IMAGE ENCRYPTION AND DECRYPTION USING 3DES

B. SURYANARAYANA MURTHY [1], KADALI . JYOTHSNA[2]
Assistant Professor MSC (CS),DEPT, Dantuluri Narayana Raju college, Bhimavaram, AndhraPradesh
Email id:-suryanarayanamurthy.b@gmail.com
PG Student of MSc Computer Science, Dantuluri Narayana Raju College, Bhimavaram, AndhraPradesh
Email id:-kadalijyothsna0@gmail.com

ABSTRACT

In today's world almost all digital services like internet communication, medical and military imaging systems, multimedia system needs a high-level security. There is a need for security level in order to safely store and transmit digital images containing critical information. This is because of the faster growth multimedia technology, internet and cell phones. Therefore, there is a need for image encryption techniques in order to hide images from such attacks. In this system we use Triple DES (Data Encryption Standard) in order to hide image. Such Encryption technique helps to avoid intrusion attacks.

1 INTRODUCTION

Introduction to Cryptography

The word cryptography comes from the Greek words Krypto (hidden or secret) and graphing (writing). Oddly enough, cryptography is the art of secret writing More generally people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmerging. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. In this book we will concentrate on the kind of cryptography that is based on representing information as numbers and mathematically manipulating those numbers. This kind of cryptography can provide other services, such as

- Integrity checking-reassuring the recipient of a message that the message has not been altered since it was generated by a legitimate source
- Authentication-verifying someone's (or something's) identity

But back to the traditional use of cryptography. A message in its original form is known as plaintext or clear text. The mangled information is known as cipher-text. The process for producing cipher-text from plaintext is known as encryption. The reverse of encryption is called decryption. While cryptographers invent clever secret codes, cryo-analysts attempt to break these codes. These two disciplines constantly try to keep an end of each other. Ultimately, the success of the cryptographer's rests on the plaintext, cipher-text, plaintext encrypt on end decryption.

Cryptographic system involves both an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person the person with whom you'd like to start communicating securely. With a good cryptographic scheme, it is perfectly OK to have everyone, including bad guys (and the cryptanalyst) know the algorithm because knowledge of concept of a key is analogous to the combination for a combination lock. Although the concept of a combination lock is well known (you dial in the secret numbers in the correct sequence and the lock opens), you can't open a combination lock easily without knowing the combination.

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing analyzing protocols that prevent third parties or the public from reading private messages various aspects in information security such as data confidentiality, data integrity, authentication, and non- repudiation are central to modern cryptography.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a

readable state to apparent text that does not make sense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons from doing the same.

Modern cryptography is heavily based on mathematical theory and computer science practice cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is not feasible to do so by any known practical means. These schemes are therefore termed computationally secure.

Examples include, improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exists information – theoretically secure schemes that probably cannot be broken even with unlimited computing power – an example is the one- time pad-but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms .

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

1.2 Terminology

The first use of the term cryptograph (as opposed to cryptogram) dates back to the 19th century- it originated in The Gold-Buy, a novel by Edgar Allan Pos.

Until modern times, cryptography referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible text (call cipher text) Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext.

1.2.1 Cipher

It is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and n cache instance by a "key". The key is a secret (ideally known only to the communicants), usually a short string of characters which is needed to decrypt the cipher text.

Formally, a “cryptosystem” is the ordered list of elements of finite possible plaintexts, finite possible cipher texts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important both formally and in actual practice, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless(or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as symmetric and asymmetric. In Symmetric systems the same key(the secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric system is faster than asymmetric as they generally use shorter key lengths. Asymmetric systems use a public key to encrypts a message a private key to decrypt it. Use of asymmetric systems include RSA (Rivest-Shamir-Adleman), and ECC (Elliptical Curve Cryptography), Symmetric models include the commonly used AES (Advanced Encryption Standard) which replaced the older DES (Data Encryption Standard).

