IMAGE ENCRYPTION AND DECRYPTION USING 3DE ENCRYPTION

TEEPARTHI SAI DURGA PRAVEENA, K. SUPARNA

1.PG STUDENT, D.N.R. COLLEGE, P.G. COURSES (AUTONOMOUS), BHIMAVARAM-534202.

E Mail Id:praveepatnaik@gmail.com

1. Assistant Professor in DEPARTMENT OF MASTER OF COMPUTER SCIENCE, BHIMAVARAM-534202.

E Mail Id:suparnakalidindi@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

Real-time left eye tracking is an advanced technology that allows for the precise monitoring and analysis of a person's left eye movements and gaze direction in real-time. This technology leverages various techniques, such as computer vision and eye-tracking hardware, to continuously capture and interpret the movement of the left eye. By tracking the left eye in real-time, it provides valuable insights into a person's visual attention, focus, and cognitive processes. This has numerous applications in fields like human-computer interaction, virtual reality, psychology, marketing research, and medical diagnostics, enabling a deeper understanding of how individuals interact with their surroundings and devices. In this discussion, we will explore the principles, applications, and implications of real-time left eye tracking technology

2. LITERATURE SURVEY AND RELATED WORK

1.1 Introduction to Cryptography:

The word cryptography comes from the Greek words Krypto (hidden or secret) and graphene (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 someane'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, cryptanalysts attempt to break these codes. These two disciplines constantly try to keep ahead of each other. Ultimately, the success of the cryptographer's rests on the plaintext, cipher-text, plaintext encrypt on end

decryption.

Cryptographic systems tend to involve 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 scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you'd like to start communicating securely. With a good cryptographic scheme, it is perfectly OK to have everyone, including the bad guys (and the cryptanalysts) know the algorithm because knowledge of the algorithm without the key does not help unmingle the information. The 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.

scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you'd like to start communicating securely. With a good cryptographic scheme, it is perfectly OK to have everyone, including the bad guys (and the cryptanalysts) know the algorithm because knowledge of the algorithm without the key does not help unmangle the information. The 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 analysing 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 exist 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 best.

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.

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 cypher 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 authentication or integrity checks. There are two kinds of cryptosystems: symmetric and asymmetric. In symmetric systems the sarne key (the secret key) is used to encrypt and decrypt a message. Data manipulation in symmetric systems is faster than asymmetric as they generally use shorter key lengths. Asymmetric systems use a public key to encrypt a message a private key to decrypt it. Use of asymmeric systems enhances the security of communication. Examples of asymmetric systems include RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography). Symmetric models include the commonly used AES (Advanced Encryption Standard) which replaced the older.

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 (eg. frequency data, better combinations, universal patterns, 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 (sometimes 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: Whitfield 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 n pq 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 pre emotive caution rather more than merely speculative.

Essentially, prior to the early 20th century, cryptography was chiefly concerned with linguistic and lexicographic patterns. Since 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

3. EXISTING SYSTEM

The existing system for image encryption and decryption may involve conventional methods like basic symmetric or asymmetric encryption algorithms. However, these methods may not provide the required level of security for sensitive image data. In the context of image encryption, the existing system might have the following limitations:

Limited Security: Existing systems may use simple encryption techniques that are not highly secure, making it easier for attackers todecrypt and access sensitive image data.

Lack of Efficiency: Older encryption methods may not be optimized for image data, leading to slower encryption and decryption processes, which can be problematic when handling large image files.

Scalability Issues: Scalability can be a challenge in the existing system when it comes to handling a large number of images and ensuring that each one is properly encrypted and decrypted.

4. PROPOSED SYSTEM

The proposed system aims to enhance the security and efficiency of image encryption and decryption using the Triple Data Encryption Standard (3DES) encryption algorithm. Here are the key features and improvements in the proposed system:

3DES Encryption: The proposed system will implement the 3DES encryption algorithm, which is a widely recognized and highly **secure symmetric encryption method. 3DES applies the Data Encryption Standard (DES) algorithm three times to each data block,** making it significantly more secure than the original DES.

Image Segmentation: To improve efficiency, the proposed system may incorporate image segmentation techniques to divide large images into smaller blocks. Each block can then be individually encrypted and decrypted, allowing for faster processing.

