UNIVERSITY INSTITUTE OF TECHNOLOGY

The University of Burdwan

DEPARTMENT OF INFORMATION TECHNOLOGY

2020 – 2024 BATCH

Project Report On

"VISUAL CRYPTOGRAPHY & SECRET MESSAGE SHARING"

A Project Under the Guidance of

Mrs. NABANITA DAS

Assistant Professor

DEPARTMENT OF INFORMATION TECHNOLOGY

UNIVERSITY INSTITUTE OF TECHNOLOGY

THE UNIVERSITY OF BURDWAN, GOLAPBAG (NORTH)

BURDWAN, 713104, WEST BENGAL

Submitted By

SAMIR ROY	(20203024)
SUBHRANIL MONDAL	(20203027)
ARNAB PATRA	(20203030)
SATYAPRIYA MONDAL	(20203036)
AVIRAJ KUMAR	(20203063)
SRISTI MITRA	(20203067)

University Institute of Technology, Burdwan University

DEPARTMENT OF INFORMATION TECHNOLOGY

BACHELOR OF ENGINEERING (B.E.)

CERTIFICATE OF APPROVAL

This is to certify that the project entitled "**VISUAL CRYPTOGRAPHY AND SECRET MESSAGE SHARING**" submitted by **SRISTI MITRA (20203067), SUBHRANIL MONDAL (20203027), SATYAPRIYA MONDAL (20203036), SAMIR ROY (20203024), ARNAB PATRA (20203030), AVIRAJ KUMAR (20203063)** under the guidance and supervision of **Mrs. Nabanita Das** as partial fulfillment for the award of the degree of **BACHELOR OF ENGINEERING** in **INFORMATION TECHNOLOGY** at **UNIVERSITY INSTITUTE OF TECHNOLOGY**. The University of Burdwan is a record of the work of the students which has been carried out under any supervision.

I hereby forward this project

Date: ……

Place: .....

_____

(Project guide)

Mrs. Nabanita Das
Assistant Professor
Department of Information technology
University Institute of Technology
University of Burdwan, 713104

University Institute of Technology, Burdwan University

CERTIFICATE

This is to certify that the work embodied in the final year project "**VISUAL CRYPTOGRAPHY AND SECRET MESSAGE SHARING**", submitted by **SRISTI MITRA (20203067)** to the Department of Information Technology are carried out under my direct supervision and guidance.
The project work has been prepared as per the regulation of The University of Burdwan and I strongly recommend that this project work can be accepted in partial fulfillment.

Date: ……

Date: ……

Head of the Department:

Mrs. Kasturi Ghosh

Assistant Professor & In-charge,

Dept. of IT

University Institute of Technology,

Burdwan University

Project Guide:

Mrs. Nabanita Das

Assistant Professor, Dept. of IT

University Institute of Technology,

Burdwan University

ACKNOWLEDGEMENT

We express our pleasure and gratitude to submit our project **"VISUAL CRYPTOGRAPHY AND SECRET MESSAGE SHARING"**. We are extremely obliged to **Mrs. Nabanita Das** ma'am who has allowed us to work on this project. They have been a perpetual source of inspiration in taking this project to such great heights on behalf of the institution UNIVERSITY INSTITUTE OF TECHNOLOGY, BURDWAN UNIVERSITY. Finally, we would like to thank THE UNIVERSITY OF BURDWAN for giving us this subject as a paper as it has not only given us the experience to work on a project but also will help shortly.

Date: ……..

Group members:

SRISTI MITRA	**SAMIR ROY**
SUBHRANIL MONDAL	**ARNAB PATRA**

SATYAPRIYA MONDAL **AVIRAJ KUMAR**

Contents Page No.

Declaration

We clarify that:

1. The work contained in the thesis is original and has been done by ourselves under the general supervision of our supervisor(s).

2. The work has not been submitted to any other Institute for any degree or diploma.
3. We have followed the guidelines provided by the Institute in writing the thesis.
4. We have conformed to the norms and guidelines given in the ethical code of conduct of the Institute.
5. Whenever we have used materials (data, theoretical analysis, and text) from other sources, we have given due credit to them by citing them in the text of the thesis and giving their details in the references.
6. Whenever we have quoted written materials from other sources, we put them under quotation marks and give credit to the source by citing them and giving the required details in the references.

Abstract

"Visual Cryptography and Secret Message Sharing" addresses the critical need for secure image transmission in digital communication. This project employs Visual Cryptography to encrypt images including hidden message. In the next step, the image is converted into grayscale including the hiding message and generates multiple shares that can be distributed securely. These shares, appearing as

random noise, are individually meaningless and ensure that the original image remains secure. At the receiver's end, combining the shares by overlapping method reconstructs the original image, and original message maintaining data integrity and confidentiality.

This includes enhanced security through user-friendly encryption and decryption processes. The project significantly reduces the risk of unauthorized access by ensuring shares are useless without the correct combination. This method is particularly beneficial for sectors requiring secure communication, such as government, military, and corporate environments.