In colloquial use, the term "code" is often used to mean any method of encryption or concealment of meaning. However, in cryptography, code has a more specific meaning. It means the replacement of a unit of plaintext with a code word (for example, "wallaby" replaces attack at dawn")

Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to crack encryption algorithms or their implementations.

Some use the terms cryptography and cryptology interchangeably in English, while others (including US military practice generally) use cryptography to refer specifically to the use and practice of cryptographic techniques and cryptology to refer to the combined study of cryptography and cryptanalysis English is more flexible than several other languages in which

cryptology (done by cryptologists) is always used in the second sense above. RFC 2828 advises that steganography is sometimes included in cryptology.

The study of characteristics of languages that have some application in cryptography or cryptology (e.g., frequency data, better combinations, etc.) is called crypto linguistics.

1.3 History of Cryptography

Before the modern era, cryptography focused on message confidentiality (i.e., encryption)-conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors without secret knowledge (namely the key needed for decryption of that message). Encryption attempted to ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

1.4 Computer Era

Cryptanalysis of the new mechanical devices proved to be both difficult and laborious. In the United Kingdom, cryptanalytic efforts at Bletchley Park during WWII spurred the development of more efficient means for carrying out repetitious tasks. This culminated in the development of the Colossus, the world's first fully electronic, digital, programmable computer, which assisted in the decryption of ciphers generated by the German Army's Lorenz SZ40/42 machine.

Just as the development of digital computers and electronics helped in cryptanalysis, it made possible much more complex ciphers. Furthermore, computers allowed for the encryption any kind of data representable in any binary format, unlike classical ciphers which only encrypted written language texts : this was new and significant. Computer use has thus supplanted linguistic cryptography, both for cipher design and cryptanalysis. Many computer ciphers can be characterized by their operation on binary bit sequences (sometime in groups or blocks) , unlike classical and mechanical schemes, which generally manipulate traditional characters(i.e., letters and digits) directly. However, computers have also assisted cryptanalysis, which has compensated to some extent for increased cipher complexity Nonetheless, good modern ciphers have stayed ahead of cryptanalysis ; it is typically the case that use of a quality cipher is very efficient (i.e., fast and requiring few resources, such as memory or CPU capability). While breaking it requires an effort many orders of magnitude larger, and vastly larger than that required for any classical cipher, making cryptanalysis so inefficient and impractical as to be effectively impossible.

Extensive open academic research into cryptography is relatively recent; it began only in the mid-1970s. In recent times, IBM personnel designed the algorithm that became the Federal (i.e., US) Data Encryption Standard: Whitield Diffie and Martin Hellman published their key agreement algorithm, and the RSA algorithm was published in Martin Gardner's Scientific American column. Since then, cryptography has become a widely used tool in communications computer networks, and computer security generally. Sone modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep connections with abstract mathematics. There are very few cryptosystems that are proven to be unconditionally secure. The one- time pad is one. There are a few important ones that are proven secure under certain unproven assumptions. For example, the infeasibility of factoring extremely large integers is the basis for believing that RSA is secure, and some other systems, but even there, the proof is usually lost due to practical considerations. There are systems similar to RSA, such as one by Michael O. Rabin that is provably secure provided factoring is impossible, but the more practical system RSA has never been proved secure in this sense. The discrete logarithm problem is the basis for believing some other cryptosystems are secure, and again there are related, less practical systems that are provably secure relative to the discrete log problem.

As well as being aware of cryptographic history, cryptographic algorithm and system design must also sensibly consider probable future developments while working on their designs. For instance, continuous improvements in computer processing power have increased the scope of brute-force attacks, so when specifying key lengths, the required key lengths are similarly advancing.] The potential effects of quantum computing are already being considered by some cryptographic system designers developing post-quantum cryptography: the announced imminence of small implementations of these machines may be making the need for this preemptive caution rather more than merely speculative.

