

A Project/Dissertation Review-1 Report

on

Encrypto

Submitted in partial fulfillment of the
requirement for the award of the degree of

B.Tech CSE



Under The Supervision of

Mr. Shubham Kumar

Department of Computer Science and Engineering

Submitted By

Name - **Md Noman Khan**

Admission No. - **19SCSE1010168**

Group no. - BT3041

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA INDIA
DECEMBER- 2021



SCHOOL OF COMPUTING SCIENCE AND
ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA

CANDIDATE'S DECLARATION

I/We hereby certify that the work which is being presented in the project, entitled "Encrypto " in partial fulfillment of the requirements for the award of the BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING submitted in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an original work carried out during the period of JULY-2021 to DECEMBER-2021, under the supervision of MS. PUNEETA SINGH , Assistant Professor, Department of Computer Science and Engineering of School of Computing Science and Engineering , Galgotias University, Greater Noida

The matter presented in the project has not been submitted by me/us for the award of any other degree of this or any other places.

19SCSE1010168- Md Noman Khan

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Supervisor Signature

CERTIFICATE

The Final Thesis/Project/ Dissertation Viva-Voce examination of Md Noman Khan - 19SCSE1010168 has been held on _____ and his/her work is recommended for the award of BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING.

Signature of Examiner(s) Signature of Supervisor(s)

Signature of Project Coordinator Signature of Dean

Date:

Place:

Abstract

Phone calls, emails, online shopping, social media, and browsing in general are online activities that we can no longer live on. While we constantly search or share information online, our data is basically stored somewhere. Most people are not sure where that "place" is, but this information should only be available to the service provider that is handling your call. However, it could be visible to the telecommunications companies transporting your Internet packages and your supposedly private and secure communications could be intercepted. As many cases have shown, corporate and user data is increasingly targeted by hackers and cybercriminals, leading to data breaches and targeted attacks. This reason alone should serve as a warning to all those who have not thought of protecting their communications with encryption.

Encrypto is an app which hides and retrieves encrypted text data in image. It basically is an implementation of steganography using AES encryption.

Encrypto can hide the text given in the provided image and that image user can send to anyone freely. The same image can be decrypted and data/text can be retrieved from it using this app.

This app is build in android using certain components of cybersecurity. We have used AES encryption , steganography and Feistel **cipher** .

After building this app we can embed any given image with a message or text that will only be decoded at the client's side without any breach. Thus , this app can be very useful in easily being used to send private/ secret messages without any information leak , that will fit in amazingly in this breachful era.

Table of Contents

Title	Page No.
Chapter 1 - Introduction	
Chapter 2 - Literature Survey/Project Design	
Chapter 3 - Functionality and working of the project	
Chapter 4 - Results and Discussions	
Chapter 5 - Conclusion and Future Scope	
References and acknowledgement and publications	

CHAPTER-1

Introduction

Encryption increases the security of a message or file by encrypting its content. To encrypt a message, you need the correct key, and you also need the correct key to decrypt it. It is the most efficient way to hide communications using encrypted information where the sender and recipient have the key to decrypt the data. The concept is not that different from children inventing secret keywords and other discrete channels of communication where only they can understand the message. Encryption is like sending secret messages between parties: if someone tries to decrypt it without the correct keys, they will not be able to understand the message.

Encrypto is an app which hides and retrieves encrypted text data in image. It basically is an implementation of steganography using AES encryption.

Encrypto can hide the text given in the provided image and that image user can send to anyone freely. The same image can be decrypted and data/text can be retrieved from it using this app.

The Advanced Encryption Standard (AES) is a symmetric block cipher . AES is carried out in software programs and hardware at some stage in the sector to encrypt sensitive information. It is important for authorities pc security, cybersecurity and digital information protection.

Steganography is the technique of hiding secret information in an ordinary, non-secret file or message to avoid discovery; secret data is then extracted at its destination. The use of steganography can be combined with encryption as an additional step to hide or protect data

In the current era of the digital world, secure information transmission becomes a greater challenging task. Cryptography is a way to defend the safety of the data and this makes use of encryption and decryption processes to maintain the message secret this means that Secret writing. However unauthorized people can get entry to the data with the aid of changing the data to be transmitted to conquer this problem steganography is used . Steganography is derived from the Greek phrase steganos which means “Covered” and graphy means “Writing”, i.e. covered writing .

The basic concept behind steganography is hiding the name of the game information in a few gadgets. Steganography makes use of distinct kinds of gadgets to hide the information like pictures, audio, and video. The most famous one is picture steganography because of their frequency on the internet. Image steganography techniques work on two distinct domains like area area additionally referred to as pixel area in which steganography operation without delay is accomplished at the pixel and rework area, in which message embedding is accomplished in the converted picture.

