

SECURE DATA COMMUNICATION USING CRYPTOGRAPHY AND STEGANOGRAPHY

Submitted in partial fulfillment of the requirements for the award of Bachelor of
Engineering Degree in Electronics and Communication Engineering

by

MATLI NAVEEN KUMAR REDDY (40130267)

TIRUMURU NITHIN KUMAR REDDY (40130265)



**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
SCHOOL OF ELECTRICAL AND ELECTRONICS**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

CATEGORY -1 UNIVERSITY BY UGC

**Accredited with Grade “A++” by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119**

APRIL - 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A++" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **T.NITHIN KUMAR REDDY (40130265), M.NAVEEN KUMAR REDDY (40130267)** who carried out the Project entitled **"SECURE DATA COMMUNICATION USING CRYPTOGRAPHY AND STEGANOGRAPHY"** under our supervision from November 2023 to April 2024.

Internal Guide

Dr. P. CHITHRA, M.E, Ph.D.,

Head of the Department

Dr. T. RAVI, M.E, Ph.D.,

Submitted for Viva voce Examination held on

Internal Examiner

External Examiner

DECLARATION

I, **TIRUMURU NITHIN KUMAR REDDY** hereby declare that the Project Report entitled "**SECURE DATA COMMUNICATION USING CRYPTOGRAPHY AND STEGANOGRAPHY**" done by me under the guidance of **Dr. P. Chitra, M.E, Ph.D.,** Dept. of Electronics and Communication Engineering, **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI**, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in **ELECTRONICS AND COMMUNICATION ENGINEERING.**

DATE: 17-4-24

PLACE: Chennai

SIGNATURE OF THE CANDIDATE:

T. NKR

DECLARATION

I, **MATLA NAVEEN KUMAR REDDY** here by declare that the Project Report entitled "**SECURE DATA COMMUNICATION USING CRYPTOGRAPHY AND STEGANOGRAPHY**" done by me under the guidance of **Dr. P. Chitra, M.E, Ph.D.,** Dept. of Electronics and Communication Engineering, **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI**, is submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in **ELECTRONICS AND COMMUNICATION ENGINEERING.**

DATE: 17-4-24

PLACE: Chennai

SIGNATURE OF THE CANDIDATE:

M. Naveen

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **The Board of Management of SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. N.M. NANDHITHA M.E., Ph.D., Dean, School of Electrical and Electronics Engineering, and Dr. T. RAVI M.E., Ph.D., Head of the Department of Electronics and Communication Engineering** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. P. CHITRA, Ph.D.**, dept. of Electronics and Communication Engineering for her valuable guidance, suggestions, and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Communication Engineering who were helpful in many ways for the completion of the project.

ABSTRACT

In today's technology environment, information security is one of the most difficult issues to solve. Various strategies have been proposed during the last decade to safeguard the transmission of secret data over the public network (Internet). Still there is a scope for the researchers to develop novel technique for secure data transmission.

A new algorithm is proposed for secure data transmission is the integration of cryptography and steganography which are the two major methods for securing, hiding and transmission of messages separately. These methods used information in order to cipher or cover their existence respectively. Crypto - steganography method is aimed for a better information security. The proposed algorithm can be implemented by using LSB - based steganography method and XOR-Cryptography for encryption and decryption of picture and secret key

INDEX

CHAPTER NO.	TITLE	PAGE NO.
	LIST OF CONTENT	
	LIST OF FIGURES	
	LIST OF TABLES	
1	INTRODUCTION	1
	1.1 Communication	1
	1.2 Secure Data Transfer	1
	1.3 Cryptography	2
	1.4 History of Cryptography	2
	1.5 Steps to Perform cryptography	3
	1.5.1 Choose an appropriate algorithm	3
	1.5.2 Generate keys	3
	1.6 Advantages of Cryptography	3
	1.6.1 Security	3
	1.6.2 Privacy	3
	1.6.3 Disadvantages of cryptography	4
	1.7 Steganography	4
	1.7.1 History of Steganography	5
	1.7.2 Types of Steganography	6
	1.7.3 Advantages of steganography	6
	1.7.4 DisAdvantages of steganography	7
	1.8 Background of the problem	8

2	LITERATURE SURVEY	9
	2.1 Previous work on crypto & steganograph	9
3	INFORMATION SECURITY TECHNIQUES	13
	3.1 Information Security	13
	3.2 Information Availability	14
	3.3 Cryptography	16
	3.3.1 Symmetric Encryption	18
	3.3.2 Asymmetric Encryption	20
	3.4 Steganography	21
	3.4.1 DWT Algorithm	23
	3.4.2 DCT Algorithm	23
	3.4.3 LSB Algorithm	24
4	METHODOLOGY	26
	4.1 Encrytion	26
	4.2 Encryption Phase	26
	4.2.1 Hiding Image in Another Image	28
	4.3 Transmission Phase	29
	4.4 Decryption Phase	29
	4.4.1 Extraction of secret image	29
5	RESULTS AND DISCUSSION	31
6	REFERENCES	37

LIST OF TABLES

TABLE NO.	CONTENTS	PAGE NO.
3.1	Algorithm Comparison	19
3.2	<u>Comparison of technologies</u>	<u>22</u>

LIST OF FIGURES

FIGURE NO.	FIGURES NAMES	Pg no.
3.1	General model of cryptographic System	13
3.2	Symmetric Encryption	16
3.3	Asymmetric Encryption	21
3.4	Pure Steganography Process	25
3.5	Process of secret key steganography	25
4.1	Proposed Methodology block diagram	26
4.2	XOR cryptography process	26
4.3	Flowchart of cryptography	28

LIST OF FIGURES

FIGURE NO.	FIGURES NAMES	PAGE NO.
4.4	LSB steganography process	28
4.5	Flowchart of Steganography	29
4.6	Flowchart of combined process of cryptography & steganography	30
5.2	Main Image	32
5.2.2	Secret Image	32
5.2.3	Encrypted Secret Message	32
5.2.4	Stegmented Image	33
5.2.5	Recovered Encrypted Image for Steganography	33
5.2.6	Decrypted Secret Message Image	33
5.3	Sample output 2	34
5.4	Sample output 3	35

CHAPTER 1

INTRODUCTION

1. Communication

Communication is the process of exchanging information, ideas, or messages between individuals or groups. It can take many different forms, including verbal or nonverbal communication, written communication, and digital communication. Effective communication is essential for building and maintaining relationships, achieving goals, and resolving conflicts. Some key elements of effective communication include active listening, clarity, empathy, and understanding the audience or recipient of the message. Communication skills can be developed and improved with practice and feedback.

2. Secure Data Transfer

Secure data transfer is the process of transmitting information between two parties in a way that ensures confidentiality, integrity, and availability of the data. This is particularly important when sensitive or confidential information is being transmitted, such as personal information, financial data, or trade secrets.

To ensure secure data transfer, encryption is often used. Encryption is the process of encoding data in such a way that it can only be read by someone who has the necessary decryption key. This can be done using various encryption algorithms such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), or Elliptic Curve Cryptography (ECC).

In addition to encryption, other security measures such as digital certificates and secure communication protocols (such as HTTPS or SSH) can be used to protect against unauthorized access and ensure the authenticity of the data being transmitted.

3. Cryptography

Cryptography is the practice of securing communication from adversaries or eavesdroppers by transforming messages into an unintelligible form that can only be read by the intended recipients who possess the necessary key or information. Cryptography involves using mathematical algorithms and techniques to ensure that information remains confidential, authentic, and tamper-proof.

There are two primary types of cryptography: symmetric and asymmetric. In symmetric cryptography, the same secret key is used to both encrypt and decrypt the message. This means that the sender and recipient must both have the same secret key. Examples of symmetric algorithms include the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES).

Cryptography is widely used in various areas such as secure communication, digital signatures, and digital certificates, protecting personal information, securing online transactions, and ensuring the authenticity of electronic documents.

4. History of Cryptography

Cryptography has a long and fascinating history that can be traced back to ancient civilizations. The first known use of cryptography was by the ancient Egyptians, who used hieroglyphs to encode their messages. The Greeks also made significant contributions to the development of cryptography. The famous Scytale was a cryptographic device used by the Spartans in the 5th century BC to send secret messages. The device was a wooden rod around which a strip of parchment was wrapped, and the message was written across the parchment. When the parchment was unwrapped, the message appeared scrambled and could only be read if the recipient had a rod of the same size and shape to wrap it around.