Key Management: The system will include robust key management mechanisms to securely generate, store, and distribute encryption keys. Proper key management is crucial for maintaining the security of the encrypted images.

Authentication: To ensure that only authorized users can decrypt the images, the proposed system may incorporate authentication mechanisms, such as password-based or token-based authentication.

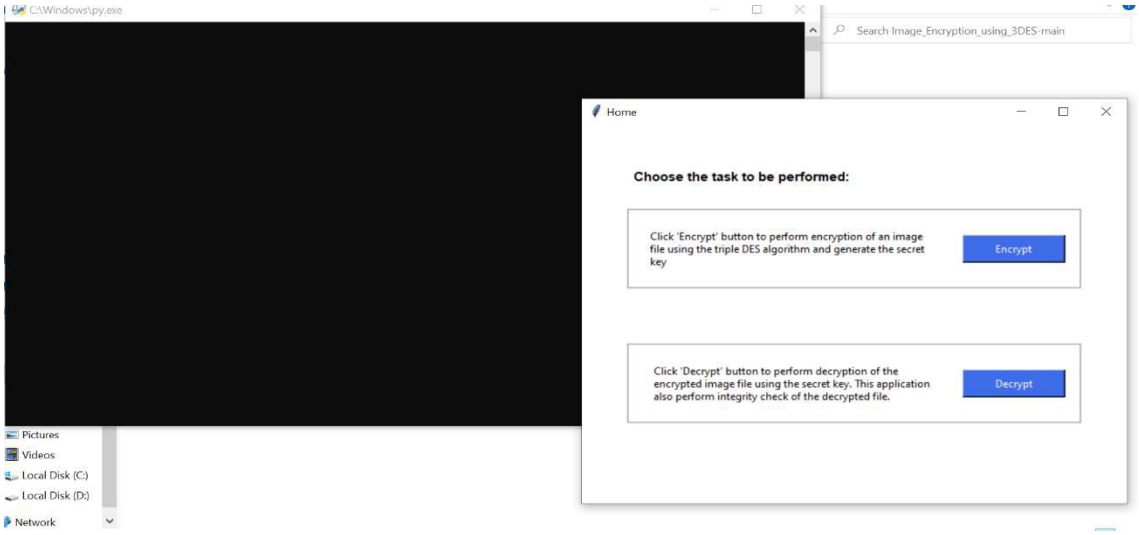
User-Friendly Interface: The proposed system will have a user-friendly interface that allows users to easily select images for encryption and decryption. It may also provide options for batch processing and encryption of various image formats.

Error Handling: Robust error-handling mechanisms will be implemented to deal with potential issues during encryption and decryption, such as corrupted images or incorrect keys.

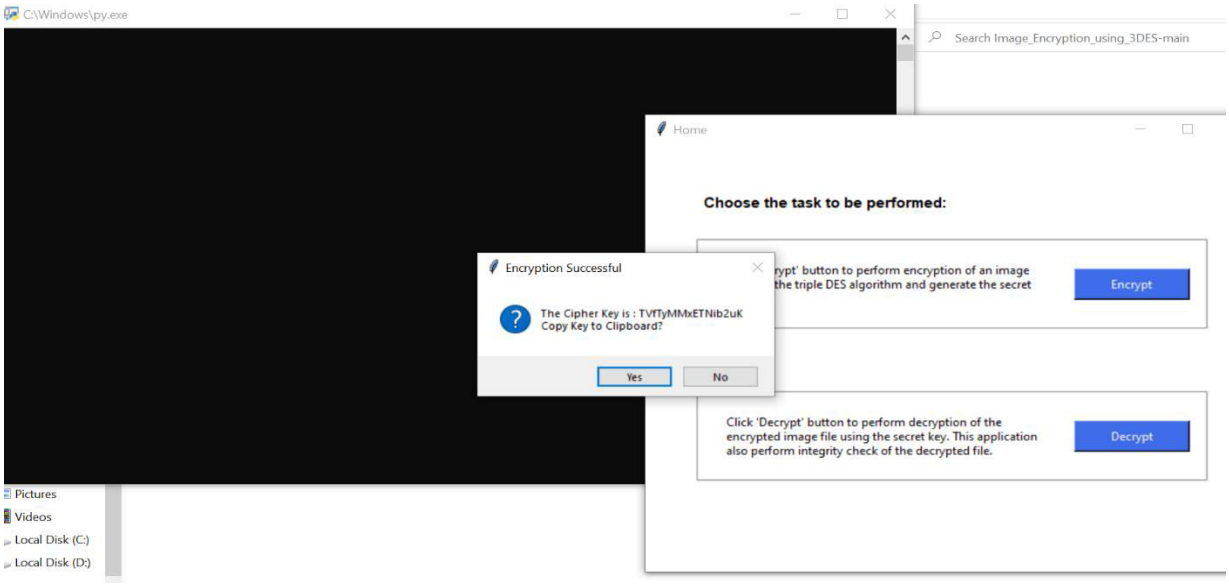
Scalability: The system will be designed to handle a large number of images efficiently. It should be capable of processing images in a scalable and parallel manner, making it suitable for both small and large-scale applications.