To securely hide a message within an image, use a method involving the division of the image into shares. Each share contains part of the image and some encoded information of the hidden message. Using an overlapping method, these shares are distributed such that the original message and image are obscured individually. Only when all shares are recombined correctly can the original image and hidden message be fully reconstructed. This technique ensures both the image and the hidden message remain secure until all shares are gathered and processed together.

In future we will focus on optimizing algorithms, integrating with other security protocols, and ensuring cross-platform compatibility. Deploying the system in real-world scenarios will provide valuable feedback for further refinement. Overall, this project demonstrates a robust approach to secure communication, laying a strong foundation for future advancements in cyber security.

Objective

Specifically, the project seeks to:

1. **Develop a Visual Cryptography-Based Encryption System:**

Create a robust encryption mechanism that converts an image into multiple shares, making each share appear as random noise and ensuring no information is discernible from individual shares.

2. **Integrate Password Protection:**

Implement an additional layer of security by requiring a user-defined password for the encryption and decryption processes, ensuring that only authorized users can access the original image.

3. **Ensure Secure Distribution:**

Enable the secure distribution of encrypted shares over potentially insecure communication channels without compromising the security of the original image.

4. **Facilitate Efficient Decryption:**

Develop a decryption process that allows the original image to be accurately reconstructed only when the correct shares and password are provided, maintaining data integrity and confidentiality.

5. **Enhance User Accessibility:**

Design a user-friendly interface that simplifies the processes of image encryption and decryption, making the system accessible to users with varying levels of technical expertise.

6. **Address Real-World Security Needs:**

Provide a secure communication solution for sectors that require high levels of data security, such as government, military, and corporate environments, addressing the growing demand for advanced security measures in the digital age.

Motivation

The motivation behind the "Visual Cryptography and Secret Message Sharing" project stems from the growing need for robust security measures in the digital age. As sensitive information spreads online fast, the risk of unauthorized access and data breaches becomes a critical concern. Traditional encryption methods, while effective, often face challenges in secure key management and complexity.

Visual cryptography offers a unique and powerful solution by transforming an image into multiple shares that appear as random noise individually but can reconstruct the original image when combined correctly. This approach eliminates the need for complex computational resources during decryption, relying instead on the human visual system, which is both intuitive and secure.

We were driven by the potential applications in sectors where data security is paramount, such as government, military, and corporate environments. Ensuring that sensitive images and messages remain confidential during transmission can prevent espionage, data leaks, and unauthorized surveillance.

Additionally, we sought to create a system that is not only secure but also userfriendly. By incorporating a password protection layer and simplifying the encryption and decryption processes, we aimed to make advanced cryptographic techniques accessible to users with varying technical expertise.

Ultimately, our project aims to contribute to the broader field of cyber security by providing an innovative solution that addresses current challenges and anticipates future threats. This motivation is rooted in a commitment to protecting privacy and enhancing the security of digital communications.

1. Introduction

The increasing need for secure communication in the digital age has spurred interest in innovative methods to protect sensitive information. One such method is **Visual Cryptography**[1], a fascinating technique that allows secret messages to be shared within an image and deciphered visually to the recipient side easily. This project explores the potential of visual cryptography to provide a robust, user-friendly approach to secure the hiding communication. By leveraging modern technologies such as image processing, digital watermarking, and cryptographic principles, we aim to create a system that ensures the safe transmission and retrieval of confidential messages. Through this project, we hope to demonstrate the practical applications of visual cryptography and its ability to enhance the security and privacy of digital communications.

1.1 Visual Cryptography

Visual cryptography is a technique that encrypts visual information, such as images or text, by splitting it into multiple shares. Individually, these shares reveal nothing, but when overlapped, they reveal the hidden message and reconstruct the image also.

This project employs visual cryptography for its simplicity, inherent security, and human decipherability. It is an ideal method for secure message sharing as it doesn't require advanced decryption tools, making it accessible and practical. By using visual cryptography, we aim to create a user-friendly system that ensures the safe transmission and retrieval of confidential messages, demonstrating the method's applicability in fields like secure communications and digital rights management.

1.2 Survey Reports

This project leverages several established visual cryptography techniques to ensure secure and efficient sharing of visual information. The techniques are inspired by pioneering research and advancements in the field, providing a robust foundation for our approach. Here are the key techniques referenced and used in this project:

- **1.2.1. Visual Cryptography by Moni Naor & Adi Shamir**

Moni Naor and Adi Shamir introduced the basic concept of visual cryptography in 1994. Their technique involves splitting an image into two shares such that each share, individually, provides no information about the original image. When combined, the

shares reveal the hidden image. This foundational technique forms the basis of our visual cryptography approach, ensuring that individual shares are meaningless and only the combination reveals the secret.