5. Steps to perform cryptography

The steps to perform cryptography depend on the type of cryptography being used. However, in general, the following steps can be taken to perform cryptography

1. Choose an appropriate algorithm:

The first step in performing cryptography is to select an appropriate algorithm based on the requirements of the task at hand. The algorithm should be secure, efficient, and appropriate for the type of data being encrypted.

2. Generate keys:

Depending on the type of cryptography being used, one or two keys may need to be generated. For symmetric key cryptography, a single key is used for both encryption and decryption, and it needs to be securely shared between the sender and receiver. For asymmetric key cryptography, a public key and private key are generated, with the public key being shared publicly, and the private key being kept secret.

6. Advantages of Cryptography

1. Security:

Cryptography helps establish trust and provides a layer of security in digital communication and transactions. By ensuring that data is encrypted, authenticated, and verified, cryptography helps create a secure environment for online activities, fostering trust between parties.

2. Privacy:

Cryptography helps protect privacy by ensuring that sensitive information remains confidential and secure. This is particularly important in contexts where privacy is paramount, such as healthcare, where patient data must be protected, and in communications where individuals have a right to privacy.

Cryptography provides mechanisms to ensure the integrity of information, meaning that any unauthorized changes to the data can be detected.

Cryptographic techniques like digital signatures can be used to verify the authenticity of data and ensure that it has not been tampered with during transmission or storage

3. Disadvantages of cryptography

While cryptography is a powerful tool for securing information, it also has some potential disadvantages, including

4. Key management:

One of the most significant challenges of cryptography is managing the keys used to encrypt and decrypt messages. If keys are not properly managed, they can be lost, stolen, or misused, compromising the security of the information.

5. Legal restrictions:

The use of certain types of cryptography may be subject to legal restrictions in some countries, which can limit their use in certain contexts.

1.7 Steganography

Steganography is the practice of hiding secret information within non-secret data, such as images, audio files, or text messages. Unlike encryption, which aims to make data unreadable to unauthorized parties, steganography aims to conceal the existence of the information.

The techniques used in steganography include replacing certain bits in a file with the secret information, using the least significant bits of a pixel in an image to hide information, or embedding information in the whitespace of a document. The goal is to make the hidden information difficult to detect without knowing where to look and without altering the visible data.

Steganography has been used throughout history for covert communication, espionage, and even as a tool for criminals to conceal their activities. Today, it is also used as a security measure to protect sensitive data from being intercepted and to prevent unauthorized access. However, steganography can also be used for malicious purposes, such as hiding malware in legitimate files. As a result, it is an area of ongoing research and development in the field of cyber security.

1.7.1 History of Steganography

One of the reasons that intruders can be successful in tracking information is that information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organisation, or use it to launch an attack. One solution to this problem is through the use of Steganography. Steganography is a key technology for achieving information security in communications, computer systems, electronic commerce, and in the emerging information society.

Some examples of use of Steganography in past times are:

During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruitjuices were used, because when each one of these substances is heated they darken and become visible to the human eye.

In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secret message.

During the World War II, the Germans invented the use of microdots. Image containing great details were scaled down to the size of microdots. The 2 German usage of secret sharing is regarded as the recent evolution of steganography.

1.7.2 Types of Steganography

Image Steganography

Hiding the information by taking the spread item as picture is alluded as Picture Steganography. In Picture Steganography pixel intensities are utilized to shroud the information. In computerized Steganography, pictures are generally utilized spread source in light of the fact that there are number of bits presents in computerized representation of a picture.

Audio Steganography

It includes concealing information in sound records. This technique shrouds the information in WAV, AU and MP3 sound records. There are distinctive for sound Steganography.

These Strategies are

- i. Low Bit Encoding
- ii. Phase Coding
- iii. Spread Spectrum.

Video Steganography

It is a procedure of concealing any sort of documents or information into computerized video position. For this situation video (mix of pictures) is utilized as bearer for concealing the information. By the large discrete cosine change (DCT) adjust the qualities (e.g., 8.667 to 9) which a video to show the information in each of the pictures in the video, which is unnoticeable by the human eye. H.264, MP4, MPEG, AVI are the arrangements utilized by Video Steganography.

1.7.3 Advantages Of Steganography

Concealment of sensitive information:

Steganography allows information to be concealed within other seemingly innocent information, such as images, audio files, or text documents. This

means that even if someone gains access to the carrier data, they may not be aware that there is hidden information within it. Which is difficult for unauthorized individuals to access or steal it.

Communication secrecy:

Steganography provides an additional layer of security for confidential information, making it more difficult for unauthorized individuals to access it. Even if someone knows that steganography is being used, they would need specialized tools to extract the hidden information.

Data protection:

Data protection is a crucial aspect of steganography, as it involves hiding sensitive information within other data to protect it from unauthorized access and it can be used to protect important data from being destroyed or altered, by embedding it in a seemingly harmless file.

Avoiding censorship:

Steganography can be used to bypass censorship by disguising the content of a message, which can be useful for people living in countries with restrictive internet policies.

1.7.4 Disadvantages of Steganography

Detection:

Steganography can be difficult to detect, which can be both an advantage and a disadvantage. If someone is using steganography to hide malicious or illegal activities, it can be very difficult for authorities to detect and prevent these activities.

Limited data capacity:

Steganography has a limited capacity for data, meaning the amount of secret information that can be hidden within the carrier data is limited by the size of the carrier data. This can be a disadvantage if a large amount of secret information needs to be transmitted.

File size increase:

The process of hiding information within a file can cause the file size to increase, making it more obvious and easier to detect.

Complexity:

Steganography can be a complex process, Using steganography can be more complex than using other encryption methods, as it requires specialized software and expertise. This can make it less accessible to the average user.

1.8 Background of the Problem

Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography include an array of secret communication methods that hide the message from being seen or discovered. Military communications system make increasing use of traffic security technique which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections.

CHAPTER 2

LITERATURE SURVEY

2.1 Previous Work on Cryptography & Steganography

K.C.Nunna.et.al proposed the use of cryptography and image steganography to ensure secure data transfer over the internet. Cryptography is used to encrypt the data while image steganography is used to hide the encrypted data within an image file. The authors propose a method for combining these two techniques to create a more robust security system. The proposed system first encrypts the data using Advanced Encryption Standard (AES) and then hides it within the Least Significant Bits (LSBs) of an image file using image steganography. The authors have implemented and tested the proposed system and achieved satisfactory results in terms of security and data transfer speed. The system has potential applications in areas such as military communication, healthcare, and banking [1].

Ahmad El Oualkadi.et.al proposed an overview of visual cryptographic systems that are based on the XOR function. XOR-based visual cryptography involves dividing an image into multiple shares that are then distributed to different parties. These shares are typically in the form of black and white images. When these shares are superimposed using the XOR function, the original image is revealed. The paper presents a brief history of visual cryptography and explains the basics of XOR- based visual cryptography. The authors also discuss various existing techniques and algorithms used in XOR-based visual cryptography. Finally, the paper concludes by highlighting the advantages and limitations of these systems [2].

S.M.Karim proposed the concepts of steganography and cryptography and highlight their individual strengths and weaknesses. They then explore the potential benefits of combining the two techniques and present a comprehensive review of recent research in this area. The authors discuss various steganographic and cryptographic algorithms, including their advantages and limitations, and compare their performance in terms of security, robustness, and computational complexity. The authors conclude that the combination of steganography and cryptography can significantly enhance data security and privacy in various applications, including digital image and video transmission, text messaging, and online transactions [7].

Flevina Jonese d'souza.et.al proposes a hybrid approach for image security by combining encryption and steganography. The authors suggest using the Advanced Encryption Standard (AES) algorithm for encryption and the Least Significant Bit (LSB) steganography technique for hiding secret information in the cover image.

The proposed method uses a secret key to encrypt the plaintext and then hides the encrypted message in the cover image using LSB steganography. The authors evaluate the performance of the proposed method by testing it on several standard images and measuring the image quality, security, and robustness. The results show that the proposed method provides good security and robustness against various attacks, such as steganalysis and brute-force attacks. The authors conclude that the proposed hybrid approach can be useful in applications that require secure and robust image transmission over the internet[8].

