IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Encryption-Then-Compression System Utilizing Least Significant Bit-Based Image Encryption for JPEG Images

[1]Neha Kakade, [2]Renuka Gaikwad, [3]Prajakta Khamgal, [4]Suparna Naik,
[1]Student, [2]Student, [3]Student, [4]Lecturer [1234]Department Of Computer Technology,
[1234] Bharati Vidyapeeth's Jawaharlal Nehru Institute of Technology (Poly), Pune, Maharashtra, India.

Abstract: In the era of digital communication and information exchange, protecting the confidentiality and integrity of sensitive data is essential. Digital pictures are necessary for many purposes, such as exchanging multimedia material, remote sensing, and medical imaging This presentation presents a unique approach to enhance the security and effectiveness of data transmission and storage through the application of picture encryption and compression algorithms. We propose "Encryption-Then-Compression" method that employs LSB-based image encryption for JPEG pictures.

The primary objectives of this system are to: (1) safeguard the integrity and privacy of JPEG pictures during transmission and storage; and (2) improve the efficiency of the data compression process to optimise resourceutilisation.

Keywords: The Encryption-Then-Compression process comprises the following key components:

1. **LSB (Least Significant Bit) Image Encryption:**
2. **Encryption Phase:**
3. **Compression Phase:**

I. INTRODUCTION

- **Concealing and Retrieving Hidden Information in Images**

In the landscape of information security and privacy that is rapidly evolving, strong data encryption and concealment techniques are vital| The concealment of text within digital images is a fascinating area in this field that combines the principles of cryptography with the complexities of image processing| The subject of this project is the art and science of hiding textual information in pictures

and the development of methods to extract and decipher the concealed content.

- **Steganography:**

It is a method of covering one message inside another| Using steganography, an encrypted file can still hide information, so even if the encrypted file is deciphered, the hidden message cannot be seen| Steganography requires special software

II. LITERATURE VIEW

III. Sr.no	Paper title with publicationyear	Abstract	Features	Future Scope
1	Image Steganography using Least Significant Bit (LSB) – A Systematic Literature Review.Jan. 25 - 27, 2022	Digital image steganography is like hiding a secret message within a normal image. One common method used for this is called Least Significant Bit (LSB). It works by subtly changing the least significant bit of each pixel in an image to encode the hidden information. Researchers have been studying different ways to use LSB for steganography, especially between 2016 and 2020.	Robustness Security Capacity. Efficiency 5. Resistance todetection Adaptability 7. Embeddingstrategies	Finally, it is analysed that the size and secrecy of secret data is biggest challenge while applying LSB techniques. In this article, the application of LSB is investigated. However, we intend to investigate and compare other image steganography approaches in near future.
2	A Password and Least Significant Bit Substitution Based Steganography Technique for Image Hiding	The description describes a new image steganography system that uses a text- based password as a symmetric key for encryption and decryption. The dynamic placement feature of the technology adds an added degree of protection to the steganography process, making it more resistant to potential network attacks. Overall, the proposed technique uses a text-based password, LSB replacement, and dynamic positioning to provide secure and lossless hiding and retrieval of secret images within cover images.	1.Text-based password symmetric key 2.LSB substitution 3. Dynamic positioning 4. Robustness 5.Security 6.Lossless Hidingand Retrieval	In future, we can use this kind of methodology in almost every kind of steganography Techniques like text steganography, audio steganography, video steganography etc. Also, we can try techniques other than LSB substitution so that more difficulty arises at the time of decryption and it may become much more secure method.