The item that is used to cowl the name of the game data is referred to as cowl picture when the primarily based total compression of picture cowl picture is divided into lossy and lossless compression. Lossy compression is greater famous at the internet site due to Very small report sizes and masses of tools, plugins, and software program aid it however as soon as the picture is compressed it can't get back to the unique picture which results in information loss on each compression picture will lose its unique photo first-rate. With 50% compression carried out, picture report length reduced with the aid of using 90%. With 80% compression carried out, picture report length reduced with the aid of using 95%. e.g. like JPEG pictures.

In lossless compression, the compressed picture will in no way lose their information and barely reduced in picture report length it continues the equal photo first-rate of the unique picture. E.g. BMP, GIF, and PNG. JPEG spatial picture information transforms into the frequency area and is subjected to lossy compression, on each compression process the picture loses its information and adds an excessive amount of noise in it. When the picture is transformed back to the spatial area it will be very hard to detect the error using error correction coding. Hence, it was concluded that steganography could now no longer be possible in JPEG images. The algorithms which might be used to conquer this problem are very complicated. Whereas for a PNG and BMP picture a simple LSB is relevant with no lack of information on compression. Also, they each fair nearly equal in terms of storing ability and picture first-rate of the very last picture. Lossy compressed images are complicated for steganography processes; it needs an extra compression algorithm to maintain the integrity of the information in which lossless pictures are properly appropriate for stenography processes.

CHAPTER-2

Literature Survey

There might be projects that have aimed for the same thing which we are doing but the major difference between those projects and mine is that they have a large budget as well as a supportive environment . Some of the projects may have similar features but mine will be different for sure.

Through my project one can embed any form of text in any picture from their own gallery and even if they are texting or chatting on any public channel their message won't be sensed by anyone as it will be inside the picture which can be only be decrypted at the user end using a 16 digit unique key which is provided by the sender .

Existing Projects:

1. Stegais :

Stegais is another free steganography app for Android. Through this app, users can hide both text messages and voice messages inside a carrier image file. It also provides a password feature to protect output carrier files from unauthorized users. This app also allows users to *take images* and use them as the carrier image file. Plus, an option to use existing images of various formats as a carrier file is also present in it. Now, check out the below steps.

2. Steganography Master :

Steganography Master is a free steganography app for Android. Through this app, users can hide text information inside an image. Plus, it also offers a decoding tool to extract hidden text information from an image. It also supports multiple image formats that give users the flexibility to hide information in images of various formats such as PNG, JPG, BMP, ICO, etc. Now, follow the below steps to hide information in an image using this app.

3. **Image Steganography :**

Image Steganography is yet another free steganography app for Android. It is another easy-to-use steganography app that allows users to hide text information inside an image of various formats. Some of the image formats that it supports are JPG, PNG, and BMP. An inbuilt decode function to extract hidden information from a carrier image file is also present in it. Now, check out the below steps to hide text information inside an image using this app.

CHAPTER-3

Working and Functionality Of the App

Methodologies-

Encryption is the process of converting plain text data (plain text) into something that looks random and meaningless (ciphertext). Decryption is the process of converting ciphertext to plain text.

Symmetric encryption is used to encrypt more than a small amount of data. Symmetric keys are used in both encryption and decryption processes. To decrypt a particular ciphertext, you must use the key used to encrypt the data.

The purpose of the encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using a key. If a really good encryption algorithm is used, there is no better way than trying all possible keys systematically. For such an algorithm, the longer the key, the harder it is to decrypt the ciphertext without it.

It is difficult to judge the quality of the encryption algorithm. Algorithms that look promising can be very easy to decipher with proper attacks. When choosing an encryption algorithm, it is advisable to choose one that has been used for several years and has withstood all attacks.

Proposed Encryption and Decryption -

The purpose of the proposed system is to provide an efficient and easy way to transfer secret data over the communication channel by using the combination of steganography and cryptography methods where the encryption method gives extra security level to get the original data.

The proposed system has the following objective.

- Stego image is PNG image format which maintains data integrity.
- More security on data.
- Provides user-friendly application.
- Maintains good image quality.

Working (overview)

Encryption-

- Inputs-Key of 16 digits, Text (to be hidden), Image (in which text to be hidden)
- Text converted to byte array and fed to AES encryption using android encryption library.
- Encrypted text in form byte array converted to Base64 encoding
- Each chr of base64 string converted to binary value and combined as string with terminating string on both sides.
- The binary string is then inserted in the image using the LSB [method](#).
- The final image can be shared now.