K.Thangadurai.et.al proposed an analysis of Least Significant Bit (LSB) based image steganography techniques. The authors evaluate several LSB-based techniques, including LSB replacement, LSB matching, and LSB matching revisited, in terms of

their performance, capacity, and security. The authors also discuss the advantages and disadvantages of each technique and compare their effectiveness in hiding secret information in the cover image. The authors conduct experiments using several standard images and measure the quality of the stego image, the hiding capacity, and the security against various attacks. The results show that LSB matching revisited provides better performance, capacity, and security than the other two techniques. The authors conclude that LSB-based steganography can be an effective method for hiding secret information in images, but the choice of the technique should be based on the specific requirements of the application[9].

R.Bhardwaj.et.al proposes an enhanced method for securing image steganography by using image encryption. The authors suggest using the Advanced Encryption Standard (AES) algorithm to encrypt the cover image before hiding the secret message in it using the Least Significant Bit (LSB) technique. The proposed method uses a secret key for both encryption and decryption of the image and the message[10].

R.Dhanaraj.et.al proposes an enhanced blend of image steganography and cryptography to achieve higher security and capacity for hiding secret messages in images. The authors suggest combining the Least Significant Bit (LSB) technique with the Advanced Encryption Standard (AES) algorithm to encrypt the secret message before hiding it in the cover image. The proposed method uses a secret key for both encryption and decryption of the image and the message. The authors evaluate the performance of the proposed method by testing it on several standard images and measuring the image quality, capacity, and security. The results show that the proposed method provides higher security and capacity compared to the traditional LSB-based steganography. The authors conclude that the proposed enhanced blend can be useful in applications that require higher security and larger capacity for hidden messages[11].

W.Stallings.et.al proposed a book that is organized into chapters that provide a detailed analysis of cryptographic algorithms, symmetric key encryption, and message authentication codes. It also explores topics such as secure email, web security, and network security management. The book includes numerous examples, case studies, and practice exercises that help readers to understand the concepts and techniques of cryptography and network security. Overall, the book is a valuable resource for students and professionals who are interested in learning about the principles and practice of cryptography and network security[12].

Latif.et.al evaluated the performance of different cryptography algorithms using LabVIEW software. The study compared the time required for encryption and decryption processes of three popular cryptography algorithms: AES, DES, and RSA. The author used different key sizes and block sizes to evaluate the impact on the processing time. The study found that the AES algorithm was the fastest among the three algorithms tested, followed by DES and RSA. The study also found that increasing the key and block sizes resulted in longer processing times for all algorithms. The results of the study can be useful for choosing the appropriate cryptography algorithm for a specific application, depending on the required level of security and the available computing resources[13].

Nitendra Kumar Vishwakarma.et.al proposed a comparative analysis of different techniques used for cryptography. The study compares five popular cryptography techniques: Caesar cipher, Playfair cipher, Hill cipher, RSA algorithm, and AES algorithm.. However, the author also noted that the level of security provided by a cryptography technique depends on the key size, and larger key sizes increase the level of security but also increase the computational complexity. The study provide useful insights into the trade-offs involved in choosing a cryptography technique for a specific application, based on the required level of security and available computing resources[14].

Buchanan.et.al proposess the role of encryption in security and forensic computing. The author provides an overview of encryption and its history, including the different types of encryption techniques such as symmetric and asymmetric encryption. The article also discusses the use of encryption in securing communication channels, data storage, and authentication processes. Furthermore, the author highlights the challenges associated with encryption, such as the need for key management and the potential for key exposure or attacks. The article concludes by emphasizing the importance of encryption in modern-day computing and the need for further research in this field to improve encryption techniques and strengthen security[15].

CHAPTER 3

INFORMATION SECURITY TECHNIQUES

3.1 Information Security

In general, security denotes "the quality or state of being secure to be free from danger". Information security refers to the practice of protecting information from unauthorized access, use, disclosure, disruption modification or destruction, in order to ensure its confidentiality, integrity and availability. It encompasses various layers of security that work together to provide comprehensive protection to information assets.

Physical security:

Physical security involves securing the physical environment where information assets are stored or processed. This includes measures such as access controls to restricted areas, surveillance systems, security guards, locks, and alarms to prevent unauthorized physical access to facilities and equipment.

Personal security:

Physical security involves securing the physical environment where information assets are stored or processed. This includes measures such as access controls to restricted areas, surveillance systems, security guards, locks, and alarms to prevent unauthorized physical access to facilities and equipment.

Operational security:

Operational security, also known as OPSEC (Operations Security), involves safeguarding the operational processes, procedures, and activities within an organization. It focuses on protecting sensitive information related to an

organization's operations, activities, and resources to prevent unauthorized access or compromise. Operational security measures may include restricting access to operational areas or facilities, implementing access controls and authentication mechanisms, monitoring and logging activities, and enforcing policies and procedures to ensure that sensitive operational information is protected from unauthorized disclosure, tampering, or misuse.

Security Awareness and Training:

Human factors play a critical role in information security. Security awareness and training programs help educate employees and users about information security best practices, policies, and procedures. This includes training on topics such as password hygiene, phishing awareness, social engineering, and other security-related topics to reduce the risk of human error and promote a security-conscious culture.

3.2 Information security:

Information security is the protection of information and the systems and hardware that use, store, and transmit that information. Information security can be defined as measures adopted to prevent the unauthorized use or modification of use of data or capabilities.

Human factors play a critical role in information security. Security awareness and training programs help educate employees and users about information security best practices, policies, and procedures. This includes training on topics such as password hygiene, phishing awareness, social engineering, and other security-related topics to reduce the risk of human error and promote a security-conscious culture.

Availability:

It is the prevention of unauthorized disclosure of information. It enables users who need access the information to do so without any interference or obstruction and to receive it in the required format. The availability of information requires the

verification of the user as one with authorized access to information. In other words the availability can be defined as "Ensuring timely and reliable access to make use of information. A loss of availability is the disruption of access to or use of information or an information system".

Accuracy:

Information should be accurate, meaning it is correct, reliable, and free from errors or distortions. Accurate information is based on factual data and provides a true representation of reality. Inaccurate information can lead to incorrect conclusions, poor decision-making, and potential negative consequences.

Confidentiality:

"The confidentiality is the quality or state of preventing disclosure or exposure to unauthorized individuals or system". Confidentiality is basically privacy and secrecy which means protection of personal data or that of data belonging to an organization. Confidentiality of information ensures that only those with the rights and privileges access a particular set of information and prevent from unauthorized access.

Prevention:

Prevention measures are designed to proactively minimize the likelihood of security incidents or attacks from occurring. This may include implementing strong access controls, using firewalls to filter incoming and outgoing network traffic, keeping software and systems up-to-date with the latest patches and updates, using strong authentication mechanisms (such as multi-factor authentication), and employing encryption techniques to protect sensitive data. Additionally, user awareness training and education can play a crucial role in preventing security incidents by educating employees about best practices for safe online behavior and how to recognize and avoid common security threats, such as phishing attacks.

Respons

Response measure involve taking immediate action in response to detected security incident or attack. This may include isolating affected systems from the network, blocking suspicious traffic, disabling compromised user accounts, changing passwords and implementing other mitigation strategies to contain the incident and prevent further damage. Incident response plans and procedures should be in place, outlining the roles and responsibilities of incident response team members, communication channels, and steps to be followed in case of a security incident.

Recovery:

Recovery measures involve restoring systems and data to their normal state after a security incident or attack. This may include restoring from backups, applying patches or updates to fix vulnerabilities, reconfiguring systems to a secure state, and conducting thorough post-incident investigations to understand the root cause of the incident and identify areas for improvement. The goal of recovery measures is to restore normal operations as quickly as possible and minimize the impact of the incident.

3.3 Cryptography

The word cryptography is derived from two Greek words which mean "secret writing". Cryptography is the process of scrambling the original text by rearranging and substituting the original text, arranging it in a seemingly unreadable format for others. Cryptography is an effective way to protect the information that is transmitting through the network communication paths.

Cryptology is the science that deals about cryptography and cryptanalysis. Cryptography is the approach of sending the messages secretly and securely to the destination. Cryptanalysis is the method of obtaining the embedded messages into original texts.