3	Image steganography using least significant bit with cryptography	Steganography is used to improve the security of messages sent via the internet. This study discussed a technique based on the least significant bit (LSB) and a novel encryption algorithm. Matching data to a picture reduces the likelihood of an attacker using steganalysis to retrieve data. Before hiding data in an image, the application encrypts it.	1.LSB bedding2.New Encryption Algorithm 3. Data matchinto Image 4. Enhanced Security 5. Resistance toattack 6. Improved Confidentiality	In the modern world, the term "hacking" is frequently heard. The act of gaining unauthorized access to data that is collected during data transmission is known as hacking. Regarding steganography, some potential future solutions for the aforementioned issue may involve the use of both steganography and cryptography. Digital watermarking is likely to be the most significant application of steganographic techniques in the near future.
4	Hide image and text using LSB, DWT and RSA based on image steganography	The abstract emphasizes how important security is in the quick-paced technological world of today. To protect the confidentiality of the message, the encrypted image is concealed within another image using LSB bits and DWT techniques. The message can be decrypted with the recipient's public key since the RSA encryption technique encrypts using the recipient's public key.	1. Security emphasis 2. Encryption with RSA algorithm 3. Publuc key Infrastructure LSB and DWT techniques 5. Secrecy Assurance	As the improvement in existing technique, the proposed method obtains higher values of PSNR and lower values of MSE for images to achieve the better result. Exceptional steganograp hy strategies can be used in the future with more hybrid cryptography for greater security.

			6. Data integrity preservation 7. Adaptability To advancing Threats	
5	Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish	The abstract underlines the increasing need of protecting confidential information, particularly in the digital arena where the internet operates. is the principal medium for data transmission. The study uses a hybrid technique, combining the LSB (Least Significant Bit) steganography algorithm with many cryptographic algorithms such as AES, RSA, DES, 3DES, and blowfish. This combination is intended to provide a strong layer of protection for hiding and encrypting messages under a cover image. Overall, the abstract proposes a hybrid approach to data security that uses both encryption and steganography. It shows experimental results that demonstrate the combined strategies' effectiveness and quality, indicating their potential utility for safeguarding sensitive information in digital communication.	Growing importance of datasecurity 2. Hybrid approach 3. Combinbatio nof algorithms 4. Robust security layer 5. Hiding and encrypting messages 6. Experimental validation 7. Potential Utility	In this paper, cryptography and steganography are combined to achieve higher security. The cryptographic algorithms are AES, RSA, DES, 3DES and Blowfish algorithms and the steganography technique is LSB. First, the data is encrypted via the mentioned algorithms. Then the secret message is embedded into the LSB algorithm to be hidden in a cover image. The experimental outcome of the method is performed on MATLAB. The execution time of RSA is more than the other algorithms due to it is a public key algorithm. Two error metrics are employed to compare the quality of cover image and the stegano-image. The high PSNR and low MSE represent the satisfaction of employing these algorithms for the first step of the method. The encrypted message is also not easily detected by the difference histogram analysis while employing cryptograph ic algorithms for the first step of steganography.

IV.METHODOLOGY

The methodologies for a project focused on hiding text in images and extracting it involve a blend of steganography and image processing techniques. Below is an outline of potential policies:

To hide a colour image (secret image) into a cover image (colour image), we must first find the cover image's location, which is where the secret image starts. A password of eight characters helps you do this. Also here we recover the hidden image with the same 8-character password. For this, first we convert the password characters into their corresponding ASCII values, and then
we convert these ASCII values into 8-bit binary numbers

After uploading split each bit of the secret encrypted message and cover image into R, G, and B colours. Represent each of the values of R, G, and B colour into a binary number. Here each LSB position of a pixel value of the cover image is substituted by the bit value of the secret message. For substitution R, G, and B colour value of the cover image is substituted by the R, G, and B colour bit value of the secret message. So, 8-bit of a pixel of the secret message is substituted to the LSB position of 8 consecutive pixels of the cover image