Decryption-

- Inputs- Key of 16 digits(the same that used for encryption),Image(in which data is hidden)
- Binary data extracted from the pixels of the image just by reversing the LSB method process.
- Binary string converted back to base64 string and base64 string again decoded to byte array.
- Byte array feeds to the AES algo and by using the key the data is decrypted.
- The final Decrypted byte array is converted to text(utf-8) and displayed on screen.

Features

The android app lets you:

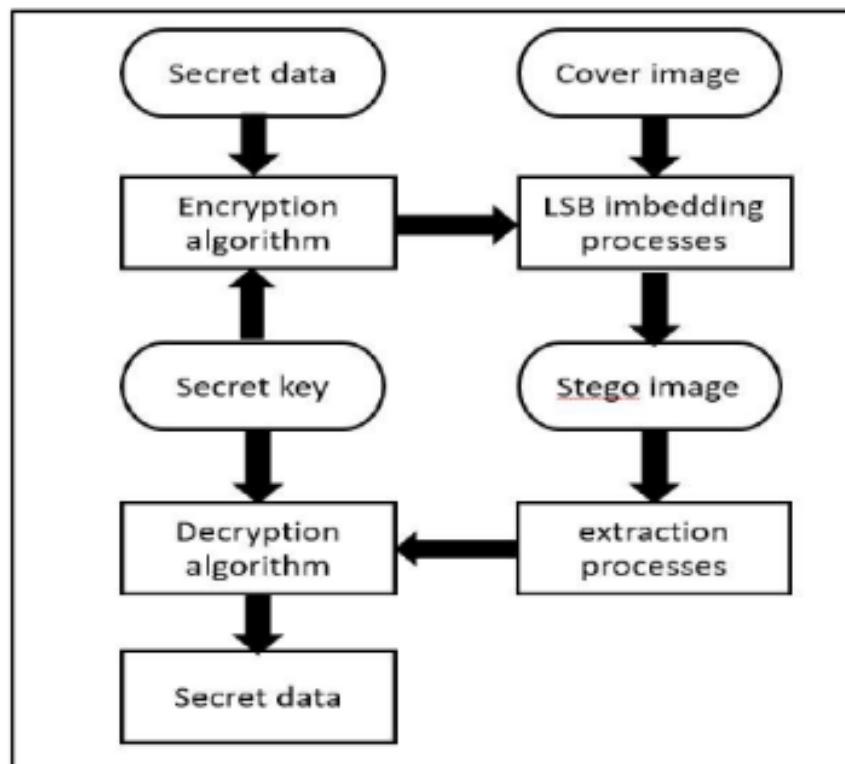
- Hide your secret text in any image.
- The image can be shared to anyone without other getting the hint about it
- The shared image can be decoded back to get the hidden text
- Can be used for both- fun or security purposes
- Service Provider Functions
- Key Generation and Exchange Functions
- Object Encoding and Decoding Functions
- Data Encryption and Decryption Functions

Total Design Idea

It is a proposed system where steganography is combined with a byte array. Hides secret data with steganography using the least significant bit (LSB) method

Image Base64 encryption method that encrypts secret data using encryption. The system proposed by has two phase encryption phase and decryption phase

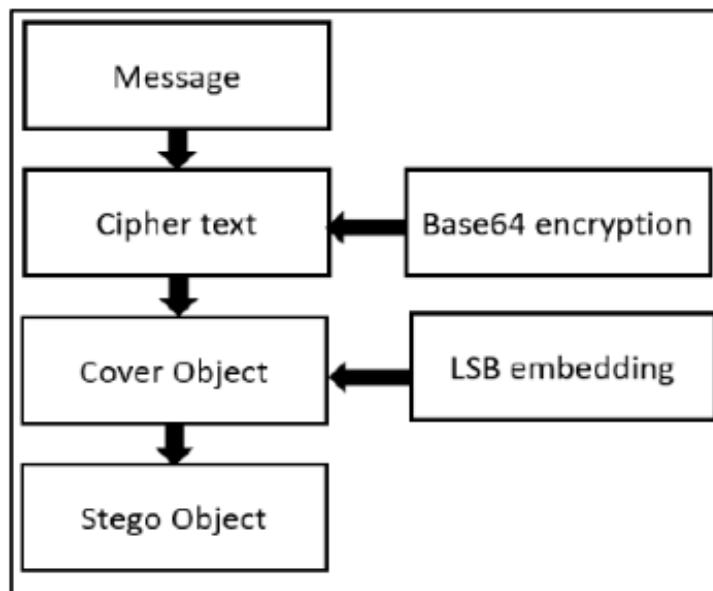
In the encryption phase , secret data is hidden in the image before it is embedded in the image. The image data is encrypted with ciphertext. In the decrypted phase, the data is first extracted from the image and then the ciphertext is converted to plain text. The image used to hide the data is called a cover object. Images with embedded data are called Stego objects.



