Abstract

Security information has become the major concern for the fast growth of the digital exchange of data storage and transmission. As there is rapid growth of using images in many fields, so it is important to protect the private image data from the intruders. Image protection has become an imperative issue. To protect an individual privacy has become a crucial task With the exponential growth of digital data, the security of sensitive information has become paramount. Image encryption and decryption are essential techniques to ensure the confidentiality of images transmitted over insecure channels. This project focuses on implementing image encryption and decryption algorithms using Python programming language. The encryption algorithm employs advanced cryptographic techniques to scramble the image data, making it unreadable without the correct decryption key. The decryption process reverses the encryption to reconstruct the original image. This report provides an in-depth analysis of the implementation, including the methodology, algorithm design, code structure, and experimental results.

IndexTerms **- Security, Image protection, Encryption, AES.**

Chapter 1

INTRODUCTION

In the digital era, data security is of paramount importance. With the exponential growth in data generation and transmission, ensuring the confidentiality and integrity of sensitive information, particularly in image communication, has become a significant concern. Image encryption and decryption techniques play a crucial role in safeguarding digital images from unauthorized access and tampering. This project focuses on developing a robust image encryption and decryption system using Python, a versatile programming language renowned for its simplicity and efficiency.

The proliferation of digital images across various domains, including medical imaging, surveillance, and multimedia communication, underscores the need for secure transmission and storage mechanisms. Traditional encryption methods designed for text-based data often fail to adequately address the unique characteristics and vulnerabilities of digital images. As such, there is a growing demand for specialized encryption techniques tailored to the intricacies of image data. This project bridges the gap by proposing a novel approach to image encryption and decryption leveraging Python's extensive libraries and cryptographic functionalities.

The primary objective of this project is to design and implement an image encryption and decryption system that ensures the confidentiality and integrity of digital images. Specifically, the project aims to achieve the following goals:

Develop robust encryption algorithms capable of securely transforming image data into an unreadable format.Implement decryption algorithms to reverse the encryption process and recover the original image without loss of information.Integrate user-friendly interfaces to facilitate seamless interaction with the encryption and decryption functionalities.Evaluate the performance and security of the proposed system through rigorous testing and analysis.

The scope of this project encompasses the entire lifecycle of image encryption and decryption, from algorithm design to implementation and testing. The system will support various image formats, including JPEG, PNG, and BMP, to ensure compatibility with diverse applications and platforms. Additionally, the project will explore different encryption techniques, such as symmetric and asymmetric encryption, to identify the most suitable approach for securing digital images. While the focus is primarily on image encryption and decryption, the project

may also address related topics, such as key management and cryptographic protocols, based on the requirements and constraints encountered during development.

The significance of this project lies in its potential to enhance data security in image-centric applications across multiple domains. By providing a reliable means of encrypting and decrypting digital images, the proposed system can mitigate the risks associated with unauthorized access, data breaches, and tampering. Moreover, the utilization of Python as the primary programming language ensures accessibility and scalability, enabling broader adoption and customization to meet specific user requirements. Ultimately, the outcomes of this project have implications for cybersecurity, privacy protection, and the integrity of digital assets in an increasingly interconnected world.

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, sendet/receiver identity authentication, digital signatures, interactive proofs and sccure 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 gererated 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 writen 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 sehemes, which generally manipulate traditional characters (i.c., 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 academie 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 Encrypticn 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 procf 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 furure 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 emptive caution rather more than merely speculative.

Essentially, pricr to the early 20th century, cryptography was chiefly concerned with linguistic and lexicographic patterns. Since then the emphasis has shifted, and eryptography 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 brarch 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 anddecrypt 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, an 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 eyphers (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