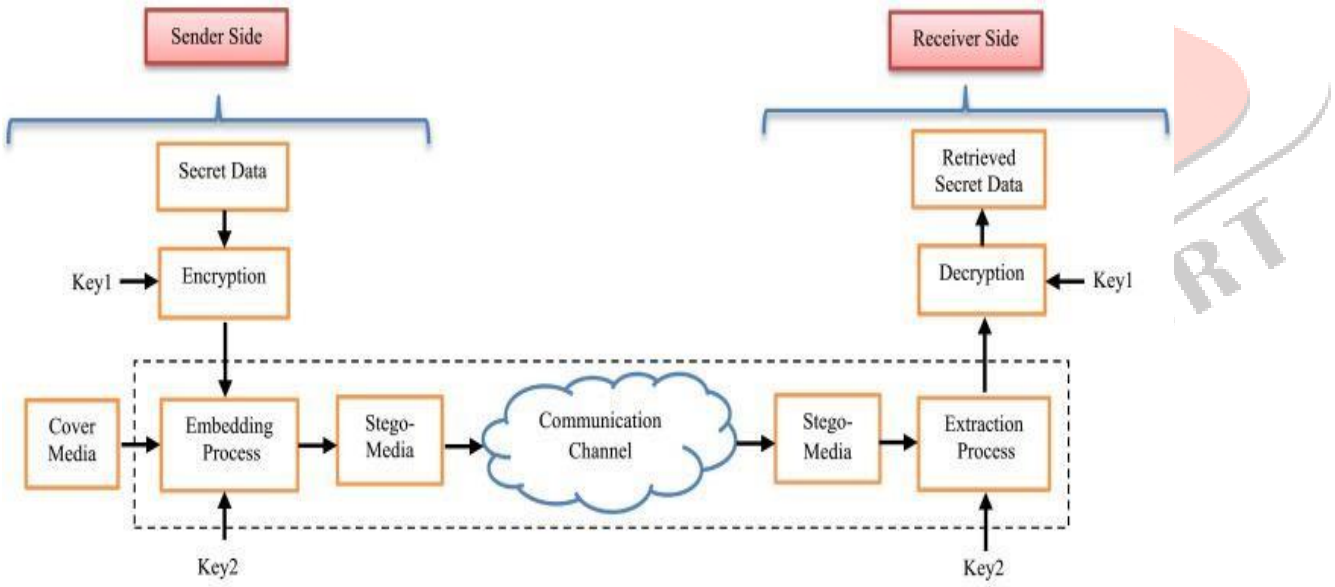
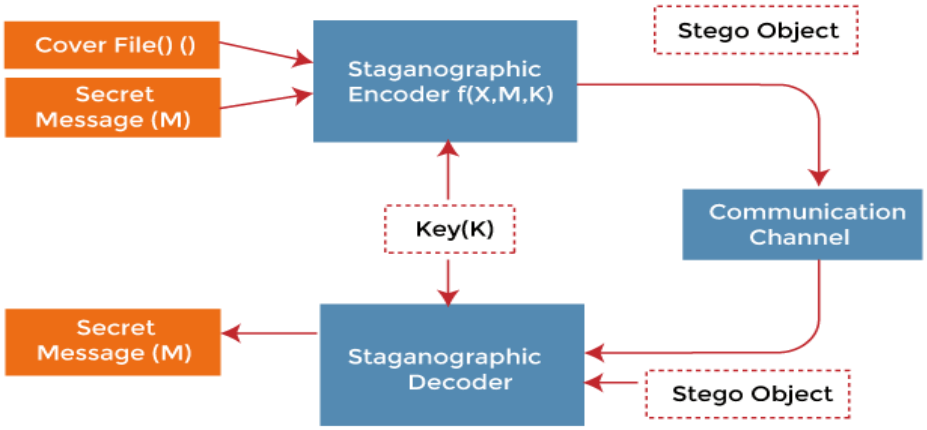


Figure 1.

V. Background: The Intersection of Steganography and Image Processing

Steganography, the practice of concealing information within other data to prevent detection, has a rich history dating back to ancient times. In the contemporary digital era, steganography has found a natural ally in image processing, leveraging the vast visual data space to embed hidden messages. This project aims explore and enhance the synergy between steganography and image processing, investigating novel methods to embed textual information seamlessly within images while preserving their visual integrity.