Encryption and Embedding method.

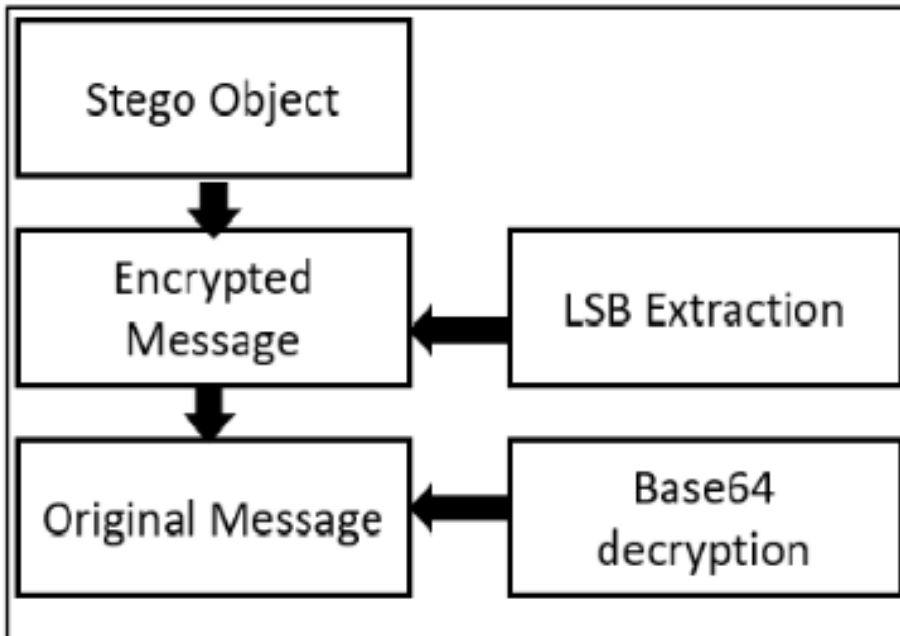
It is the encryption phase and embedding phase. This phase secret data is first encrypted with base64 method in clear text in format, secret information is converted to ASCII code then ,converts ASCII code to binary data, and binary data converts to ciphertext.

The ciphertext is now embedded in the cover object. Cover object can be any image type (e.g. JPEG, PNG, BMP) that forms a stego object using the LSB steganography process. Maintains data integrity.



Extraction and Decryption method.

Shows the Extract and Decrypt phases. In this phase, the first information in is extracted from . The Steak image extraction information is decrypted and returned to the original image.



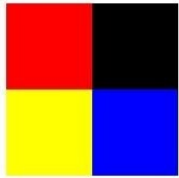
Implementation of Proposed Method

In steganography, image compression is a frequently used technique. Lossy compressed images (e.g., JPEG image format) do not maintain their original data when they are transmitted. Lossless compressed images (e.g., JPEG picture format) do. When attackers try to extract information from an image, they lose some critical data, whereas lossless compression protects all of the image's original data, hence lossless compression is used for LSB steganography (e.g., BMP, PNG, and GIF image format).

Steganography is integrated with cryptography in the suggested approach to increase the security of secret information. This technique ensures that a secret message is encrypted before being hidden in the cover image, so that even if hackers get the data from the cover image, they won't be able to access the encrypted data. This adds an extra layer of security, and it's done by employing efficient encryption and decryption techniques. algorithm. The proposed system employs two main technologies for secure data transmission: steganography, which embeds sensitive data in an image using the most widely used technique known as Least Significant Bit (LSB), and cryptography, which alters the meaning of a message using a cypher and method known as encryption.

Base64 is the planned system. An effective system is designed to convey secret data from the sender to receivers in such a way that the intruder is unaware of the information's existence. The Embedding function and the Extraction operations are the two aspects of the system design. Secret message encryption using base64 is used in the embedding function, and the encrypted data is subsequently hidden in the cover. The LSB method is being used to create an image. To construct a stego object, it ensures that encrypted data is integrated in the cover image. Extraction takes place in the second section of the system, where ciphertext is extracted from the stego object using the LSB technique and then decrypted to retrieve back the secret data in the reverse order of the base64 method.