Essentially, prior to the early 20th century, cryptography was chiefly concerned with linguistic and lexicographic patterns. Since then, the emphasis has shifted, and cryptography now makes extensive use of mathematics, including aspects of information theory, computational complexity, statistics, combinatorics, abstract algebra, number theory, and finite mathematics generally. Cryptography is also a branch of engineering, but an unusual one since it deals with active, intelligent, and malevolent opposition (see cryptographic engineering and security engineering); other kinds of engineering (e.g., civil or chemical engineering) need deal only with neutral natural forces. There is also active research examining the relationship between cryptographic problems and quantum physics (see quantum cryptography and quantum computer).

1.5 Modern Cryptography

Encryption in modern times is achieved by using algorithms that have a key to encrypt and decrypt information. These keys convert the messages and data into "digital gibberish" through encryption and then return them to the original form through decryption. In general, the longer the key is, the more difficult it is to crack the code. This holds true because deciphering encrypted message by brute force would require the attacker to try every possible this in context, each binary unit of information, or bit, has a value of 0 or 1. An 8-bit key would then have 256 or 28 possible keys. A 56-bit key would have 256, or 72 quadrillion, possible keys to try and decipher the message. With modern technology, cyphers using keys with these lengths are becoming easier to decipher DES, a Carly US Government approved cypher, has an effective key length of 56 bits, and test messages using that cypher have been broken by brute force key search. However, as technology advances, so does the quality of encryption. Since World War II, one of the most notable advances in the study of cryptography is the introduction of the asymmetric key cyphers (sometimes termed public-key cyphers). These are algorithms which use two mathematically related keys for encryption of the same message. Some of these algorithms permit publication of one of the keys, due to it being extremely difficult to determine one key simply from knowledge of the other.

2. LITERATURE SURVEY AND RELATED WORK

A literature survey on image encryption and decryption using Triple Data Encryption Standard (3DES) is a comprehensive review of research articles, papers, and studies that focus on the application of 3DES for securing digital images.

1. “Security enhancement: Combining cryptography and steganography” by D. Seth, L. Ramanathan, and A. Pandey, International Journal of Computer Applications (0975–8887) Volume, 2010. This paper focus on the strength of combining cryptography with steganography and various works in the area of combination of these 2 techniques. In today’s world of high technology, it is not safe to share confidential and important data on any network. Intruders are always in wake of it. They hack the data and use it for their benefit. These malicious people try to gain benefit, get attention, or to harm someone. In either case, message sender or receiver has to pay the price. To avoid these undesirable acts, Steganography and cryptography are used together to ensure security of the covert and secure message. One of the most efficient and secure algorithms is Data Encryption Standard (DES). Steganography is the art and science of writing hidden messages in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden message.
2. “Combining cryptography and steganography for data hiding in images,” by H. Abdul Zahra, R. AHMAD, and N. M. NOOR, ACACOS, Applied Computational Science, pp. 978–960, 2014. The primary purpose of this paper is to improve a new method of hiding secret messages in the image, possibly by combining steganography and cryptography. Cryptography and Steganography are the two popular methods for secure data hiding and transmission available broadly. The techniques used information in order to cipher or cover their existence respectively. Cryptography is the science of using mathematics to encrypt and decrypt data; the data are converted into some other gibberish form, and then the encrypted data are transmitted. While Steganography is the art and science of hiding communication, a stenographic system, thus embeds hidden content in the unremarkable cover media so as not to provoke an eavesdropper’s suspicion. In steganography the secret message embeds in a harmless looking cover such as a digital image file, then the image file is transmitted. The primary purpose of this paper is to improve a new method of hiding secret messages in the image, possibly by combining steganography and cryptography.

3. "Data Hiding in Image Using least significant bit with cryptography" by Mr. Vikas Tyagi(2012), International Journal of Advanced Research in computer science and Software Engineering, Volume 2, Issue 4. In this paper, we propose three efficient Steganography techniques that are used for hiding secret messages. Steganography is the art of hiding data in a seemingly innocuous cover medium. For example – any sensitive data can be hidden inside a digital image. Steganography provides better security than cryptography because cryptography hides the contents of the message but not the existence of the message. So, no one apart from the authorized sender and receiver will be aware of the existence of the secret data. Steganographic messages are often first encrypted by some traditional means and then a cover image is modified in some way to contain the encrypted message. The detection of steganographically encoded packages is called steganalysis. In this paper, we propose three efficient Steganography techniques that are used for hiding secret messages. They are LSB based Steganography, Steganography using the last two significant bits and Steganography using diagonal pixels of the image. Symmetric and asymmetric key cryptography has been used to encrypt the message.