VI. Research Objectives: Bridging Security and Practicality

The project's main objectives are two: first, to design efficient methods for the extraction and decoding of this concealed data, and second, to develop advanced algorithms for safely embedding textual data within pictures| The project aims to create a robust system

that ensures the hidden text remains impervious to detection while allowing for the dependable retrieval required.

VII. Significance: Applications and Implications

The ability to hide information in images has significant implications for several domains, including secure communication, digital forensics, and intellectual property protection. With the increasing use of digital communication, covert information transfer techniques are becoming more and more in demand. This work provides a thorough analytical method for safe text retrieval and embedding in the visual realm to address this demand. The methods employed, a thorough review of prior steganography and image processing research, and a demonstration of our unique contributions to expanding the realm of textual information extraction and concealment in images are all covered in the following sections. We hope that our work will make a positive impact on the information security environment by providing creative answers to the problems that the rapidly growing digital world presents. secret message. For substitution R, G, and B colour value of the cover image is substituted by the R, G, and B colour bit value of the secret message. So, 8-bit of a pixel of the secret message is substituted to the LSB position of 8 consecutive pixels of the coverimage

VIII. LSB Algorithm:

This code appears to be implementing a simple algorithm for hiding information in the least significant bit of the red channel of thefirst 32 pixels in an image

Step 1 Read the Image:

Reads the image from a ByteArrayInputStream

BufferedImage originalImage = ImageIO.read(new ByteArrayInputStream(imageFile.getBytes()));

Step 2 Get Image Width and Initialize Variables:

Retrieves the width of the image and initializes a variable to keep track of the current pixel index.int width = originalImage.getWidth();

int pixelIndex = 0;

Step 3 Loop Through Each Pixel (First 32 Pixels):

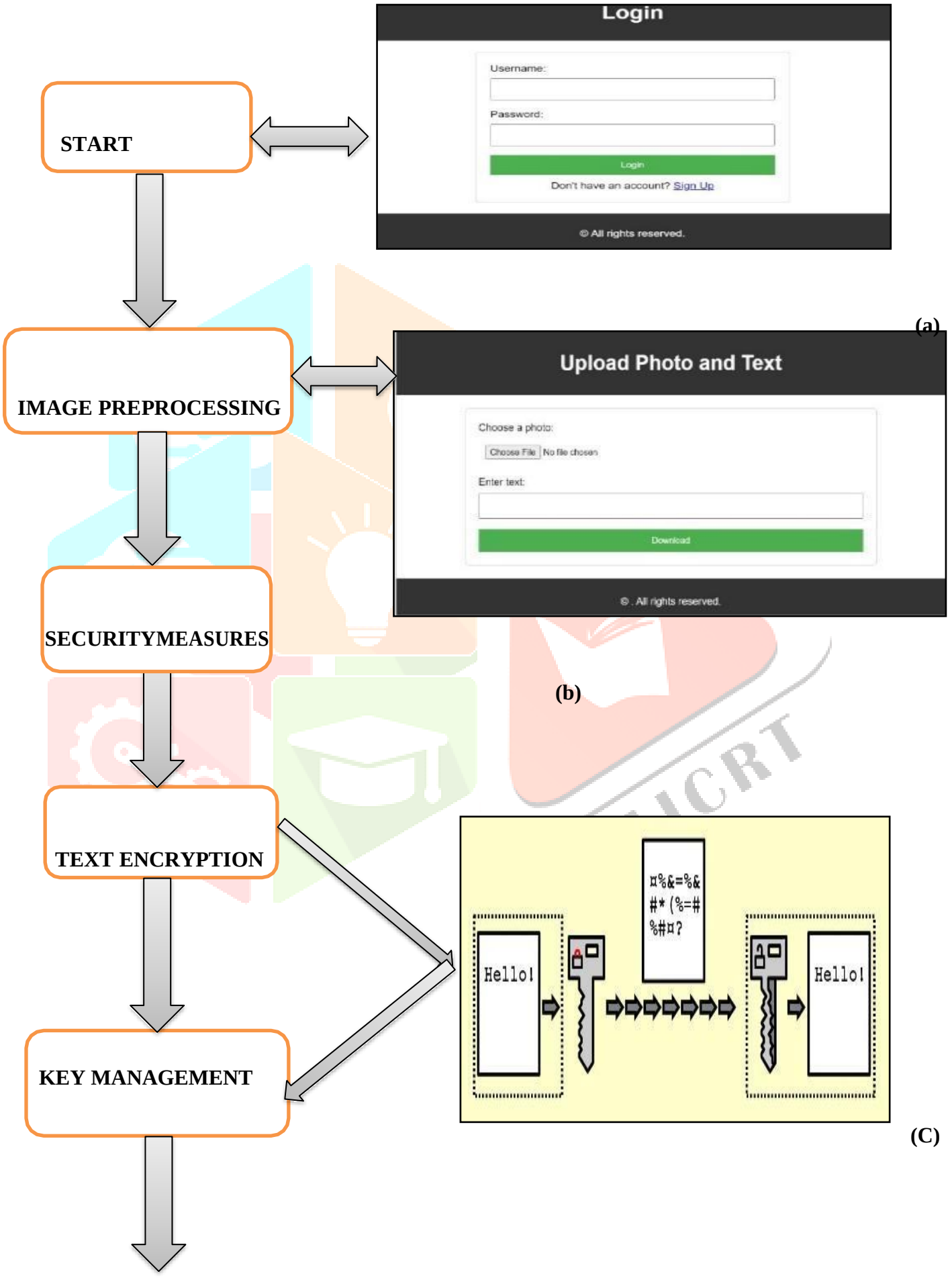
Iterates through the first 32 pixels of the image.for (int i = 0; i < 32; i++)