Original Image



```
11111111 00000000
00000000 00000000
00000000 00000000

11111111 00000000
11111111 00000000
00000000 11111111
```

Least Significant Bit Steganography

Stego Image



```
11111101 00000011
00000010 00000001
00000000 00000010

11111100 00000011
11111101 00000001
00000001 11111100
```



c **a** **t**
01 10 00 11 01 10 00 01 01 11 01 00

C. Algorithm of the proposed system:

Algorithm to hide data into image:

Algorithm Hiding:

Input: CoverImage, SecreteMessage, SecreteKey

Output: StegoImage

Read the CoverImage, SecreteMessage, and SecreteKey

Ciphertext = Compress (SecreteKey, SecreteMessage)

 FindLSBs (CoverImage)

 While (CoverImage):

StegoImage = Embbed (Ciphertext into CoverImage)

 Return StegoImage

Algorithm to Unhide data from image:

Algorithm Unhiding:

Input: StegoImage, SecreteKey

Output: CoverImage, SecreteMessage

Read the StegoImage, and SecreteKey

If (SecreteKey == StegoImage(SecreteKey))

 FindLSBs (StegoImage)

 While (StegoImage):

CoverImage, SecreteMessage = Uncompressing
(StegoImage)

Return CoverImage, SecreteMessage

CHAPTER-4

RESULTS AND DISCUSSIONS






An android utility is designed to perform photo steganography processes. Select the cowl photo of any layout, input the mystery information and then give a mystery key for authentication purposes. First mystery information will be converted into ciphertext the usage of the Base64 encoding method then encoded text embedded into the cowl photo. Encoded images will get saved in the tool in.png layout to conquer the trouble of information loss. Now withinside the decode section pick the photo and input the equal mystery key to get right of entry to the name of the game information if the name of the game secret is the incorrect utility offers a message wrong key if secret is accurate mystery information might be displayed. The end result of the feature device is evaluated using three parameters Peak Signal to Noise Ratio, Mean Square Error (MSE) and Histogram.

Compression desk of PNG (portable community graphics) and JPEG (joint photographic expert group) photos are executed withinside the TABLE 1.

One withinside the above desk which tells that PNG photograph layout is nicely appropriate for LSB steganography techniques wherein it shops huge quantities of facts with excessive payload capacity, less distortion in the resulting photograph and low stego evaluation detection while as compared to JPEG photograph. Due to the free less compassionate nature of the JPEG photograph, it no longer keeps facts integrity. When it undergoes a few compression facts loss occurs to overcome this hassle; entropy encoding is used to provide stego photograph that's a totally complex compression technique to keep the facts integrity. Table 2 shows the comparison of the results obtained by the proposed method with PSNR and MSE .

Property Comparison of PNG and JPEG

PROPERTY	LSB in PNG	LSB in JPEG
VISIBILITY	LOW	LOW
INDEPENDENT OF FILE FORMAT	LOW	LOW
ROBUSTNESS AGAINST STATISTICAL ATTACK	LOW	MEDIUM
STEGO ANALYSIS DETECTION	LOW	MEDIUM
PAYLOAD CAPACITY	HIGH	MEDIUM
DATA CAPACITY	HIGH	LOW
EFFICIENT WHEN AMOUNT OF DATA REASONABLE	HIGH	MEDIUM
ROBUSTNESS AGAINST IMAGE MANIPULATION	LOW	MEDIUM
PERCENTAGE DISTORTION LESS RESULTANT IMAGE	HIGH	MEDIUM

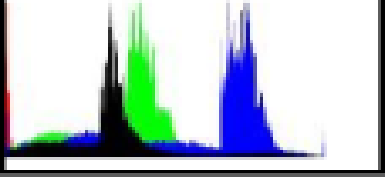
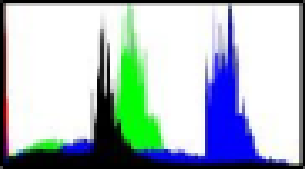
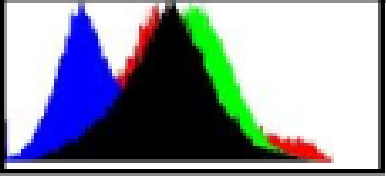
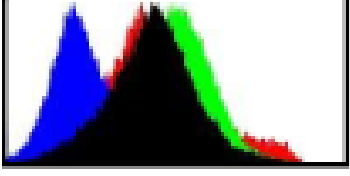
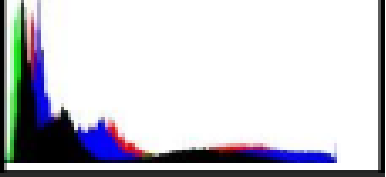
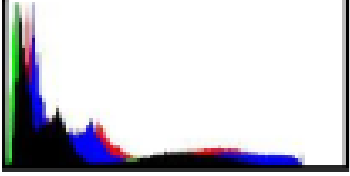