- **1.2.2. Efficient Visual (EVC) by Supriya Kinger**

Supriya Kinger's Efficient Visual Cryptography (EVC) technique focuses on optimizing the traditional visual cryptography method to enhance performance and reduce computational overhead. EVC ensures that the shares are generated quickly and efficiently, making the process more practical for real-world applications. This technique is employed in our project to improve the speed and efficiency of share generation and combination.

- **1.2.3. Visual Cryptography Using Binary Array Oriented Holograms (AOHs) by Lina Zhou, Yin Xiao, Zilan Pan, Yonggui Cao & Wen Chen**

This technique utilizes binary Array Oriented Holograms (AOHs) to encode visual information. By leveraging binary AOHs, the method enhances the security and robustness of the visual cryptography scheme. The use of binary patterns allows for more complex and secure share generation, ensuring that the original image is effectively hidden until the correct shares are combined. Our project incorporates this advanced technique to provide an additional layer of security.

- **1.2.4. Visual Cryptography for Biometric Privacy by Arun Ross & Asem Othman**

Arun Ross and Asem Othman introduced a visual cryptography scheme specifically designed to protect biometric information. This technique ensures that biometric data, such as fingerprints or facial images, can be securely shared and stored. The shares generated using this method preserve the privacy of the biometric information until they are combined by an authorized party. In our project, this approach is adapted to secure sensitive visual data, providing privacy protection for biometric and other confidential images.

1.3 Need for Visual Cryptography

Visual cryptography enhances security by ensuring only intended recipients can access the message, is simple and easy to use without advanced tools, and allows for human decipherability without digital devices. It is immune to digital cyber-attacks due to its manual decryption process and finds versatile applications in fields like military communications, secure voting, and digital rights management.

Additionally, it is cost-effective, does not require expensive hardware or software, is ideal for non-digital decryption in remote areas or during power outages, and secures sensitive printed materials. Overall, visual cryptography is an essential technique for protecting visual information in various contexts.

1.4 Visual Cryptography Techniques

- **1.4.1. Visual Cryptography Scheme (VCS)**

- **(k, n)-Threshold Scheme:** This is the most common scheme where an image is divided into n shares, and any k out of n shares can be used to reconstruct the image. For example, in a (2, 2)-threshold scheme, the image is split into 2 shares, and both are required to view the image.
- **Share Generation:** Each pixel in the original image is represented by multiple sub-pixels in the shares. For instance, two identical patterns in both shares might represent a white pixel, while complementary patterns might represent a black pixel.

- **1.4.2. XOR-Based Visual Cryptography**

- **XOR Operation:** Instead of traditional **Superimposing**[2], this method uses the **XOR**[3] operation to combine shares. It often offers better visual quality for the reconstructed image.

  Example: For a simple (2, 2) XOR-based scheme:

  Original pixel: 1 (black)

  Share 1: 0

  Share 2: 1

  XOR(Share 1, Share 2): $0 \oplus 1 = 1$ (black)

- **1.4.3. Extended Visual Cryptography**

- **Color Images:** Traditional schemes work with binary images. Extended schemes handle grayscale or color images, often by breaking down each color channel (RGB) into separate binary layers.

- **Meaningful Shares:** Instead of random noise, shares can be made to look meaningful (like regular images), which can enhance security and usability.

Advanced Techniques

Progressive Visual Cryptography

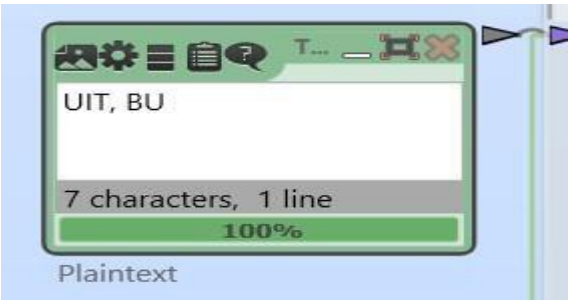
- **Concept**: Allows partial decryption of the image with fewer than the required number of shares.
- **Process**:
  - The quality of the decrypted image improves as more shares are added.
  - Useful for applications where some information can be revealed with partial shares.