In general, cryptography is transferring data from source to destination by altering it through a secret code. The cryptosystems uses a plaintext as an input and generate a cipher text using encryption algorithm taking secret key as input. The important elements in cryptosystems are

1. Encryption algorithm
2. Secret key
3. Chiper text
4. Decryption algorithm

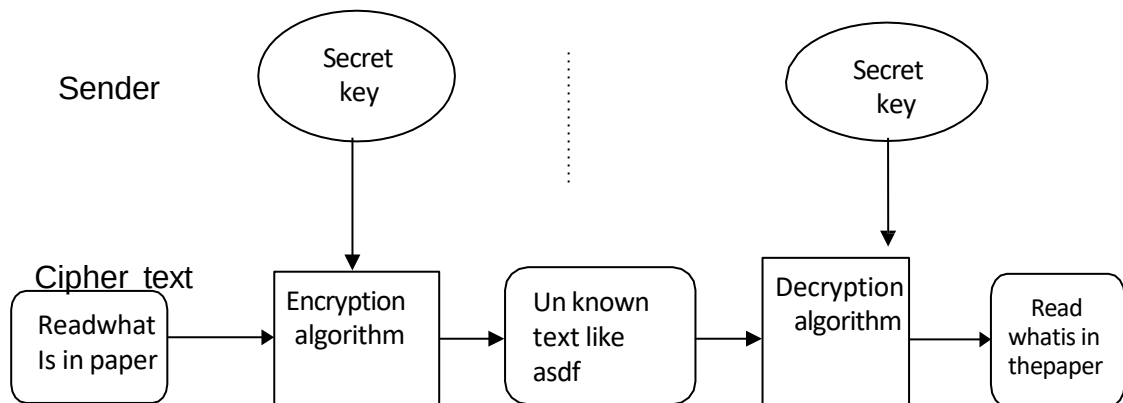


Fig 3.1: General model of cryptographic System

Plain text:

Plain text refers to the original, unencrypted message or data that is input into the cryptosystem for encryption. It can be any type of digital data, such as text, numbers, or other forms of data.

Encryption algorithm:

The encryption algorithm is a mathematical process or set of rules used to transform the plain text into cipher text. It determines how the data will be transformed and how the encryption will be performed. Common encryption algorithms include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and DES (Data Encryption Standard).

Secret key:

The secret key is a piece of information that is known only to the authorized parties involved in the communication or data exchange. It is used as input to the encryption algorithm to produce the cipher text and as input to the decryption algorithm to recover the plain text from the cipher text. The secrecy

and confidentiality of the secret key are crucial to the security of the cryptosystem.

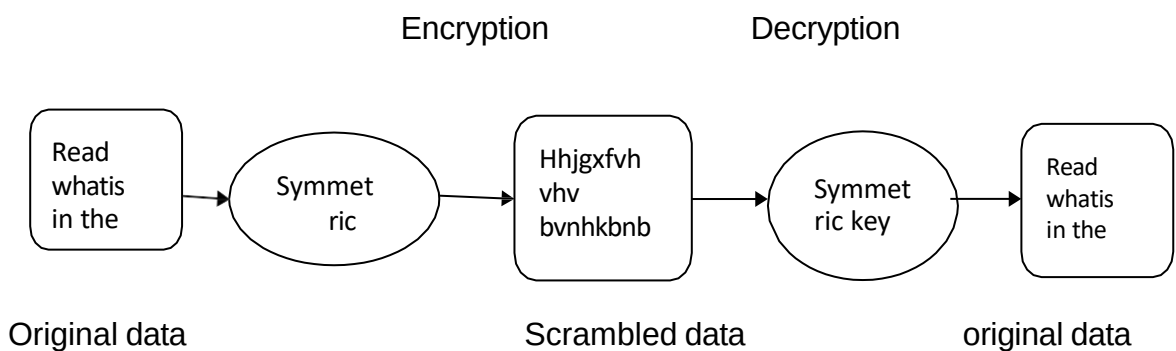
Cipher text:

Cipher text refers to the encrypted form of the plain text that is generated by the encryption algorithm using the secret key. It is usually a scrambled or unintelligible form of the original plain text, and it is intended to be unreadable and meaningless to unauthorized parties who do not possess the secret key.

3.3.1 Symmetric Encryption

Symmetric encryption is also known as secret key or private key encryption, this type of algorithm uses the same secret key for both encryption and decryption. The sender and receiver must share the same secret key and keep it confidential.

Examples of symmetric key encryption algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple Data Encryption Standard) as shown in below fig 3.2



There are two types of methods that will attack on symmetric encryption systems. The first one is Cryptanalysis. If the attacker gets to know some information about the plain text and cipher text, he analyses the characteristics of the algorithms used for encryption and tries to generate keys. The second type of attack is known as "brute force attack". In this type of attack, the defender attempts to know the cipher text and try every possible

key for translation. To avoid this problem, the user should use the key that no longer can be estimated like 128 or 168 bit keys.

The different symmetric encryption algorithms are

- Data Encryption Standard
- Advanced Encryption Standard

Table 3.1: Algorithm Comparison

Parameters	DES	3DES	RC5	DEA	AES
Key Size	64	112	128	128	128,192
Block Size	64	64	34,64	64	128
Attacks	Brute force attacks	Differential and related key	Co-relation and timing attacks	Linear attack	Side channel Attacks
Level of security	Adequate security	Adequate security	Secure	Secure	Excellent security
Encryption Speed	Very slow	Very slow	slow	Fast	Fast

Data Encryption Standard (DES):

"Data Encryption Standard" (DES) is also known as Data Encryption Algorithm (DEA). DEA takes 64 bits of plain text and 56 bits of key to produce 64 bits cipher text block. The DES algorithm always functions on blocks of equal size and uses the permutations and substitutions in algorithm

The data encryption algorithm uses 56 bit key so it is not possible for the defender for analysing the key. So, the problem of Cryptanalysis is avoided using this algorithm. But the drawback of the algorithm is Brute-force attack. This can be avoided using the Triple DES algorithm

Triple DES is an extension to the DES algorithm. Triple DES uses the same approach for encryption as DES. 3DES takes three 64 bit keys which has a total length of 192 bits. We can give more than one key that is two or three keys for encryption as well as for decryption such that the security will be stronger. It is approximately 256 times stronger than the normal DES algorithm, so that this algorithm can avoid the brute force attack. The main drawback of using 3DES algorithm is that the number of calculations is high reducing the speed to a greater extent. And the second drawback is that both DES and 3DES use same 64 block size to avoid security issues. "Advanced Encryption Standard" algorithms are used to avoid these limitations.

3.3.2 Asymmetric Encryption

"Asymmetric encryption" is also known as "Public key encryption". The AES works same as Symmetric encryption, the main difference between AES and Symmetric encryption is in using keys. In asymmetric encryption, the encryption and decryption will be done by two different keys. It will use plain text, encryption algorithm and decryption algorithm same as Symmetric encryption as discussed in above section. The block diagram of Asymmetric encryption. Any data encrypted with the public key can only be decrypted with the corresponding private key, and vice versa. Examples of asymmetric key encryption algorithms include RSA (Rivest- Shamir-Adleman), DSA (Digital Signature Algorithm), and ECC (Elliptic Curve