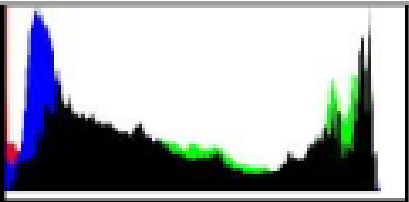
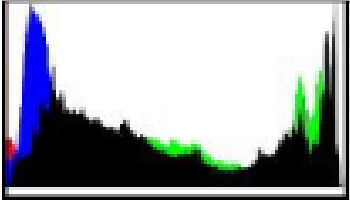
Sr. No	Cover Image(.Jpeg)	Proposed system		Existing system	
		PSNR	MSE	PSNR	MSE
1	 nature	75.56	0.0018	59.85	0.0677
2	 animal	73.54	0.0028	60.25	0.0617
3	 flower	79.85	0.00067	60.63	0.0567
4	 smiley	91.62	4.47	63.34	0.0303
5	 peacock	86.2	0.0015	62.21	0.0394

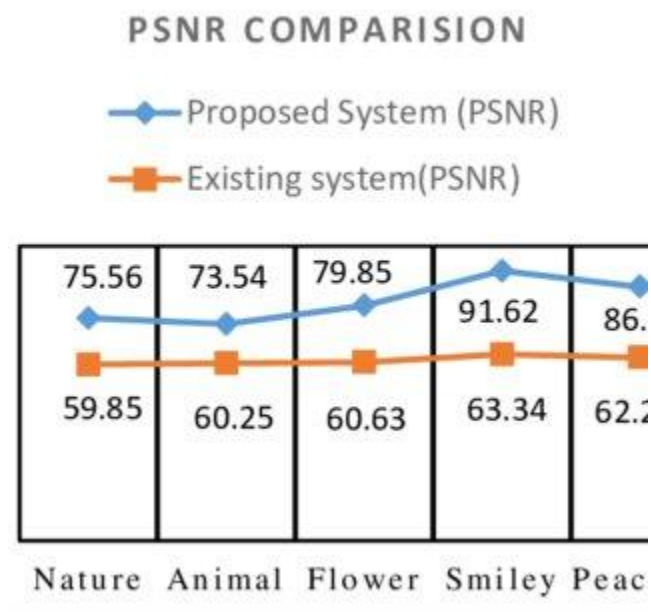
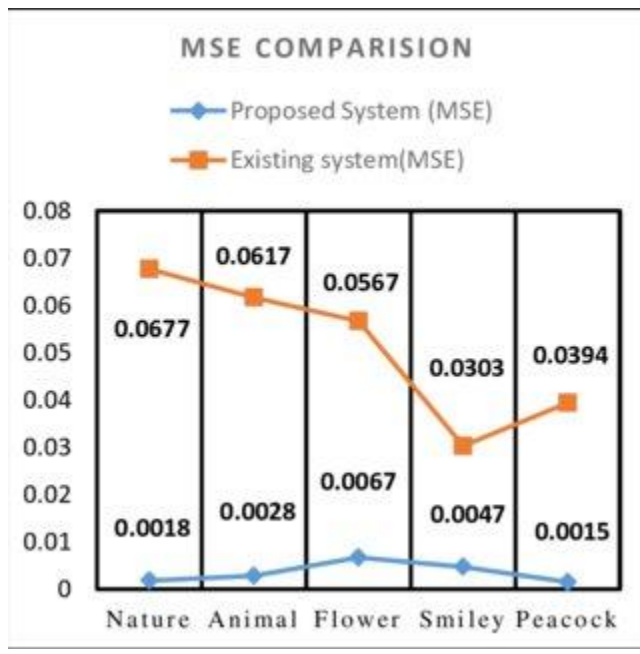
The photograph quality of an photograph is measured the use of top sign to noise ratio (PSNR) and suggest rectangular error (MSR) for stego photograph and cowl photograph and additionally histogram is used to measure the distortion of stego photograph and cowl photograph the use of the subsequent equations

$$\text{PSNR} = 20 \log_{10} \left(\frac{\text{MAX}_f}{\sqrt{\text{MSE}}} \right)$$