Step 4 Get RGB Values of the Pixel:
Get the red components of the current pixel.
int pixel = originalImage.getRGB(pixelIndex % width, pixelIndex / width);int red = (pixel >> 16) & 0xFF; int green = (pixel >> 8) & 0xFF;int blue = pixel & 0xFF;;
Step 5 Get a Bit from the ID:
Get a bit from the id based on the current loop.int bit = ((id >> (31 - i)) & 1);
Step 6 Hide the Bit in the Red Channel:
Clears the LSB of the red channel and sets it to the value of the retrieved bit.red = (red & 0xFE) | bit;
Step 7 Create the New Pixel with Modified Red Channel:
Combines the modified red channel with the original green and blue channels to create a new pixel value.int newPixel = (red << 16) | (green << 8) | blue;
Step 8 Set the Modified Pixel in the Image:
Sets the newly created pixel back into the same position in the image. originalImage.setRGB(pixelIndex % width, pixelIndex / width, newPixel);**Step 9 Increment Pixel Index:**
Moves on to the next pixel in the image.pixelIndex++;
The purpose of this code is to hide information in the red channel of the first 32 pixels of the image by modifying the least significant bit of the red channel with bits from a 32-bit integer (id).

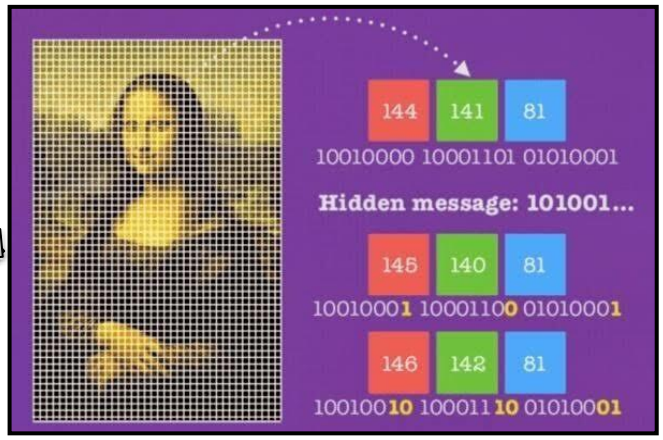
IX.RESULTS AND DISCUSSION

The project's result analysis shows that the Least Significant Bit (LSB) method was successfully used for text embedding and extraction| The process discreetly transmits information by hiding text within image pixels| However, it
is important to remember that in scenarios involving image compression, there may be limitations. This is because compression algorithms can add artifacts and change LSB values, which can make it hard to retrieve embedded textaccurately| Future iterations should look into alternative steganographic techniques or consider using compression-
resistant techniques to ensure consistent text extraction across various image conditions in order to strengthen the system(https://imageencryptorpro.up.railway.app)

FLOW CHART:


START
IMAGE PREPROCESSING
SECURITYMEASURES
TEXT ENCRYPTION
KEY MANAGEMENT
Login
Username:
Password:
Login
Don't have an account? Sign Up