Visual Cryptography for Grayscale Images

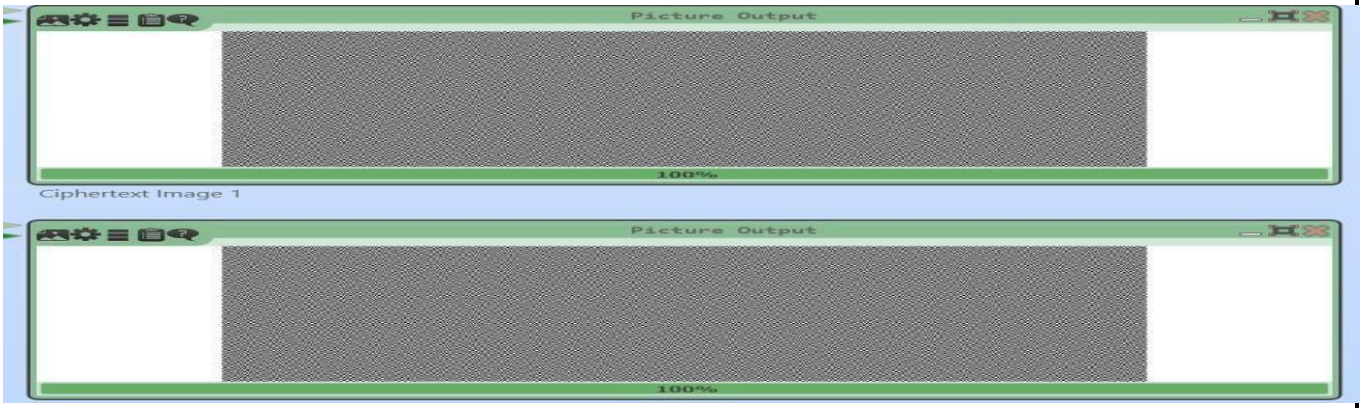
- **Concept**: Extends traditional binary visual cryptography to handle grayscale images.
- **Techniques**:
  - Grayscale images are quantized into multiple levels.
  - Each level is processed using visual cryptography techniques.
  - Shares for each level are then combined to form the final shares.

1.5 Input / Output

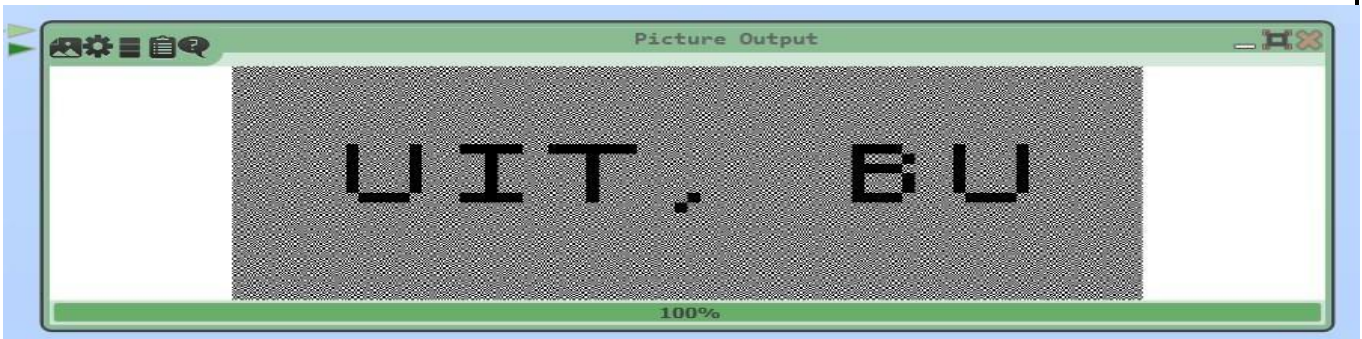
Input: We are using **CrypTool**[4] to show the implementation of visual cryptography. At first, we write a message to hide in between an image or a transparent paper.



Then after execution, it will generate 2 shares, if we overlap these 2 shares we will get our message at a point.



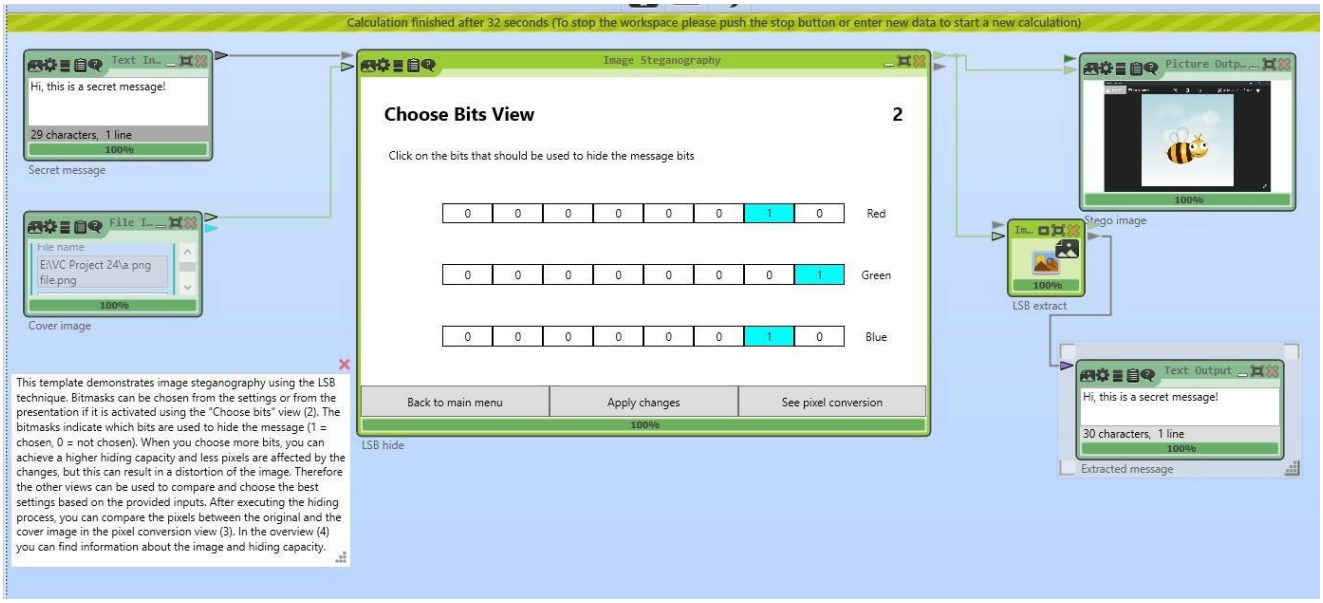
Output: We are getting the message in this format