4."An Improved Secure Image Encryption Algorithm Using 3DES" by S. Kumaravel & K. Muneeswaran International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2013. This paper introduces an enhanced image encryption algorithm using 3DES for securing images. The authors discuss the algorithm's resistance to common attacks and its practicality. We all know that in this growing world digital services usage has become more, the digital services are like communication over the internet, medical field, military imaging systems these need will need a high level of security. To correctly store and transmit digital photographs containing sensitive information, a security level is required. This is due to the rapid advancement of multimedia technologies, the internet, and cell phones. As an outcome, image encryption resolutions are compulsory to safeguard photos from such attacks. In this system, we employ Triple DES to hide photographs (Data Encryption Standard). This sort of encryption helps to keep both active and passive threats at bay.**EXISTING SYSTEM**

Easily identifies trends and patterns: Machine Learning Models can review large volumes of data and discover specific trends and patterns that would not be apparent to humans. For instance, for an e-commerce website like Amazon, it serves to understand the browsing behaviours and purchase histories of its users to help cater to the right products, deals, and reminders relevant to them. It uses the results to reveal relevant advertisements to them.

No human intervention needed (automation): With implementation of ML model, there is no need to have any eye on the project at every step of the way. Since, giving machines the ability to learn, lets them make predictions and also improve the algorithms on their own. A common example of this is anti-virus softwares; they learn to filter new threats as they are recognized. ML is also good at recognizing spam.

Continuous Improvement: As ML algorithms gain experience, they keep improving in accuracy and efficiency. This lets them make better decisions.

3 EXISTING WORK

The Data Encryption Standard (DES) is a symmetric-key block cipher algorithm that was widely used for securing data in the past. However, it's considered outdated and no longer recommended for secure cryptographic applications due to its relatively short key length (56 bits), which makes it vulnerable to brute force attacks with modern computing power. It has been replaced by more secure encryption algorithms like 3DES (Triple Data Encryption Standard) .

4 PROPOSED WORK AND ALGORITHM

Triple Data Encryption Standard (3DES) was still used encryption algorithm in various applications, including image encryption and decryption. A system for image encryption and decryption using 3DES involves generating a secure 3DES encryption key, applying 3DES encryption to input images, and securely distributing keys. It ensures data security and aims to preserve image quality.

Designing a proposed system for image encryption and decryption using Triple Data Encryption Standard (3DES) involves creating a framework for secure image communication. Here's a general outline of how you can propose such a system:

Image Encryption:

• User selects an image for encryption.

- The system generates a random encryption key (3DES key).
- The selected image is encrypted using 3DES with the generated key.
- The encrypted image is prepared for transmission along with key information.

Data Transmission:

- The encrypted image and key information are securely transmitted to the recipient.

Image Decryption:

- The recipient receives the encrypted image and key information.
- The recipient uses the provided key to decrypt the image using the 3DES decryption algorithm.
- The decrypted image is displayed or saved.

.

5 METHODOLOGIES

MODULES

1.Encryption

Using this module, the sender can upload an image that needs to be encrypted in order to securely send the image over internet. In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.

2.Decryption

In the Decryption module , the receiver decrypts the encrypted image using the secret key that was sent along with the encrypted image. The decrypted image was stored on the receiver system. Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system.