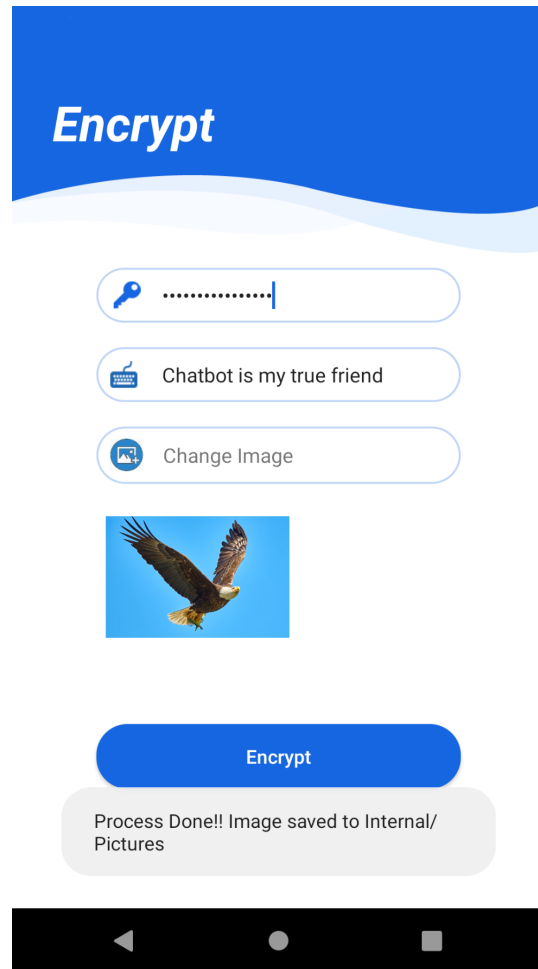
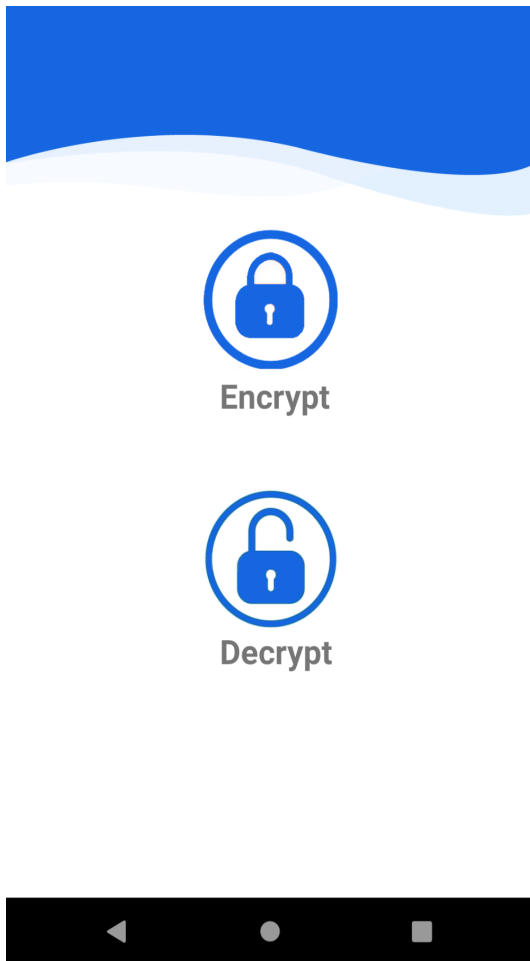
$$\text{MSR} = \frac{1}{mn} \sum_0^{m-1} \sum_0^{n-1} \|f(i, j) - g(i, j)\|^2$$

Mean square cost is calculated for the unique photograph and compressed photograph lesser the cost much less mistakes within side the photograph, that's an inverse relation among MSE and PSNR which means a higher cost of PSNR is properly because it means that the ratio of signal to noise is higher. MSR and PSNR values of the stego photograph and cowl photograph of a photograph and depth of the pictures is proven in Table 3.

Sl. No	Cover image	Stego image
1	 <p data-bbox="477 373 610 422">nature</p>	 <p data-bbox="948 407 1081 455">nature</p>
2	 <p data-bbox="477 646 610 695">animal</p>	 <p data-bbox="1023 646 1156 695">animal</p>
3	 <p data-bbox="477 900 610 949">flower</p>	 <p data-bbox="1023 900 1156 949">flower</p>
4	 <p data-bbox="477 1171 610 1220">smiley</p>	 <p data-bbox="1023 1171 1156 1220">smiley</p>
5	 <p data-bbox="477 1451 643 1499">peacock</p>	 <p data-bbox="1023 1451 1188 1499">peacock</p>



OUTPUT -



CHAPTER-5

CONCLUSION AND FUTURE WORK

In this study, steganography is blended with the Base64 encoding and decoding method for statistics protection purposes. An android software is constructed which is a fast, steady and user-pleasant interface to encode and decode images. To evaluate the performances of the proposed device PSNR and MSR, parameters are calculated. The result shows that the proposed device can store a greater quantity of mystery statistics at the same time as a stego photo is maximum comparable to the cover photo. Histogram graphs show distortions much less among the quilt photo and stego photo. Comparison graphs are drawn to expose a proposed device PSNR and MSE values are improved by 33% and 43% respectively than the existing device. This proposed device is carried out to boost the safety of the statistics while transmitted via an extraordinarily susceptible and insured network.