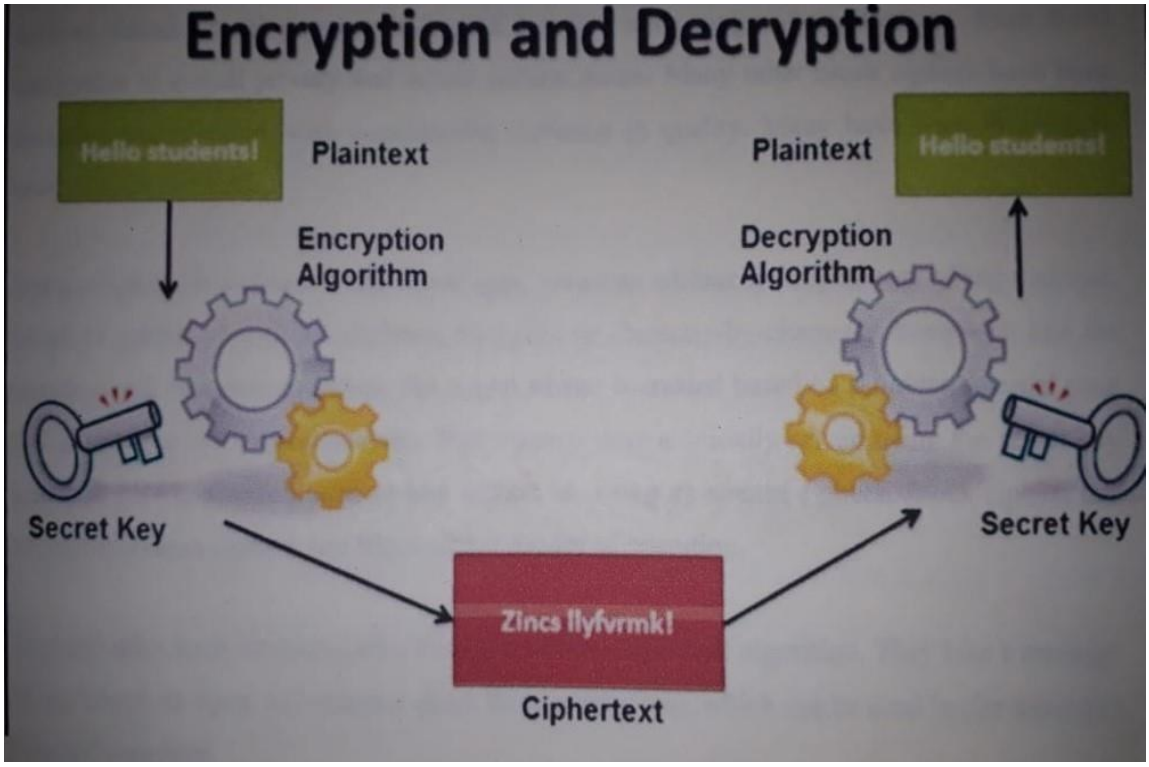

Fig. 1.1. Encryption and Decryption

1.5.1 Symmetric-Key Cryptography (Private Key Cryptography)

Symmetric-key cryptography refers to eneryption methods in which both the sender and receiver share the same key (or, less commorly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.Symmetric key ciphers are implemented as either block c phers or stream ciphers. A block cipher enciphers input in blecks of plainext as opposed tc indivicual characters, the input form used by a stream cipher.

The Data Encryption Standerd (DES) and the Advanced Encryption Standard(A ES) are block cipher designs that have heen designated cryptography standerds by the US govemment (though DESs designation was finally withdrawn after the AFS was adopted) Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access Many

other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken, such as FEAI.

Stream ciphers, in contrast to the block' type, creare an arbitrarily long stream of key material, which is combined with the plaintext bic-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state that changes as the cipher operates. That internal state is iritially set up using the secret key material. RC4 is a widely used stream cipher; see category stream ciphers. Block ciphers can be used as stream ciphers; see block cipher modes of operation.

Cryptographic hash functions are a third type of cryptographic algorithm. They take a message of any length as input, and output a short, fixed length hash, which can be used in (for example) a digital signature.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt; the additional complication blocks a attack scheme against bare digest algorithms, and so has been thought worth the effort.