6 RESULTS AND DISCUSSION

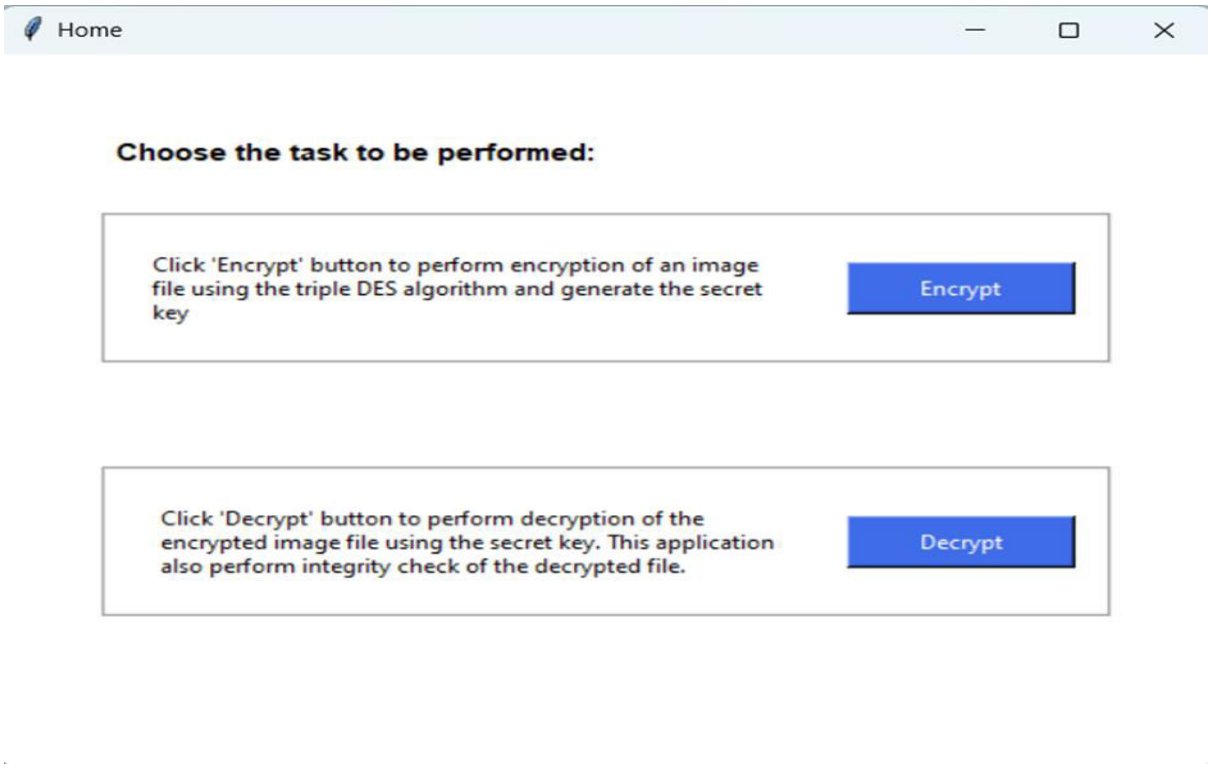

Fig 1:- Homescreen

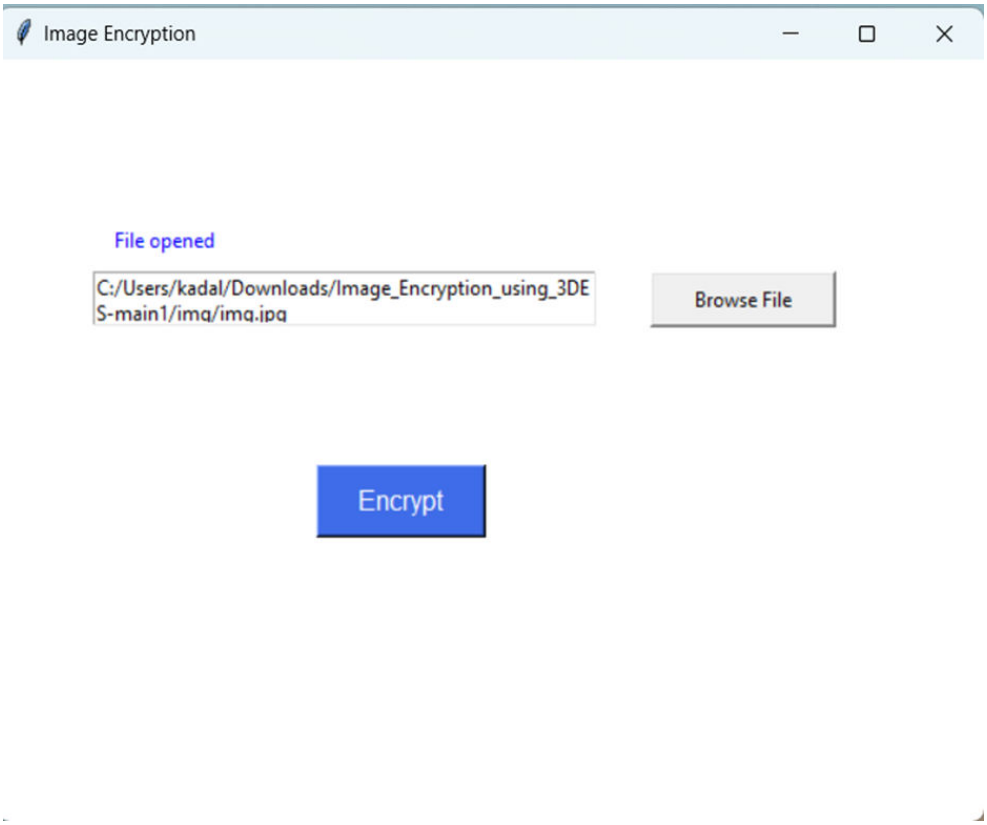

Fig 2:- Image Encryption

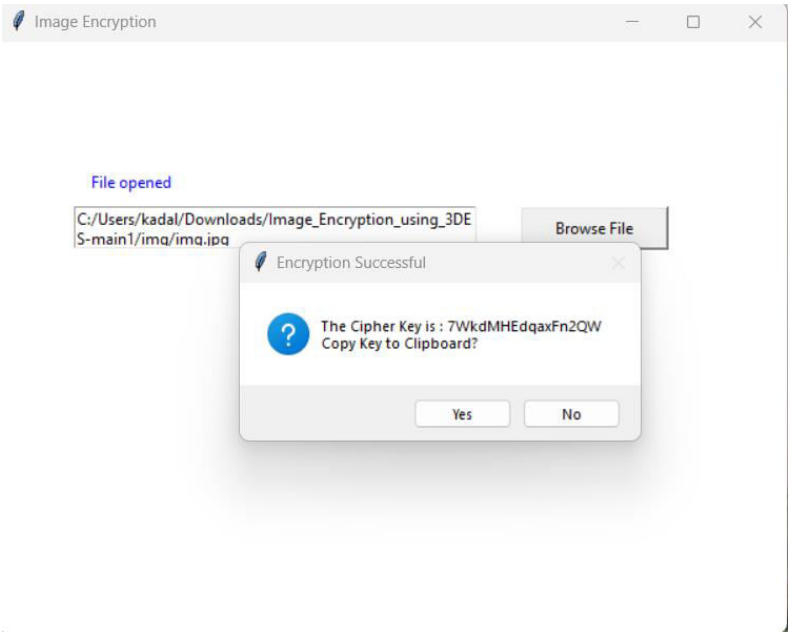

Fig 3: Encrypted File

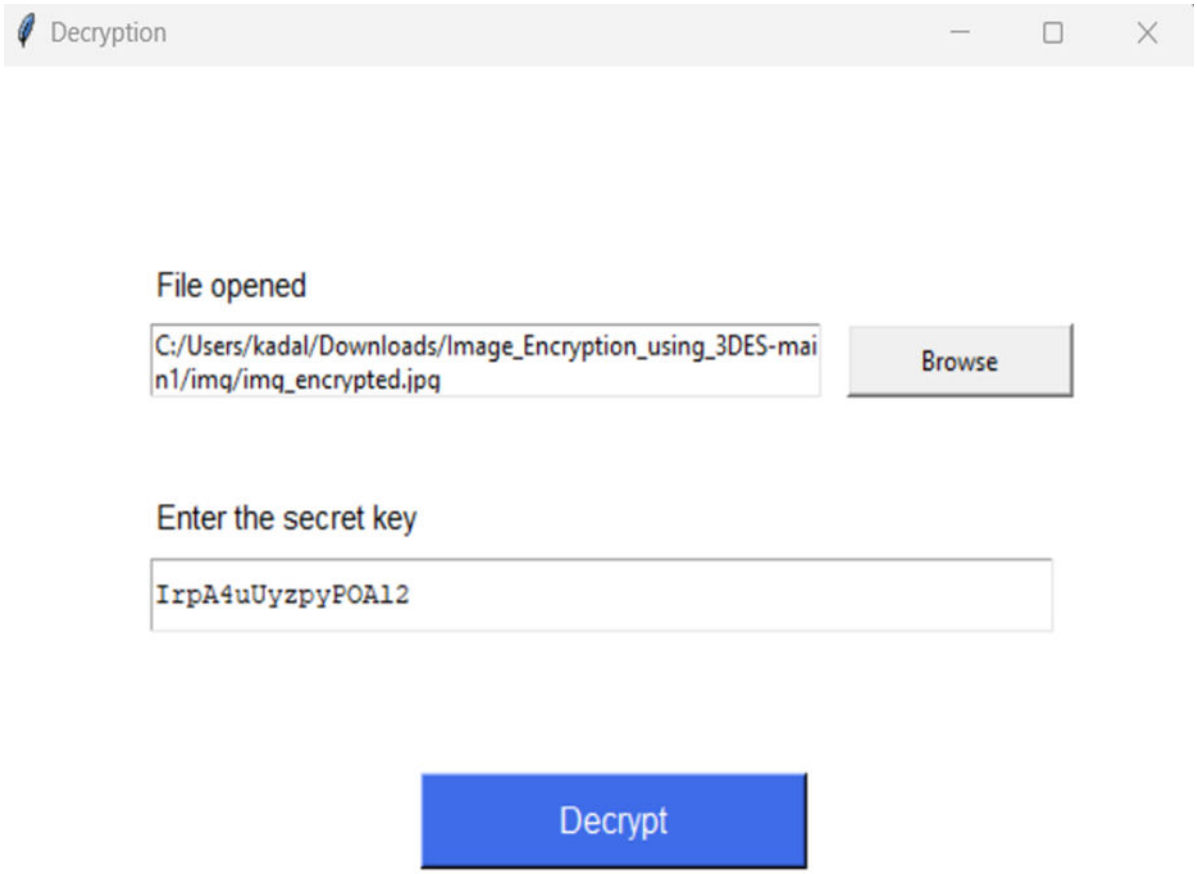

Fig 4 : Decrypted File

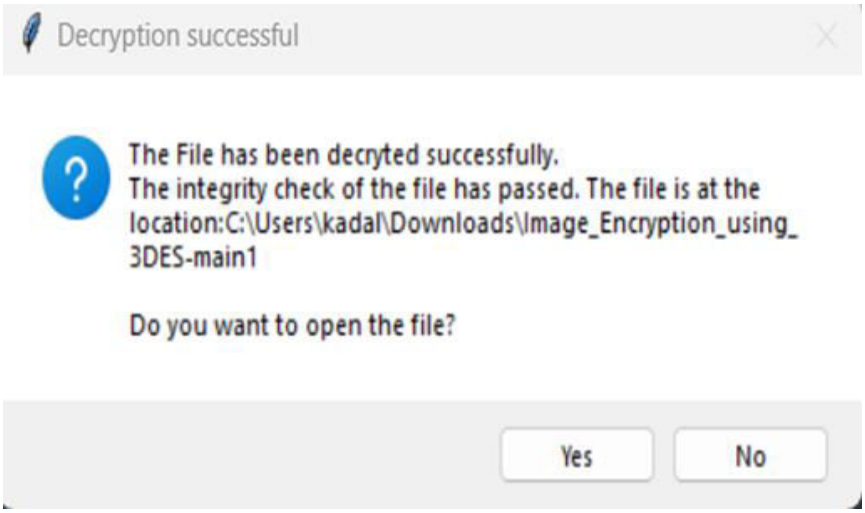

Fig 5: File open

6.CONCLUSION AND FUTURE SCOPE

In this project, we deal with the concepts of security of digital data communication across the network. This project is designed for combining the steganography and cryptography features factors for better performance. We performed a new steganography method and combined it with RSA algorithm. The data is hidden in the image so there will be no chances for the attacker to know that data is being hidden in the image. We performed our method on image by implementing a program written in Python language. The method proposed has proved successful in hiding various types of text, images, audio and videos in color images. We concluded that in our method the Image files and RSA are better. Because of their high capacity.

This work presents a scheme that can transmit large quantities of secret information and provides secure communication between two private parties. Both steganography and cryptography can be woven in