Cryptography) as shown in below fig 3.3

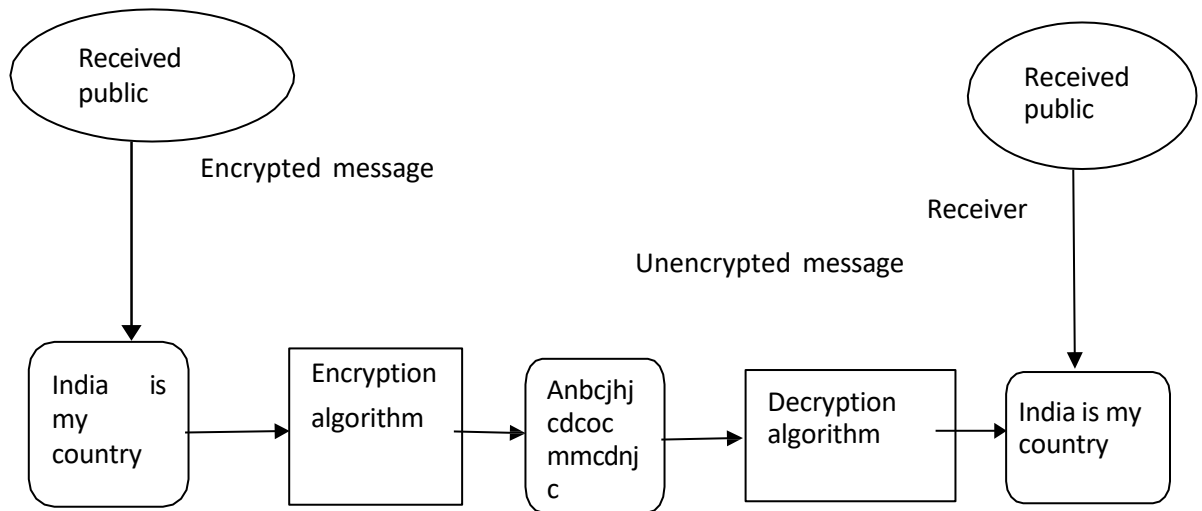


fig 3.3: Asymmetric Encryption

In "Asymmetric encryption", only the data that is encrypted using public key can be decrypted using the same algorithm. And the message which is encrypted using private key can be decrypted using only the matching public key. The main problem with Asymmetric algorithm is "cipher keys". Whenever two different people want to exchange the data simultaneously using asymmetric encryption they need to have four different keys. It will be more confusing to resolve as the corresponding key is required for the particular file to open.

3.4 Steganography

Steganography in Greek means "covered writing". Steganography is the process of hiding the one information into other sources of information like text, image or audio file, so that it is not visible to the natural view. There are varieties of steganographic techniques available to hide the data depending upon the carriers we use.

Steganography and cryptography both are used for the purpose of sending the data securely. The same approach is followed in Steganography as in cryptography like encryption, decryption and secret key. In Steganography the message is kept secret without any changes but in cryptography the original content of the message is differed in different stages like encryption and decryption.

Steganography supports different types of digital formats that are used for hiding the data. These files are known as carriers. Depending upon the redundancy of the object the suitable formats are used. "Redundancy" is the process of providing better accuracy for the object that is used for display by the bits of object.

The main file formats that are used for Steganography are Text, images, audio, video, protocol.

While performing steganography, the cover image is divided into pixels for easy embedding. And mostly the techniques used for this purpose is

1. DWT technique
2. DCT technique
3. LSB technique

Table 3.2: Comparison of technologies

Existed Technologies	Spatial Domain	Capacity	Robustness
L.S.B-Least Significant Bit	YES	HIGH	HIGH
DCT-Discrete Cosine Transform	NO	MEDIUM	HIGH
D.W.T- Discrete Wavelet Transform	NO	MEDIUM	LOW

1. Discrete Wavelet Transform (DWT):

Discrete wavelet transforms are used to convert the image in spatial domain to frequency domain, where the wavelet coefficients so generated, are modified to conceal the image. In this kind of transformation the wavelet coefficients separates the high and low frequency information on a pixel to pixel basis. The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. It represents the data into a set of high pass (detail) and low pass (approximate) coefficients. When DWT is applied on an image, it divides the image in frequency components.

The low frequency components are approximate coefficients holding almost the original image and high frequency components are detailed coefficients holding additional information about the image.

2. Discrete Cosine Transform (DCT):

DCT is a signal processing technique that is a popular and frequently used transformation function. This transformation has the function of converting the signal type from spatial domain to frequency domain. Because of its excellent performance, this technique has been widely used in many fields, such as image compression, pattern recognition, and other image processing.

Basically, DCT changes the color of the original image, but because of the limitations of the human senses, the changes are not visible. In research, it has been shown that DCT is superior in terms of stego image quality compared to wavelet transforms. It is just because the cover image is broken down into small sub-blocks the process becomes more complicated.

Messages embedded with the DCT method also proved more resilient than JPEG attacks.

The different types of Steganographic techniques that are available are

1. Pure Steganography
2. Secret key Steganography

3.4.3 LSBAlgorithm

LSB (Least Significant Bit) steganography is a technique used to hide information within a digital file, such as an image, audio file, or text file, without changing the perceptual quality of the file. It is a form of steganography, which is a practice of concealing messages or data within other seemingly innocuous data.

In LSB steganography, the least significant bit of each byte or pixel in the cover file is modified to represent a bit of the hidden message. The least significant bit is the rightmost bit in a binary representation of a number, and it has the least impact on the numerical value of the byte or pixel. Modifying the least significant bit usually results in minimal visual or audible changes, and the cover file appears unchanged to human perception.

For example, let's consider an 8-bit gray scale image where each pixel is represented by a single byte. The value of the byte ranges from 0 to 255, which in binary is represented as 8 bits (e.g., 00101101). In LSB steganography, the least significant bit of each byte can be used to store a bit of the hidden message. For instance, if we want to hide the binary message "01010101" within the image, we would modify the least significant bit of each byte in the image to match the corresponding bit in the message, without changing the other bits.

Pure Steganography:

Pure Steganography is the process of embedding the data into the object without using any private keys. This type of Steganography entirely depends upon the secrecy. This type of Steganography uses a cover image in which data is to be embedded, personal information to be transmitted and encryption decryption algorithms to embed the message into image. The block diagram of pure steganography process is as shown in Fig 3.4

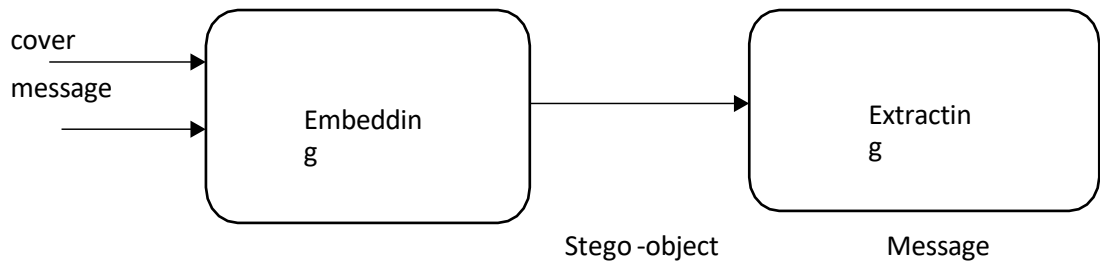


fig3.4: Pure Steganography Process

This type of steganography cannot provide the better security because it is easy for extracting the message if the unauthorized person knows the embedding method. It has one advantage that it reduces the difficulty in key sharing.

Secret key Steganography:

Secret Key steganography is another process of steganography which uses the same procedure other than using secure keys. It uses the individual key for embedding the data into the object which is similar to symmetric key. For decryption it uses the same key which is used for encryption.

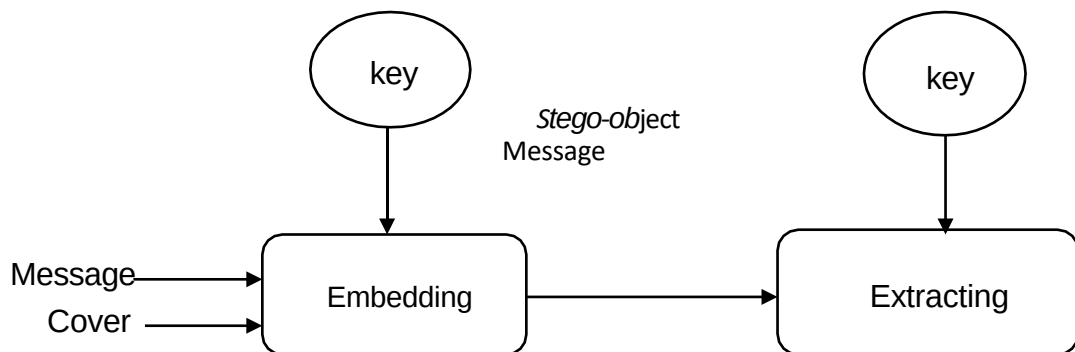


Fig 3.5: Process of secret key steganography

CHAPTER 4

METHODOLOGY

4.1 : Encryption

Before encryption and decryption, consider secret image which we want to transmit. Secret image will be embedded in carrier image by using the secret keys by the process of encryption algorithm. The resultant image is stego image which is transmitted through channel. At the receiver secret information will be recovered by using same three secret keys which are used at transmitter by the process of decryption algorithm. The block diagram of steganography is as shown in below Fig 4.1.