FUTURE SCOPE -

A text steganography technique in the JPEG picture changed into studied and proposed a machine with the aid of Abbas Darbani et al. [3]. Here JPEG photos are used for steganography because of the smaller size which is appropriate for transmission and Least Significant Bit technique is used for steganography. Since a part of the information might be misplaced due to the lossless compression nature of the picture proposed machine wherein a message is embedded after the discretization stage and adjust pixel is used and embedding techniques are trusted alternative desks with a purpose to be a major issue. JPEG photos are now no longer properly appropriate for steganography techniques. A new technique of hiding information in BMP picture the usage of Caesar Vigenere Cipher Cryptography and test is completed with the aid of using I Gede Arya Putra Dewangga et al. In this observe, cryptography is used to cover the name of the game message that is stimulated with the aid of using the Vigenere cipher method after which the message is inserted into the LSBs to cover one byte of a secret message it uses the eight-byte of the cowl picture without compromising the document quality. PSNR and MSR values are calculated to degree in cowl and stego picture qualities. A survey on LSB steganography among the BMP and JPEG is done with the aid of using Eltyeb E. Abed Elgaba .

A Comparison observe is carried out on lossless compressed photos (e.g. BMP, PNG, and GIF) and lossy compressed photos (e.g. JPEG) for LSB steganography. Strengths and weaknesses were observed. BMP pictures can conceal a big quantity of information and picture distortion will now no longer arise and JPEG pictures use much less space however robustness in opposition to picture manipulation and resistance to statistical assaults is low and the quantity of information distortion additionally increases. Compared to digital picture document formats the usage of distinct compression strategies is carried out with the aid of using Bharat Sinha. Images are sorts of document layout one is lossless compression technique data will now no longer lose after transmission and lossy compressed method information will lose after transmission assessment observe is carried out among the PNG and JPEG wherein PNG picture will greater appropriate for LSB steganography each BMP and PNG photos have comparable characteristics. A survey is carried out on a stenographic device for the BMP picture layout with the aid of Prof.SumedhaSirsikar et al. [9]. Various gear performances are evaluated through PSNR for stego and cowl photos values are very much less and gear are furnished through GUI and command line which may be very complex to use. Image steganography, primarily based totally at the RSA set of rules, is implemented through Rituparna Halder et al. [10]. Steganography is combined with RSA cryptography set of rules to provide greater security to statistics along with encryption and decryption upload authentication module for extra security from all above prevision studies in this examine might be used steganography with greater green and easy cryptography method i.e. Base64 and LSB steganography used for PNG image format which is distortionless, hold statistics integrity and save greater statistics. An android utility is constructed which consumer pleasant and extensively utilized for personal communication. JPEG photos are not well suitable for LSB steganography due to the fact that statistics loss occurs. The compression set of rules that's used to hold statistics integrity is complex to implement. Steganography by myself has much less security.

ACKNOWLEDGEMENT

This is a matter of pleasure for me to acknowledge my gratitude to the School of Computer Science and Engineering, Galgotias University for allowing me to explore my abilities via this paperwork. I would like to express my sincere gratitude to our project guide, MS PUNEETA SINGH , for her valuable guidance and advice in completing this paperwork and for the wholehearted support extended to me throughout the conduct of the study. Last but not the least, I would like to express my sincere thanks to my family members, friends for their immense support and best wishes throughout the curriculum duration and the preparation of this paper.

REFERENCES

- 1.) Sheelu1 and Babita Ahuja, “An Overview of Steganography”, in IOSR Journal of Computer Engineering, Volume 11, Issue 1 (May. - June.2013), PP 15-19.
- 2.) An_Efficient_Encryption_and_Decryption_Method_for_Image_Steganography
- 3.) Somchai and Wen Dong,” Research on Base64 Encoding Algorithm and PHP Implementation”, in 26th International conferences on GEOINFORMATION .
- 4.) AES_Encryption_Study_Evaluation
- 5.) Image Steganography Techniques: An Overview - BY NAGAM HAMID