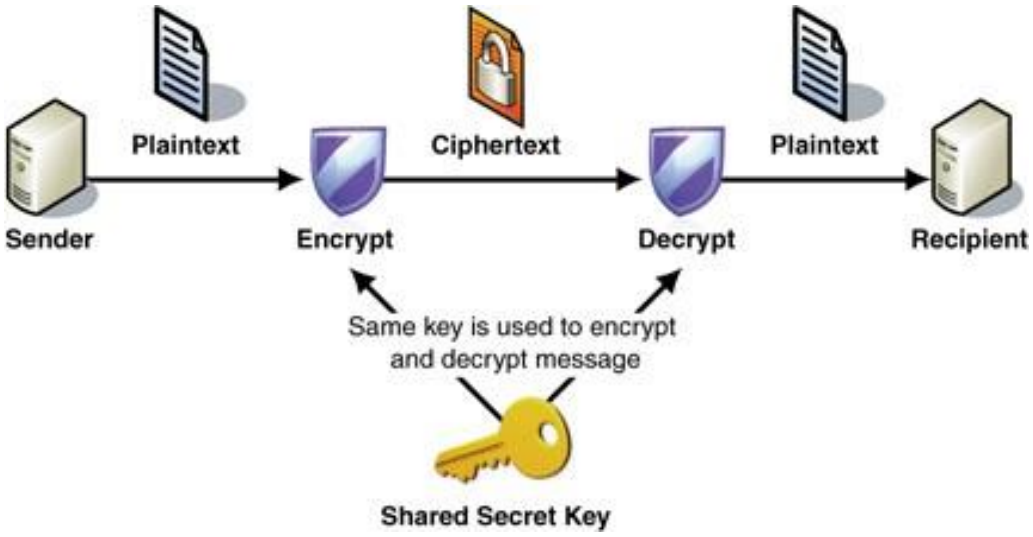

Fig. 1.2. Symmetric Key Algorithm

1.5.2 Asymmetric-Key Cryptography (Public-Key Cryptography):

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the Key Management necessary to use them securely Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well. The number of keys required

increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and sccrct. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

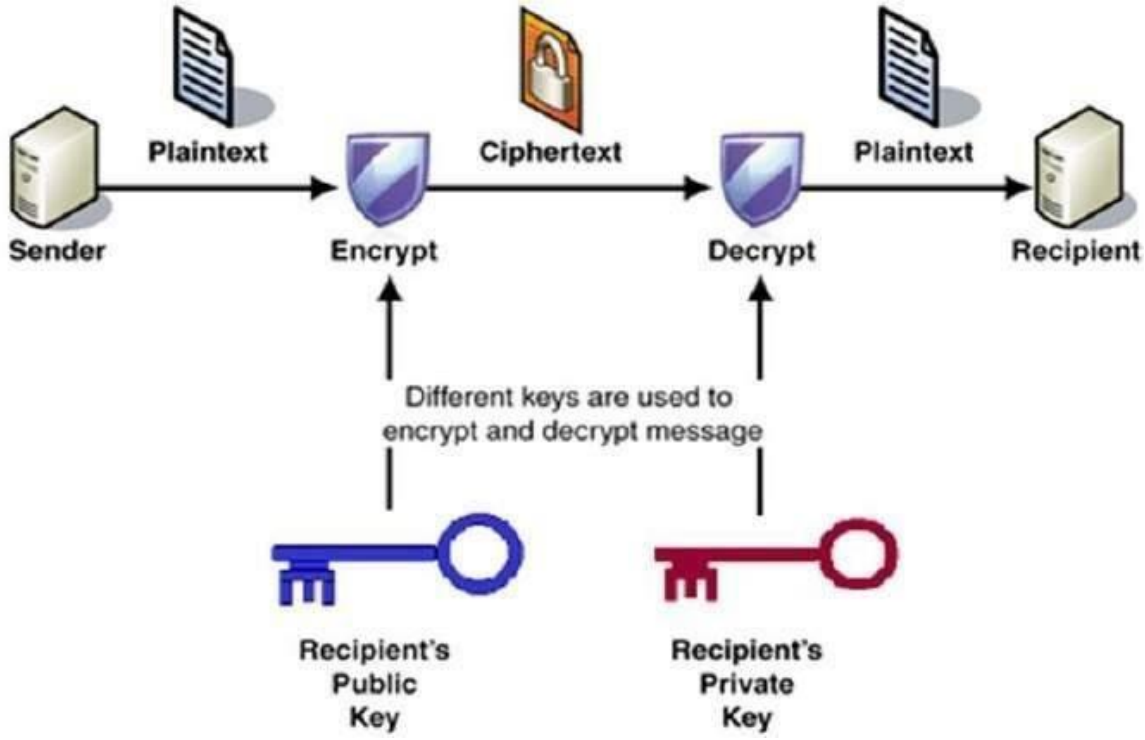

Fig. 1.3. Asymmetric Key Cryptography

In a ground-breaking, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used-a public key and a private key. A public key system is so constructed that calculation of one key (the 'private key) is computationally infeasible from the other (the 'public key"), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. The historian David Khan described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance"

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption. While Diffie and Hellman could not find such a system, they showed that public-key cryptography was

indeed possible by presenting the Diffie-Hellman key exchange protocol, a solution that is now widely used in secure communications to allow two parties to secretly agree on a shared encryption key. Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir and Len Adleman, whose solution has since become known as the RSA algorithm.

The Diffie-Hellman and RSA algorithms, in addition to be the first publicly known examples of high quality public-key algorithms, have been among the most widely used. Others include the Cramer-Shoup cryptosystem, ElCamal encryption, and various elliptic curve techniques.Too much surprise, a document published in 1997 by the Government Communications Headquarters (CCHQ), a British intelligence organization, revealed that cryptographers a GCHQ had anticipated several acedemic developments. Reportedly, around 19 Ellis had conceived the principles of asymmetric key cryptography. In 1973, Clifford Cocks invented a solution that essentially resembles the RSA algorithm. And in 1974, MaleolmJ Williamson is claimed to have developed the Diffie-Hellman key exchange.