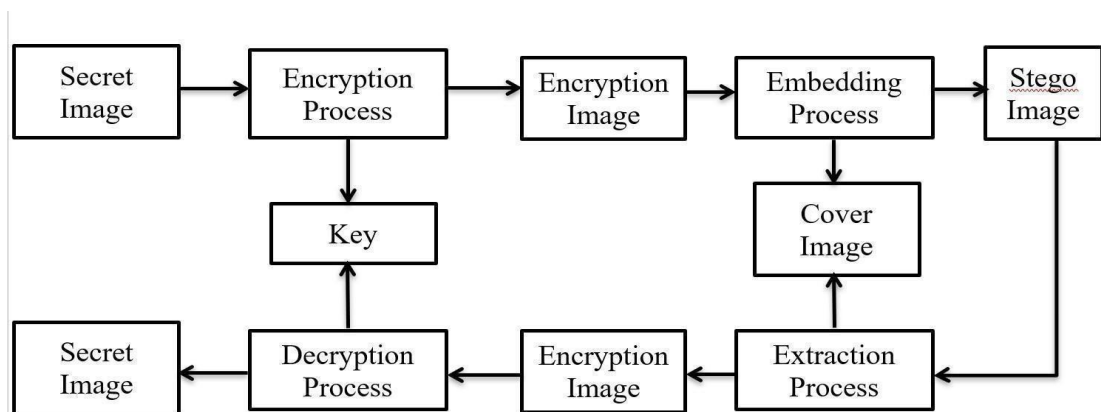


Fig 4.1: Proposed Methodology block diagram

4.2 Encryption Phase

In the Encryption process we use XOR Cryptography process XOR encryption is a simple and efficient encryption technique that can be used to encrypt images. The encryption process of XOR cryptography for an image involves the following steps:

Convert the image into binary format: Before encrypting the image using XOR, it is necessary to convert it into a binary format. This can be done by representing each pixel in the image as a binary value.

Generate a random key: A random key of the same length as the binary image is generated. This key should be kept secret and shared only with the intended recipient.

XOR the binary image with the key: Each bit of the binary image is XORed with the corresponding bit in the key. This produces a new binary string, which represents the encrypted image.

Convert the encrypted binary image back into an image format: The encrypted binary string can be converted back into an image format by reversing the process used to convert the original image into a binary format.

XOR Cryptography, also known as XOR encryption, is a simple encryption process that uses the XOR (exclusive OR) logical operator to encrypt and decrypt data.

The XOR operation returns a value of 1 if the corresponding bits of two operands are different and 0 if they are the same. Using this method the XOR encryption works by applying an XOR operation between the plain text message and a secret key. The resulting cipher text can only be decrypted by performing the same XOR operation between the ciphertext and the same secret key.

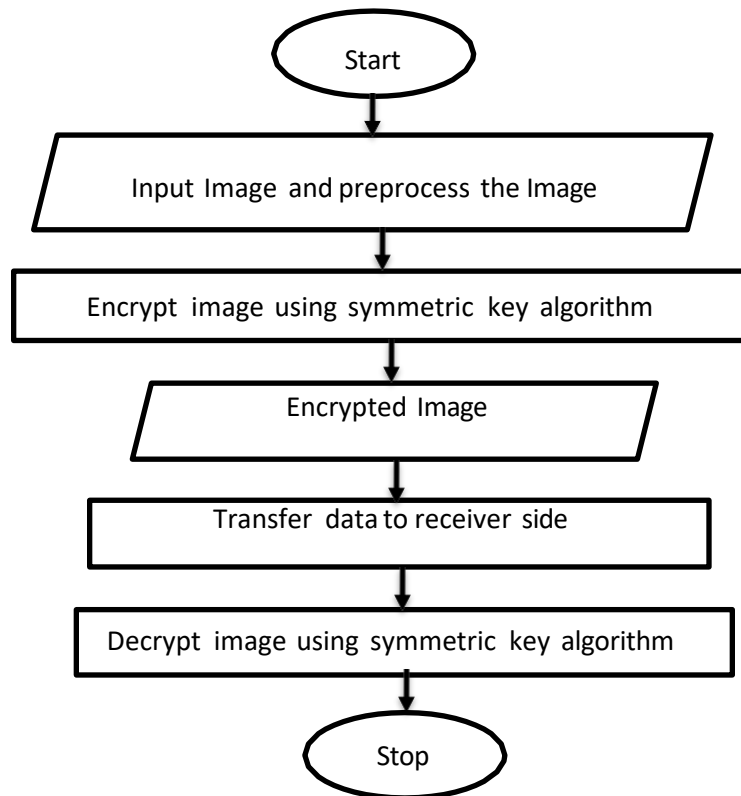


Fig 4.3: Flowchart of cryptography

4.2.1 Hiding image in Another image

LSB (Least Significant Bit) steganography is a technique used to hide a message within a digital image.

Encryption can be added to this process to provide additional security to the hidden message. Here is a general overview of how encryption can be added to the LSB steganography process:

Generate a secret key: A secret key is a unique piece of information that is used to encrypt and decrypt the hidden message. It should be kept secret between the sender and the receiver.

Convert the message into a binary format: The message that needs to be hidden is converted into binary format so that it can be easily embedded in the digital image using the LSB technique.

Encrypt the binary message using the secret key: The binary message is encrypted using a symmetric encryption algorithm, such as AES or DES, along with the secret key. The encrypted message is then converted back to binary format

3. Transmission Phase

The transmission phase is one of the important sections for sending the data to destination securely. The encryption section generates the cover image in which the data is embedded or hidden. This image is secured using the secret key. Usually we use e-mail or web for transferring the data. If the person hacks the e-mail or web and obtains the image, the secret key helps from unauthorized modification.

4. Decryption phase

The decryption process of LSB (Least Significant Bit) steganography involves extracting the hidden message from a digital image that has been embedded with the LSB technique and encrypted using a symmetric encryption algorithm. Here is a general overview of the decryption process:

Receive the digital image: The receiver of the hidden message receives the digital image through a secure channel.

Extract the LSBs from the pixels: The receiver extracts the LSBs from the pixels in the digital image where the message was hidden. The LSBs form the binary message that was embedded in the image.

Decrypt the binary message using the secret key: The binary message that was embedded in the image was encrypted using a symmetric encryption algorithm along with a secret key. The receiver uses the same secret key to decrypt the binary message and obtain the original message.

Convert the binary message into its original format: The decrypted binary message is converted back into its original format, such as text or an image, to obtain the hidden message.

1. Extraction of Secrete Image

The decryption process of XOR cryptography for an image involves the following steps:

Obtain the encrypted binary image: The encrypted binary image is obtained, which is the result of XORing the original binary image with a secret key.

Obtain the secret key: The secret key used to encrypt the binary image must be obtained.

XOR the encrypted binary image with the secret key: Each bit of the encrypted binary image is XORed with the corresponding bit in the secret key. This produces a new binary string, which represents the original binary image.

3. Convert the binary image back into an image format: The original binary string can be converted back into an image format by reversing the process used to convert the original image into a binary format. This produces the original image.

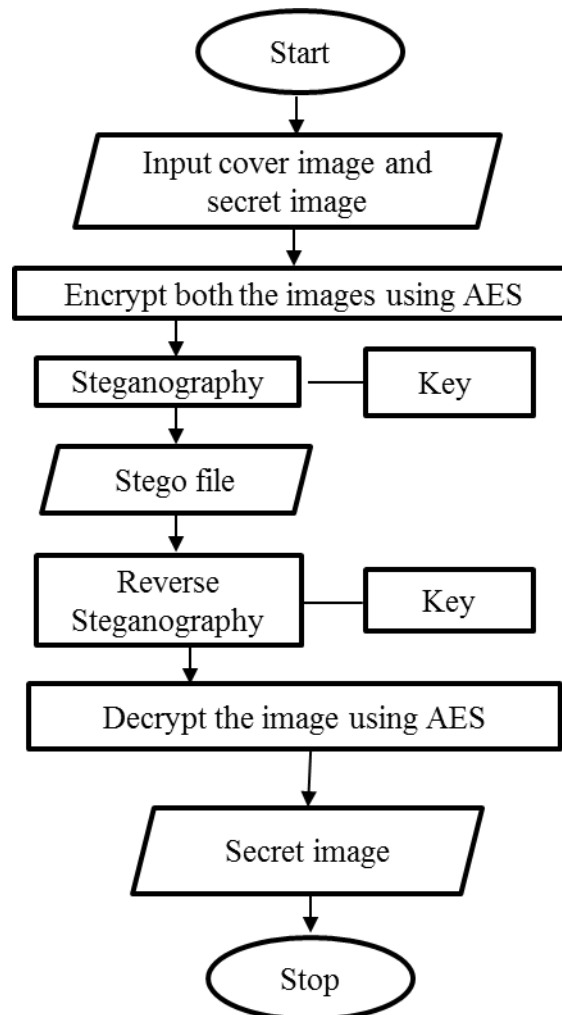


Fig 4.6: Flowchart of combined process of Cryptography & Steganography

CHAPTER 5

RESULTS AND DISCUSSIONS

5.1 : Discussions

In this integration of cryptography and steganography there are two input images one is the carrier image and other is a secret image. Encryption of both carrier and secret image is done with an advanced algorithm called Advanced encryption standard (AES). Then two images are converted to one image and that is sent to receiver which does not permit the third party to see the secret image. At receiver decryption is done and carrier and secret images are separated. The main advantage of proposed method is to enhance the security of the image to be transmitted. The major application areas of this project are military and RAW agencies.