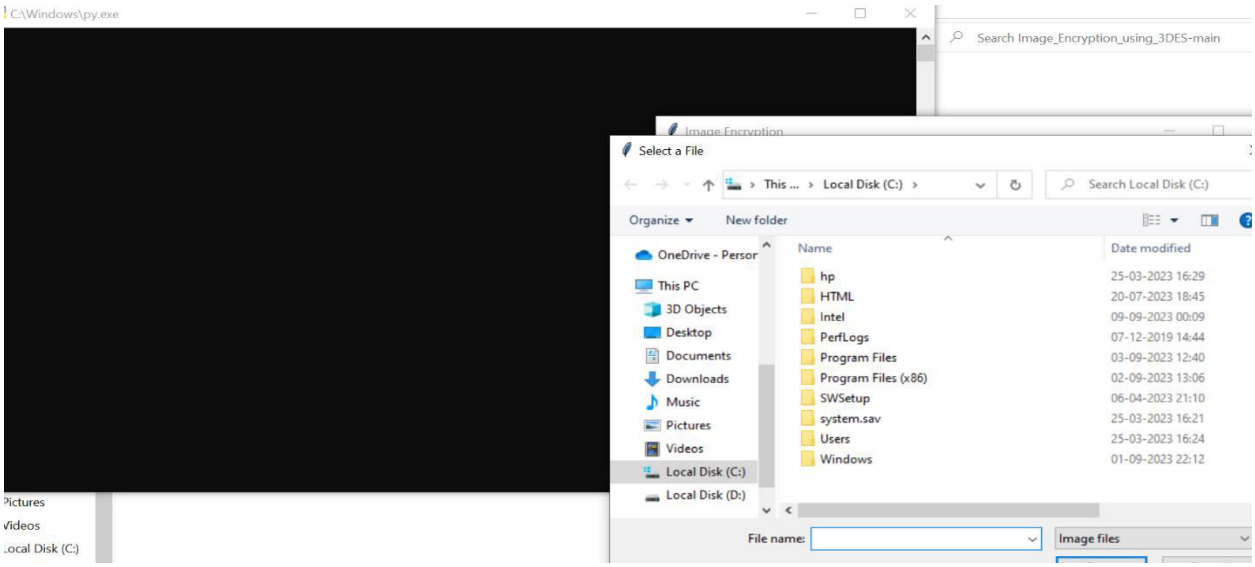
5. RESULTS AND DISCUSSION SCREEN SHOTS

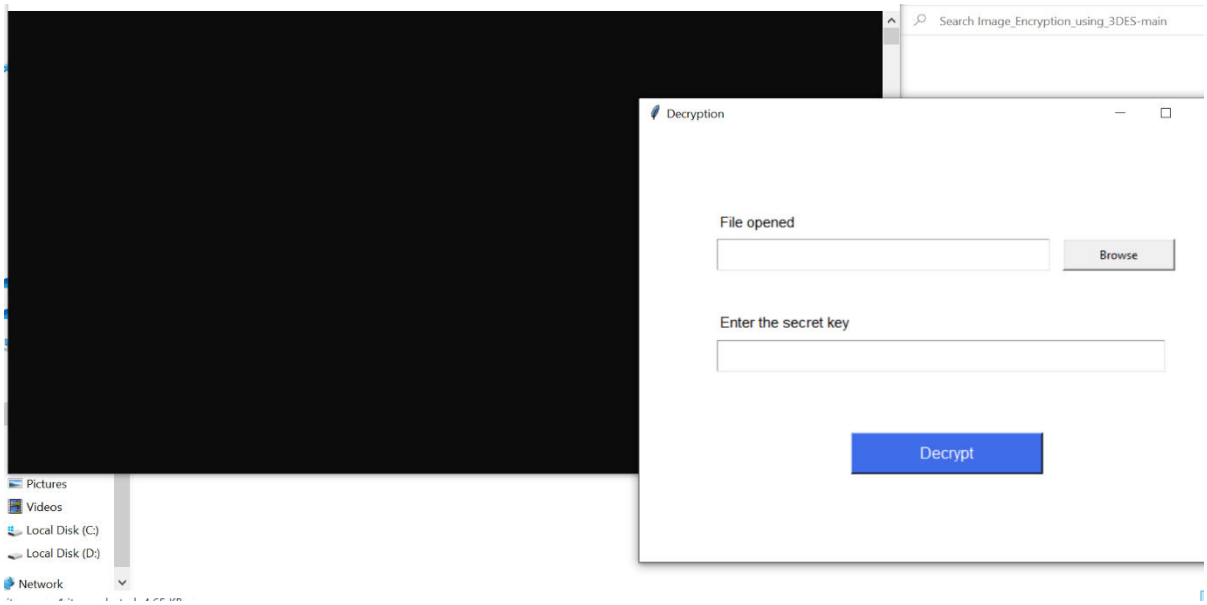
SCREEN SHOTS



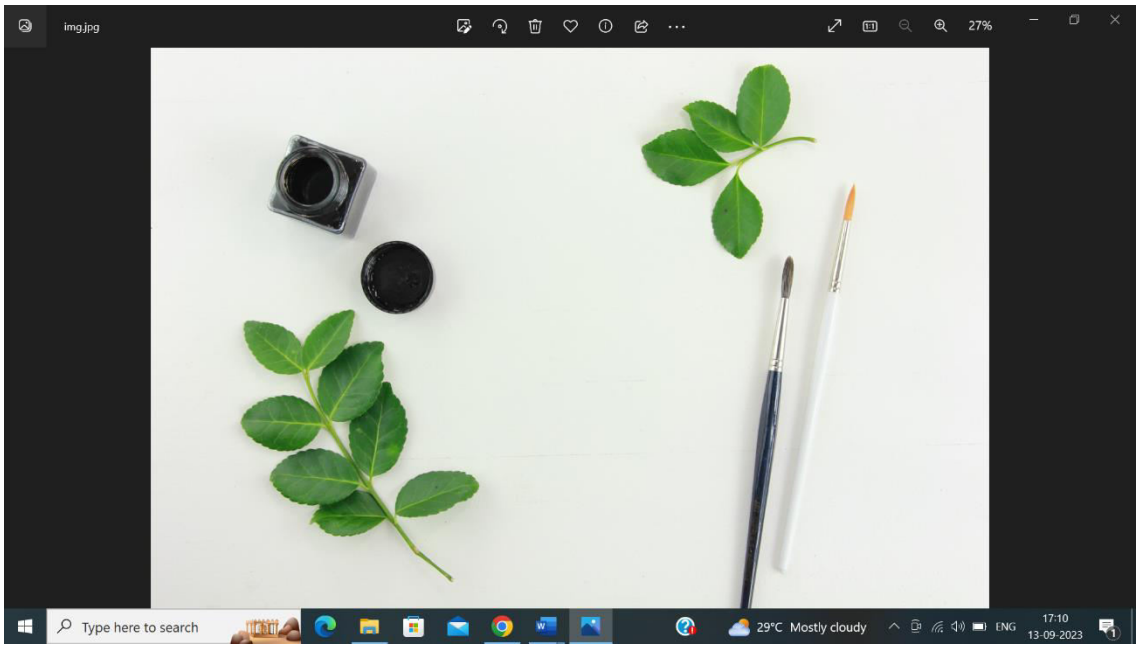
ENCRYPT IMAGE







ENCRYPT AND DECRYPT IMAGE:



6. CONCLUSION AND SCOPE

CONCLUSION

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.

7.REFERENCE

[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. Abdul- Zahra, 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, "Cryptography-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.