Puhlic-key cryptography can alsc be used for implementing digital signature schemes. A digital signature is reminiscent of an ordinary signature; they both have the characteristic of being easy for a user to produce, but difficult for anyone else to forge. Digital signatures can also be permanently tied to the conten: of the message being signed; they cannot then be moved' from one document to another, for any attempt will be detectablc. In digital signature schemes, there are two algorithms: one for signing, in which a secret key is used to process the message (or a hash of the message, or both), and one for verification, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes (e.g.. SSL/TLS, many VPNs, etc.).

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie-Hellman and DSA are related to the discrete logarithm problem. More recently, elliptic curve cryptography has developed, a system in which security is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve

operations such as modular multiplication and exponentiation, which are much more computationally expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly hybrid. cryptosystems, in which a fast high-quality symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message but encrypted using a public-key algorithm.

II. PROBLEM DEFINITION

2.1 Existing System

The variation in the characteristics of the multimedia data such as correlation among the pixels and high redundancy of the image. Therefore there were some limits where same techniques cannot be used for protection all type of multimedia data. The traditional encryption algorithms may not use to encryption the image directly because of these reasons:

- As the size of image will be not same as the text it may varies. Hence the traditional encryption algorithm may take longer time to encrypt and decrypt the image compare to text.
- There is condition which says that the text encryption both decrypted and original text must be equal but it can be never true for the image. For decryption of image the small distortion is also accepted by the human perceptive.
- Computational time is high in exiting system.
- High computing power is required.
- For networking Systems it is not efficient. □

3.1 Proposed System

There should be a reliable storage and transmission of digital image where it has been served such as multimedia systems, medical and military imaging systems. The security of image is the most critical problem, due to increase in the growth of internet, cell phones and multimedia technology in the society.

This project is to propose a secure image encryption and decryption form by using AES algorithm. The AES algorithm is widely used in the applications of daily life, such as smart cards, cell phones, automated teller machines and WWW servers. AES encrypts a plaintext to a cipher text, which can be decrypted to the original plaintext by using common private key. The cipher text is made very different form so that it should not have any idea of the original plain text. For image encryption and decryption, the AES encrypt the image in different form using the key which should have no idea of original form. After decrypting it, it should be in the original form. The encryption of image should be strong so that it should not be known by the intruders.

Strengths of AES:

- AES is extremely fast compared to other block ciphers.
- As the round transformation is parallel for the design, which makes the important for the hardware to allow it for fast execution.

- AES was designed to be agreeable to pipelining.
- There is no arithmetic operations for the cipher, so there is no bias towards the big or little endian architectures.
- AES is fully self-supporting.
- AES is not based on obscure or not well understood processes.

III. LITERATURE SURVEY

In [1] the authors present a new Chaotic Key-Based Design for Image Encryption and Decryption. The VLSI architecture for image encryption and decryption algorithm is proposed. The XORed or XNORed bit-by-bit is used to predetermine keys for the chaotic binary sequence of the gray level of each pixel. There are the following features such as low computational complexity, no distortion, and high security. VLSI architecture has advantages such as low hardware cost, high computing speed, and hardware utilization efficiency. The architecture is also integrated with MPEG2 scheme and simulation results are also known. In [2] the authors present a Modified AES Based Algorithm for Image Encryption. Most common technique to provide the security for image is encryption. There are wide applications of image and video such as internet communication, multimedia systems, medical imaging, tele medicine and military communication. There are different image protection techniques such as vector quantization. There are different methods for vector quantization where the image is decomposed into vectors where encoding and decoding is done by vector by vector. Or by dividing the image into desired form into large number of shadows that guarantee the undetectable to illegal users. In [3] the authors present secure image encryption using AES. Security is the main and major issue in today's world. The transmission of image for communication has been increased and providing confidentiality from unauthorized access is the major task. It is difficult to provide an individual the security. There are various methods to protect the data from unauthorised user. AES is used for encryption and decryption of the image where the image using the key is converted into a form which cannot be recognised and later by authorised receiver it is converted back to original image.In [4] the authors present an image encryption and decryption using AES algorithm. The design of effectively security for the communication of the image is done by using AES algorithm for encryption and decryption. AES has replaced Data Encryption Standard (DES) by providing more security. AES key expansion uses the 128 bit key for encryption process by using bit wise exclusive or operation of image set pixels.