2. Image Steganography

2.1 Concept

Image steganography[5] conceals secret data within images, keeping their visible appearance unchanged. It embeds information within pixel values, producing a stego (resultant) image that appears identical to the original. Techniques like **LSB**[6] insertion subtly modify pixels to hide data, making detection by unauthorized users difficult. This method is used in secure communication, digital watermarking, and covert messaging, enhancing privacy and security. Detecting hidden data in stego images requires specialized steganalysis algorithms and software, ensuring data confidentiality and integrity.



2.2 Need of Image Steganography

It is crucial for secure and covert communication, providing a means to hide sensitive information within images discreetly. It ensures data security by allowing the secure transmission of confidential data without raising suspicion. This covert communication capability is valuable in military, intelligence, and corporate contexts. Additionally, steganography is used in digital watermarking for copyright protection and authentication. It also safeguards privacy by hiding personal or proprietary data within images. On the flip side, steganalysis is vital for detecting hidden information in stego images, aiding digital investigations and cybersecurity efforts. Overall, image steganography is a versatile tool that addresses data security, privacy protection, and covert communication needs in various domains.

2.3 Usage

Image steganography is widely used for secure communication, digital watermarking, privacy protection, covert operations, anti-forensics, and digital investigations. It conceals confidential messages within images, ensuring data security in military, intelligence, and diplomatic contexts. Digital watermarking employs steganography to embed copyright information and verify digital asset authenticity. Individuals and organizations use steganography to safeguard personal and proprietary data, enhancing privacy protection. Law enforcement and intelligence agencies leverage steganography for covert operations and surveillance, while cybercriminals may exploit it for anti-forensics. Conversely, steganalysis aids cybersecurity professionals in detecting hidden threats and analyzing digital evidence during digital investigations. Overall, image steganography is a versatile tool with applications in data security, privacy, covert communication, and forensic analysis.

3. Visual Cryptography and Secret Message Sharing

It is a cyber security project focused on securely transmitting sensitive images. The project utilizes visual cryptography to encrypt images into multiple shares, which can be distributed to recipients. These shares, individually meaningless, can only be used to reconstruct the original image when combined with the correct password.

3.1 About It

In our project, "Visual Cryptography and Secret Message Sharing," we developed a secure method to transmit sensitive information by embedding secret messages within color images. The process begins with the user selecting an image and providing a secret message, which is then encrypted using a password. This ensures that only authorized individuals can access the hidden information.

The secret message is converted into an 8-bit binary format, with each character represented by a binary code. This binary data is then embedded into the image by manipulating the pixel values. Each pixel in a color image consists of three RGB (Red, Green, Blue) values. We hide the binary bits of the secret message within these RGB values based on specific rules: if the binary bit is `0`, the corresponding RGB value is made even; if the bit is `1`, the RGB value is made odd. For example, to hide the binary

sequence `010` in a pixel with RGB values (124, 135, 146), we adjust the values so that they align with the binary bits, resulting in minimal perceptible change to the image.

The embedding process continues through the image pixels until the entire secret message is hidden. Given the vast number of pixels in typical images, this method allows for the embedding of substantial amounts of data without noticeable changes to the image quality. The password protection adds an extra layer of security, ensuring that even if the image is intercepted, the hidden message cannot be retrieved without the correct password.

On the recipient's side, the image is decrypted using the correct password, and the hidden binary message is extracted by analyzing the RGB values. This binary message is then converted back to its original text format, revealing the hidden information.

This project showcases an effective combination of visual cryptography and steganography to enhance data security. By embedding secret messages within images and protecting them with passwords, we ensure the confidentiality and integrity of the information, making it useful for secure communication in government, military, corporate, and personal contexts. Future enhancements may include optimizing the embedding algorithms, integrating additional cryptographic measures, and developing cross-platform applications to further improve the system's efficiency and usability.

3.2 Purpose

The purpose of the "Visual Cryptography and Secret Message Sharing" project is multifaceted, aimed at addressing the growing need for secure communication in an increasingly digital world. The project leverages the principles of visual cryptography and steganography to create a robust system for embedding and transmitting secret messages within images. This innovative approach enhances data security and privacy, providing a reliable method for protecting sensitive information.