this scheme to make the detection more complicated. Any kind of text data can be employed as secret msg. The secret message employing the concept of steganography is sent over the network. In addition, the proposed procedure is simple and easy to implement.

The Embedding of data is done such as Audio, Video, Image is done in the image, by choosing a distinct and new image, we can prevent the chance for the attacker to detect the data being hidden. Results achieved indicate that our proposed method is encouraging in terms of security, and robustness.

6.2 FUTURE SCOPE

The future scope of image encryption and decryption using the Triple Data Encryption Standard (3DES) algorithm depends on various factors, including advancements in technology, security requirements, and emerging trends in the field of encryption and image processing. Here are some potential future directions for image encryption and decryption using 3DES:

1. **Integration with Blockchain:**

Combining image encryption with blockchain technology can provide enhanced security and provenance for digital assets, such as artwork, medical images, or sensitive documents. This integration can ensure the integrity and authenticity of encrypted images.

2. **Machine Learning Integration:**

Incorporating machine learning techniques for improved image analysis and encryption key management could be a future direction. This might involve using AI to automatically classify and encrypt images based on content or context.

3. **Cloud-Based Encryption Services:**

Cloud computing is becoming increasingly prevalent. The future may involve the development of cloud-based image encryption and decryption services that offer scalability and accessibility while maintaining strong security measures.

4. **Advanced Encryption Standards:**

While 3DES is still used in some legacy systems, modern encryption standards like AES (Advanced Encryption Standard) are more widely adopted due to their superior security and efficiency. The future may see a gradual transition from 3DES to more advanced encryption standards for image encryption.

5. **Secure Multimedia Communication:**

With the increasing demand for secure multimedia communication, image encryption will play a vital role in protecting sensitive visual data in applications such as video conferencing, telemedicine, and secure messaging.

6. **Cross-Platform Compatibility:**

Ensuring that encrypted images can be securely exchanged and decrypted across different platforms and devices will continue to be important. Future developments may focus on improving cross-platform compatibility and standardization.

7 REFERENCES

1.D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," International Journal of Computer Applications (0975–8887) Volume, 2010.

2.H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Combining cryptography and steganography for data hiding in images," ACACOS, Applied Computational Science, pp. 978–960, 2014.

3.J. V. Karthik and B. V. Reddy, "Authentication of secret information in image stenography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.

4.M. H. Rajyaguru, "Crystography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.

5.M. K. I. Rahmani and N. P. Kamiya Arora, "A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.

6.Mr. Vikas Tyagi(2012), "Data Hiding in Image Using least significant bit with cryptography", International Journal of Advanced Research in computer science and Software Engineering, Volume 2, Issue 4.

7.P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography," 2013.

8.R. Poornimal and J. Iswarya (2013) "An Overview of Digital Image Steganography", International Journal of Computer Science & Engineering Survey Vol.4,NO.1,February.

9.R Praveen Kumar, V Hemanth, MShareef, Securing Information Using Steganography, 2013 International Conference on Circuits, Power and Computing Technologies.