internet Transfer" 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

Ashish Chauhan, et. al. "Software to increase Data Security using Cryptographic Algorithms." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 23(3), 2021, pp. 58-69.