Key Objectives:

1. Enhancing Data Security:

The primary purpose of this project is to significantly enhance the security of data transmission. By embedding secret messages within images and using password protection, the project ensures that sensitive information is protected from unauthorized access. The combination of visual cryptography and steganography provides a dual-layer security mechanism, making it extremely difficult for malicious actors to intercept and decode the hidden messages.

2. Ensuring Privacy:

Protecting privacy is another crucial purpose of this project. In an age where digital communication is prevalent, maintaining the confidentiality of personal and sensitive information is paramount. By hiding messages within images, the project ensures that the content remains confidential, visible only to those with the correct password and the necessary shares to reconstruct the original message.

3. Providing a User-Friendly Solution:

The project aims to develop a system that is not only secure but also accessible to users with varying levels of technical expertise. By simplifying the processes of encryption and decryption, the system ensures that users can easily embed and extract secret messages without requiring extensive knowledge of cryptographic techniques. This user-friendly approach broadens the applicability of the system, making it useful for a wide range of users.

4. Facilitating Secure Communication:

The project is designed to facilitate secure communication in various sectors where data security is critical. Government and military organizations can use this system to transmit classified information securely. In the corporate sector, businesses can protect sensitive data and communications from competitors and cyber threats. On a personal level, individuals can safeguard private communications and personal data from unauthorized access.

5. Mitigating Risks of Data Breaches:

Data breaches and cyber attacks are significant concerns in today's digital landscape. The project aims to mitigate these risks by providing a secure method for transmitting sensitive information. By embedding messages within images and using robust encryption techniques, the system reduces the likelihood of data being intercepted and misused by unauthorized parties.

6. Supporting Research and Development in Cyber Security:

The project also contributes to the broader field of cyber security by exploring and implementing advanced cryptographic techniques. By integrating visual cryptography and steganography, the project demonstrates the potential for innovative solutions to address contemporary security challenges. This can inspire further research and development in the field, leading to more robust and sophisticated security measures.

Detailed Process:

Image Selection and Message Encryption:

Users begin by selecting a color image and a secret message. The message is encrypted using a password, converting it into an 8-bit binary format. Each character of the message is represented by its binary **ASCII**[7] code.

Embedding Binary Data:

The binary message is embedded into the image by manipulating the RGB values of the image's pixels. Each pixel, consisting of three RGB values, can hold three bits of the binary message. Depending on whether the bit is `0` or `1`, the RGB values are adjusted to be even or odd, respectively. This subtle manipulation ensures the message is hidden without noticeably altering the image.

Distribution and Transmission:

The resulting image, now containing the hidden message, can be transmitted over potentially insecure communication channels. The password protection ensures that only authorized recipients can access the hidden message.

Decryption and Message Extraction:

Upon receiving the image, the recipient uses the correct password to decrypt the image and extract the hidden binary message. The binary data is then converted back to its original text format, revealing the secret message.

In conclusion, the "Visual Cryptography and Secret Message Sharing" project is designed to provide a highly secure, efficient, and user-friendly method for transmitting sensitive information. By combining visual cryptography with steganography, the project addresses critical security and privacy needs, offering a robust solution for protecting data in various contexts.

3.3 Implementation

The implementation of the "Visual Cryptography and Secret Message Sharing" project involves several key steps, each designed to ensure the secure embedding and transmission of a secret message within a color image. Here is a brief overview of the process:

1. Image and Message Input User

Input:

1. How many share generated
2. The user provides a secret message they wish to hide within the image.

Encryption

```
Enter the number of shares: 5
Enter the message to hide in the shares: UIT BU
5 shares generated successfully with embedded message: 'UIT BU'.
```

embed_message(image_array, message):

- Description: Embeds a secret message into an image.
- Parameters:
  - image: The image object (PIL Image), check image dimensions
  - message: i) Convert the message to bytes
  - ii) The secret message to embed into the image.
- Returns: The modified image with the embedded message.

generate_shares(image_path, num_shares, message):

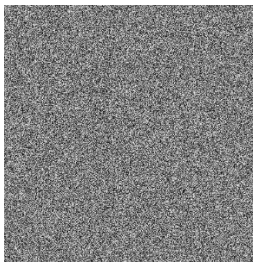
- Description: Generates shares of an image using visual cryptography or other techniques.
- Parameters:
  - image: i) The grayscale image is converted to a NumPy array for easier manipulation.

ii) The given message is embedded into the image array using the embed_message function.

  - num_shares: Number of shares to generate by image array.
  - technique: The last share is computed by XORing the original image array with all shares together will reconstruct the original image with the embedded message.

- Returns: List of shared images. ● Save Shares as Images:

Original image



Share Patch

Reconstructed image

image share preparation:

- In the given code snippet, `num_shares - 1` random binary matrices are generated iteratively using NumPy's `np.random.randint()` function. Each matrix is created with dimensions `(height, width)` and filled with random integer values between 0 and 255 (`dtype=np.uint8`). These matrices represent partial shares of an image intended for cryptographic distribution, ensuring that no single share alone reveals the original image or message content.