5.2 Combined Results:

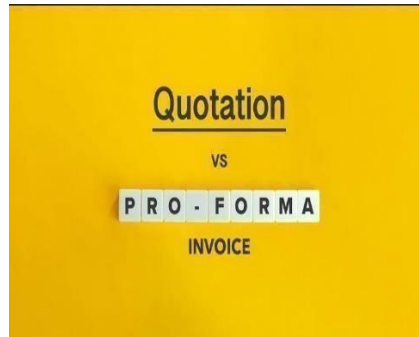


Fig 5.2.1 Main image

In the transmission side the we are going to send two input images. One image is given as a cover image or a main image as shown above and it can be any image. The image is used to hide the secret image.



Fig 5.2.2: Secret image

The second image is given as a Secret image or a Hidden image as shown above and it can be any image. The image is act as secret image and we going to hide this image.

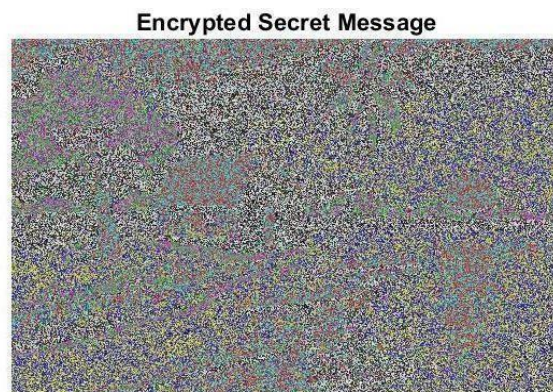


Fig 5.2.3: Encrypted Secret Message

Here the main image and the secret image is going to Encrypted into a single image that is Encrypted Secret message or Encrypted Secret image.

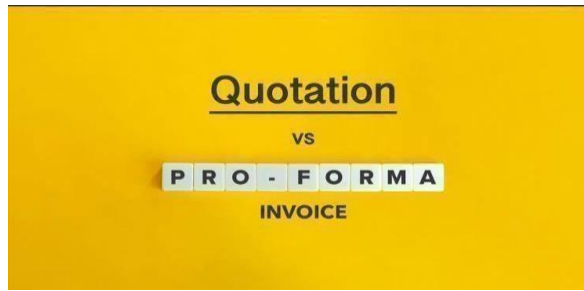


Fig 5.2.4: Stegmented image

The secret image is embedded into the main image the generated or embedded image is segmented image. The stego image is send from sender to receiver.

Recovered Encrypted Image from Steganography

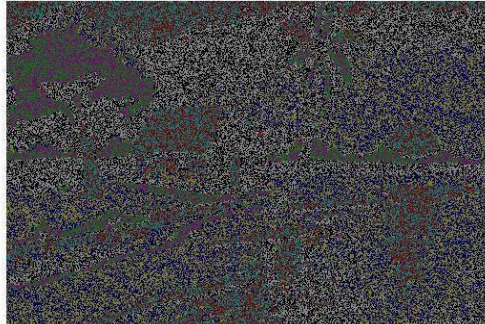


Fig 5.2.5: Recovered Encrypted image from Steganograph

In the receiver side the secret image is decrypted and get an encrypted secret image this process is done by reverse steganography.



Fig 5.2.6: Decrypted Secret Message Image

The secret image is extracted or decrypted from the recovered encrypted image and this is the final recovered image. These are some other outputs

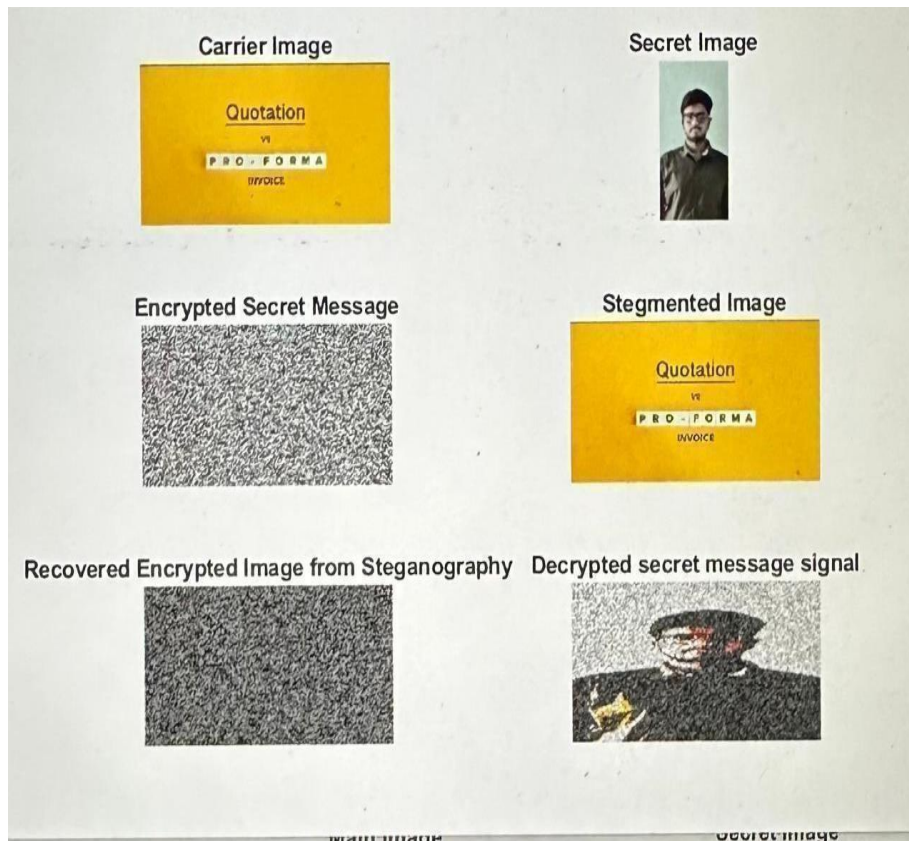
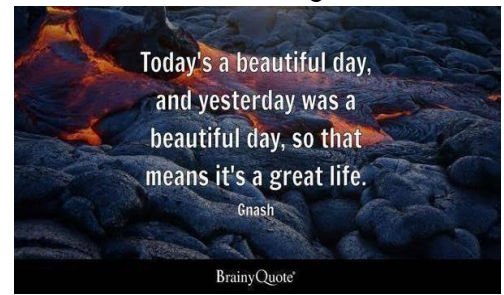