© All rights reserved.
(a)
Upload Photo and Text
Choose a photo:
Choose File No file chosen
Enter text:
Download
© . All rights reserved.
(b)
Hello!
¤%&=%&
#*(%=#
%#¤?
Hello!
(C)

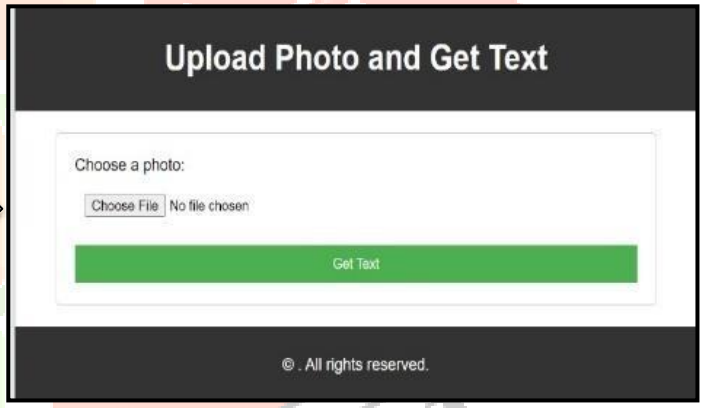
DATA STORED



TEXT EMBEDDING

(d)

UPLOAD PROCESSEDIMAGE



(e)

TEXT EXTRACTION

TEXT DECRYPTION

END

X. FUTURE SCOPE

Although this project is a significant advancement in the field of secure text hiding and extraction, travel continues| Improved security, new encryption algorithms, and machine learning could be the subjects of future research.

Finally, the goal of this project is to redefine the landscape of information concealment in digital images by combining steganography and image processing| Our work not only contributes to the academic debate but also holds potential applications in secure communication, digital forensics, and beyond by combining security, efficiency, and practicality| As technology
advances, it is also necessary to innovate in securing information transmission. This project demonstrates our commitment to advancing the frontiers of digital security.

XI. CONCLUSION

With combination of steganography using LSB, image processing and encryption has given the project which has aim to secure the data by using many layers of encryption and total security. This project aims to significantly advance the art and science of text hiding and extraction from image

REFERENCES

1. Image Steganography using Least Significant Bit (LSB) – A Systematic Literature Review. Jan. 25 - 27, 2022 (978-1-6654-3605-2/22)
Authorized licensed use limited to: Hamad Bin Khalifa University

2. A Password and Least Significant Bit Substitution Based Steganography Technique for Image Hiding (2347-5552,volume-10, ISSUE-5, September 2023)

3. Image steganography using least significant bit with cryptography(2229-371X, Volume-3, No-3, March-2012)

4. Hide image and text using LSB, DWT and RSA based on image steganography[0976-9102(online), DOI:10.21917/IJIVP/2019.0275]

5. Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish[2249-8958(online), Volume-8, Issue-6S3, September-2019]