Decryption

extract_message(image_array, message_length):

- **Image Array** : An empty list of message_bits is created to store the least significant bits (LSBs) of each pixel in the image array.
- **Bit Extraction Loop**: Iterates through each pixel in the flattened array, extracting the LSB (Least Significant Bit) of each pixel.
- **Message Conversion**: After Converting message Bits to Bytes, Convert message_bytes to a string using **UTF-8**[8] decoding.

```
Reconstructed image saved as 'constructed.png'.
Hidden Message: UIT BU
```

reconstruct_image(shares_paths):

- **XOR Operation**: Loads each shared image specified in shares_paths, converts them to NumPy arrays (shares), and initializes the reconstruction with the first share.
- **Message Extraction**: Sequentially performs XOR operations on all shares except the first to reconstruct the original image (reconstructed_image).

Technical Considerations

Programming Language: The implementation is typically done using a programming language like Python, which offers robust libraries for image processing (e.g., OpenCV, PIL).

Efficiency: The algorithm ensures efficient embedding and extraction processes, minimizing computational overhead.

Libraries: We used several Python libraries in the process of implementation, they are:

1. PIL (Python Imaging Library):

Usage: Pillow, the Python Imaging Library (PIL) fork, is used for image processing in Python. You can install it via `pip install pillow` and import it with `from PIL import Image`. Basic operations include opening (`Image.open('path.jpg')`), saving (`image.save('path.jpg')`), and displaying images (`image.show()`). It supports resizing, cropping, rotating, and filtering images, as well as drawing operations and text rendering. Pillow's versatility makes it an essential tool for handling image files in various formats.

Functions: Pillow, known as the Python Imaging Library (PIL) fork, provides comprehensive image processing capabilities in Python. It allows for opening and saving images with `Image.open()` and `image.save()`, respectively. Image manipulation functions include resizing (`resize()`), cropping (`crop()`), rotating (`rotate()`), and flipping (`transpose()`). You can enhance images using filters like blurring or sharpening (`filter()`), adjust brightness and contrast, and apply color balance adjustments. Additionally, Pillow supports drawing operations (`ImageDraw`) for adding shapes and `ImageFont` for rendering text onto images. Its versatility and simplicity make it indispensable for handling and manipulating image files in various formats.

2. NumPY:

Usage: NumPy is a core Python library for numerical computing, offering efficient array and matrix operations, advanced mathematical functions, and support for large datasets. Essential for data science, machine learning, and scientific computing, it provides functionalities like broadcasting, linear algebra, and random number generation.

Functions: NumPy is a crucial Python library for numerical computing, offering a variety of functions for array creation (`array`, `zeros`, `ones`, `arange`, `linspace`), manipulation (`reshape`, `flatten`, `transpose`, `concatenate`), and mathematical operations (`add`, `subtract`, `multiply`, `divide`, `dot`, `sqrt`, `exp`). It also includes statistical functions (`sum`, `mean`, `std`, `var`), linear algebra operations (`det`, `inv`, `eig`, `solve`), and random number generation (`rand`, `randint`). NumPy's comprehensive functionality makes it indispensable for data science, machine learning, and scientific computing.

3.4 Real Life Scenarios

1. **Secure Communication in Government and Military:**

Intelligence agencies need to transmit confidential information without arousing suspicion.Embedding secret messages within seemingly innocuous images allows secure transmission over public channels. For instance, a covert operative might receive orders embedded within an image of a tourist destination.

2. **Corporate Data Protection:**

   Companies need to safeguard sensitive business information, such as intellectual property or confidential project details.Embedding proprietary data within images shared internally ensures that even if the images are intercepted, the embedded data remains hidden and secure.

3. **Digital Watermarking:**

   Artists, photographers, and content creators need to protect their work from unauthorized use. Embedding a digital watermark within an image serves as proof of ownership. The watermark is invisible to the naked eye but can be extracted to verify authenticity.

4. **Protecting Personal Privacy:**

   Individuals want to share private messages or personal information without the risk of interception. Personal photos shared on social media or through messaging apps can contain embedded messages that only the intended recipient can decode, ensuring privacy.

5. **Journalism and Whistleblowing:**

   Journalists and whistleblowers need to communicate sensitive information without revealing their sources or content. Embedding critical information within images allows journalists to share data with colleagues or the public without exposing the source of the information.

6. **Medical Data Security:**

   Healthcare providers need to protect patient information while sharing medical images.Embedding patient data within medical images (e.g., X-rays, MRIs) ensures that the information is securely transmitted and only accessible to authorized medical personnel.

7. **Anti-Counterfeiting Measures:**

Manufacturers need to verify the authenticity of their products and prevent counterfeiting.Embedding unique identifiers or serial numbers within product images ensures that only genuine products can be authenticated, helping to combat counterfeiting.