Fig 5.2.6: Sample output 2

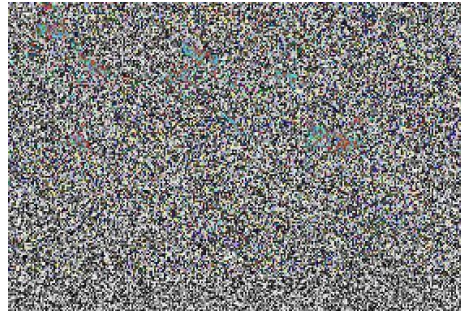
Main image



Secret Image



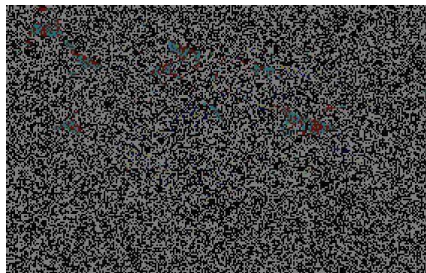
Encrypted Secret Message



Stego Image



Recovered Encrypted Image from Steganography



Decrypted secret message image

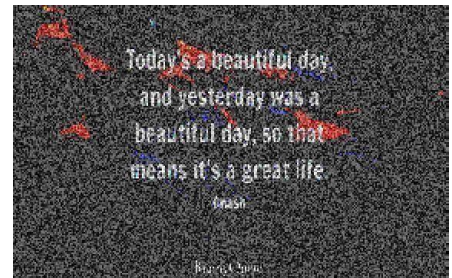


Fig 5.2.1.3: Sample output 3

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In this project we are going to conclude that with the use of integration of Cryptography & steganography can achieve security from third party. In this technique we are going to embedded an image into another image which gives high security to the hidden information. If we share the data or image through public network (Internet) no other can alter the data because it can't be seen to others. Combination of Cryptography & steganography can achieve high level of security and AES algorithm provides large key size and Block size. LSB steganography provides robustness. Which improves Quality of Communication along with security.

6.1 Future Scope

The work can further be extended to hiding a video into another video or hiding an image into a video which improves security to the data to be hidden with the change in techniques or methodology one can improve the quality of the data to be hidden. AES algorithm provides security up to some extent if use different algorithms, It may achieve better quality.

References

1. Nunna, K. C., & Marapareddy, R. (2020, March). Secure data transfer through internet using cryptography and image steganography. In 2020 SoutheastCon (Vol. 2, pp. 1-5). IEEE.
2. Hilmi, A., Mezroui, S., & El Oualkadi, A. (2018, May). Overview of Visual Cryptographic Systems Based on XOR Function. In 2018 6th International Conference on Multimedia Computing and Systems (ICMCS) (pp. 1-4). IEEE.
3. Alamsyah, M. A. M., & Prasetyo, B. (2015). Data hiding security using bit matching-based steganography and cryptography without change the stego image quality. *Journal of theoretical and applied information technology*, 106-112.
4. Agarwal, N., & Sharma, H. (2013). An Enhanced Pixel-Shuffling based Approach to Simultaneously Perform Double-DCT Image Compression, Encryption and Secondary-Steganography. *International Journal of Computer Applications*, 75(7)..
5. Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In 14th international conference on computer and information technology (ICCIT 2011) (pp. 286-291). IEEE.
6. D'souza, F. J., & Panchal, D. (2017, May). Advanced encryption standard (AES) security enhancement using hybrid approach. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 647-652). IEEE.
7. Baby, A., & Krishnan, H. (2017). Combined Strength of Steganography and Cryptography-A Literature Survey. *International Journal of Advanced Research in Computer Science*, 8(3).
8. Saini, J. K., & Verma, H. K. (2013, December). A hybrid approach for image security by combining encryption and steganography. In 2013 IEEE second international conference on image information processing (ICIIP-2013) (pp. 607- 611). IEEE.

9. Bhardwaj, R., & Khanna, D. (2015, December). Enhanced the security of image steganography through image encryption. In 2015 Annual IEEE India Conference (INDICON) (pp. 1-4). IEEE.
10. Phadte, R. S., & Dhanaraj, R. (2017, July). Enhanced blend of image steganography and cryptography. In 2017 International conference on computing methodologies and communication (ICCMC) (pp. 230-235). IEEE.
11. Stallings, W. (2017). The principles and practice of cryptography and network security 7th edition, isbn-10: 0134444280. Pearson Education, 20(1), 7.
12. Latif, I. H. (2020, February). Time evaluation of different cryptography algorithms using labview. In IOP Conference Series: Materials Science and Engineering (Vol. 745, No. 1, p. 012039). IOP Publishing
13. Nitendra Kumar Vishwakarma 2013 -Comparative Analysis of Different Techniques.
14. Latif, I. H. (2020, February). Time evaluation of different cryptography algorithms using labview. In IOP Conference Series: Materials Science and Engineering (Vol. 745, No. 1, p. 012039). IOP Publishing.
15. Buchanan, W. J. (2011). Security and forensic computing: encryption.
16. ¹Wafaa, A. A. N., & Zahary, A. A Comparative Study among Cryptographic Algorithms: Blowfish, AES and RSA.
17. Tripathi, R., & Agrawal, S. (2014). Comparative study of symmetric and asymmetric cryptography techniques. International Journal of Advance Foundation and Research in Computer (IJAFRC), 1(6), 68-76.
18. Chalurkar, S. N., Khochare, N., & Meshram, B. B. (2011). Survey on modular attack on RSA algorithm. IJCEM, 14, 106-110.
19. Rachmawanto, E. H., & Sari, C. A. (2017, October). A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size. In 2017 International Seminar on Application for Technology of Information and Communication (iSemantic) (pp. 16-21). IEEE.
20. Ardiansyah, G., Sari, C. A., & Rachmawanto, E. H. (2017, November). Hybrid method using 3-DES, DWT and LSB for secure image steganography

- algorithm. In 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE) (pp. 249-254). IEEE.
21. Ahmad, S. S. (2016, April). Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm. In 2016 4th International Conference on Cyber and IT Service Management (pp. 1-6). IEEE.
 22. Saraf, K. R., Jagtap, V. P., & Mishra, A. K. (2014). Text and image encryption decryption using advanced encryption standard. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 3(3), 118-126.
 23. Islam, M. R., Siddiqua, A., Uddin, M. P., Mandal, A. K., & Hossain, M. D. (2014, May). An efficient filtering-based approach improving LSB image steganography using status bit along with AES cryptography. In 2014 International Conference on Informatics, Electronics & Vision (ICIEV) (pp. 1-6). IEEE.
 24. Singh, A., & Singh, H. (2015, March). An improved LSB based image steganography technique for RGB images. In 2015 IEEE International Conference on electrical, computer and communication technologies (ICECCT) (pp. 1-4). IEEE.
 25. Susanto, A., Sari, C. A., & Rachmawanto, E. H. (2017, August). Hybrid method using HWT-DCT for image watermarking. In 2017 5th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.
 26. Umaroh, L., Sari, C. A., Astuti, Y. P., & Rachmawanto, E. H. (2016, August). A robust image watermarking using hybrid DCT and SLT. In 2016 International Seminar on Application for Technology of Information and Communication (ISemantic) (pp. 312-316). IEEE.
 27. Deshmukh, P. U., & Pattewar, T. M. (2014, February). A novel approach for edge adaptive steganography on LSB insertion technique. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-5). IEEE.
 28. Sivadasan, E. T. (2015, December). Secure transmission of data by splitting image.

- In 2015 International Conference on Computing and Network Communications (CoCoNet) (pp. 362-368). IEEE.
29. Mantoro, T., Permadi, D. D., & Abubakar, A. (2016, October). Stegano-image as a digital signature to improve security authentication system in mobile computing. In 2016 International Conference on Informatics and Computing (ICIC) (pp. 158- 163). IEEE.
 30. Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 3(4), 307-312.
 31. Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques. *International Journal of Advanced Science and Technology*, 54, 113-124.
 32. Sutojo, T., Rachmawanto, E. H., & Sari, C. A. (2017, August). Fast and efficient image watermarking algorithm using discrete tchebichef transform. In 2017 5th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.
 33. Jain, M., & Lenka, S. K. (2015, October). Secret data transmission using vital image steganography over transposition cipher. In *2015 international conference on green computing and internet of things (ICGCIoT)* (pp. 1026-1029). IEEE.
 34. Rachmawanto, E. H., & Sari, C. A. (2017). Secure image steganography algorithm based on dct with otp encryption. *Journal of Applied Intelligent System*, 2(1), 1-11.
 35. Sari, C. A., & Rachmawanto, E. H. (2017, September). Robust and imperceptible image watermarking by DC coefficients using singular value decomposition. In *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)* (pp. 1-5). IEEE.
 36. Akhtar, N., Johri, P., & Khan, S. (2013, September). Enhancing the security and quality of LSB based image steganography. In *2013 5th International Conference and Computational Intelligence and Communication Networks* (pp. 385-390). IEEE.