8. **Educational Institutions:**

   Schools and universities need to protect sensitive student data and internal documents. Embedding sensitive information within images used in presentations or shared documents ensures that the data is secure and only accessible to authorized staff and students.

These real-life scenarios highlight the versatility and importance of image steganography in enhancing security and privacy across various fields, from government and corporate environments to personal use and beyond.

4. Future Improvements

1. Optimize algorithms to embed larger messages without affecting image quality.
2. Use blockchain for a tamper-proof log of image and message transactions.
3. Now, we need all shares to reconstruct the original image , but we try to improve reconstruct image with less shares.

Conclusion:

Our project, "**Visual Cryptography and Secret Message Sharing**" demonstrates a significant advancement in cyber security through the innovative use of visual cryptography techniques. This project aimed to securely transmit a secret image by converting it into encrypted shares, which could only be reconstructed with the correct shares and password, ensuring high-level security and privacy.

Key Achievements:

1. Enhanced Security:

We successfully utilised visual cryptography to encrypt images into individually meaningless shares. This method ensures the original image remains secure even if some shares are intercepted.

2. Password Protection:

Adding a password layer to the decryption process provides an additional security measure. Without the correct password, the shares cannot be used to reconstruct the original image, significantly reducing the risk of unauthorized access.

3. Effective Share Generation and Reconstruction:

We developed a process to generate encrypted shares from an original image, allowing secure distribution over insecure channels. At the receiver's end, these shares can be combined and decrypted using the correct password to retrieve the original image.

4. User-Friendly Interface:

The encryption and decryption processes are designed to be simple and accessible. Users can easily upload an image, input a password, and generate shares, making the system practical for various applications.

Impact and Future Directions

1. Scalability and Optimization:

Future efforts will focus on optimizing the algorithms for faster processing and handling larger images, ensuring the system is scalable and efficient.

2. Doing from less shares:

Getting the secret message using fewer image shares is a very challenging task, although we are seeking any future improvements to get that solution.

3. Integration with Other Security Protocols:

Combining visual cryptography with other security measures like blockchain or quantum cryptography could further enhance the security framework, providing additional layers of protection.

4. Real-World Applications:

Deploying the system in real-world scenarios will offer insights into its practical applications and effectiveness. User feedback will help refine the system and address any challenges that arise.

5. Advanced Cryptographic Techniques:

Future research could explore integrating advanced cryptographic techniques such as homomorphic encryption, enabling computations on encrypted data and further enhancing security.

6. Cross-Platform Compatibility:

Developing cross-platform applications will ensure our solution is accessible and usable across various devices, catering to a broader audience.

References:

1. "**Visual Cryptography**" - Naor, M., & Shamir, A. (1994). Visual cryptography. *Advances in Cryptology — EUROCRYPT'94*. Lecture Notes in Computer Science, vol 950. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0053419
2. "**Superimposing**" - Horadam, K. J. (2003). Hadamard Matrices and Their Applications. *Princeton University Press*.
3. **"XOR"** - Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
4. "**CrypTool**" - CrypTool Team. (n.d.). CrypTool - Educational software project about cryptography and cryptanalysis. Retrieved from https://www.cryptool.org
5. "**Image Steganography**" - Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *IEEE Computer*, 31(2), 26-34. https://doi.org/10.1109/2.659930
6. **"LSB"** - Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3), 469-474. https://doi.org/10.1016/j.patcog.2003.08.007
7. **"ASCII"** - American National Standards Institute. (1986). *ANSI X3.4-1986: Coded Character Set - 7-bit American Standard Code for Information Interchange (ASCII)*. American National Standards Institute.

8. **“UTF-8”** - Yergeau, F. (2003). UTF-8, a transformation format of ISO 10646. *The Internet Society*. Retrieved from https://datatracker.ietf.org/doc/html/rfc3629

9. Naor, M., & Shamir, A.(1995).Visual Cryptography.Advances in Cryptoloreferencesgy—EUROCRYPT ’94,1–12
10. Kinger,S.(2013).Efficient Visual Cryptography using Random Grids. International Journal of Computer Applications, 74(21),1-5.
11. Image Steganography Based on Hamming Code and Edge Detection- The International Arab Journal of Information Technology 15(5)
12. Zhou L, Xiao Y, Pan Z, Cao Y and Ch0en W (2022) Visual Cryptography Using Binary Amplitude-Only Holograms. doi: 10.3389/fphot.2021.821304.
13. IEEE Transactions on Information Forensics and Security (Volume: 6, Issue:1, March 2011)
14. Visual Cryptography and Secret Image Sharing [BOOK] (EDITED BY STELVIO CIMATO, CHING-NUNG YANG)
15. Hide your secret messages in an Image! (Like the Cicada 3301) - Tech Raj YT.
16. https://www.youtube.com/watch?v=U2EK_gzAlh0&t=514s
17. CrypTool 2.1 (Stable Build 9778.2)