In [5] the authors present an Image Encryption Based n AES Key Expansion. There are specific characteristics of image such has high rate of transmission with limited bandwidth, redundancy, bulk capacity and correlation among the pixels. These are characteristics has to be notice will

encrypting the image. So, AES algorithm is used with the key expansion where encryption process is done by using bit wise exclusive or operation of image pixels set along with 128 bit key. The key is generated at the sender and receiver side based on the AES Key Expansion.

IV AIMS AND OBJECTIVES

The model for encryption and decryption of an image is designed with the some objectives:

- For transmission of the image based on data as well as storage it should have confidentiality and security by using suitable key.
- To study the architecture of the image file.
- To encrypt the image file by developing the application.
- Eventually, the image is focused on most famous file type of image format i.e. JPG.
- The image is focused to JPG file type which is the most famous type of image format.
- The application must be simple, easy to use and powerful.
- Many factors have to be considered in order to develop the application such as processing speed of image, the strength of encryption result and ease of use to end users.

V METHODOLOGY

AES encrypts a plaintext to a cipher text, which can be decrypted to the original plaintext by using common private key,

an example is shown in Figure 1a, It can be seen the cipher text should be in different from and gives no clue to the original plaintext. Figure 1a shows the Encryption of AES operation using cipher key. Where the plain text along with key is given to encryptor, which encrypt the plain text into cipher text, which is the result of encryption process. In reverse the decryption take place where the cipher text along with key is given to decryptor and it result into the original plain text.

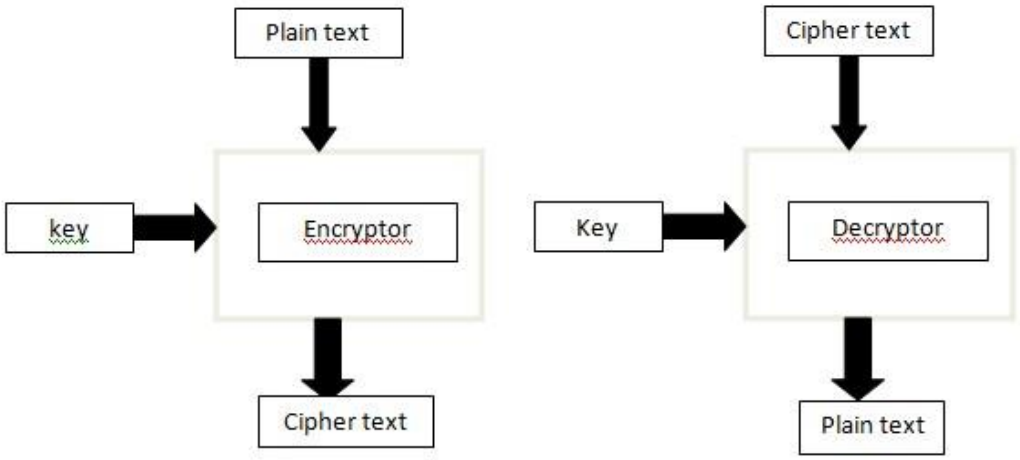

Fig 1a: Encryption and decryption of AES operation.

For the applications of AES image encryption and decryption, the encrypted image should be different from and give no clue to the original one, an example figure1b is shows the encrypted image and that encrypted image to original image.

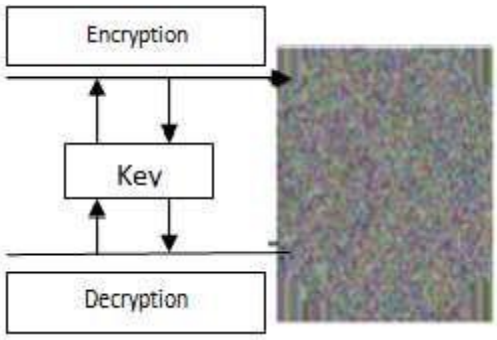

Fig 1b: Example for AES Encryption and Decryption

With AES encryption, the secret key is known to both the sender and the receiver. The AES algorithm remains secure, the key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text. The AES algorithm is designed to use one of three key sizes (Nk). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. These keys, unlike DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are then expanded via a key expansion routine for use in the AES cipher algorithm.

IV. Result and Conclusion

The image which has to be encrypted is chosen from the folder and the encrypt button is clicked. The original input image taken in the form of .GIF file as shown in fig 3. Once the image is encrypted successfully then the message is displayed fig 4. And when the image is viewed it show that the image is encrypted fig 5. For decryption of the image which has been encryptedthen the encrypted image has to be select and then decrypted button is clicked, then the successful decryption messaged is shown fig 6. When the image is viewed then it shows the original image shown in fig 7.

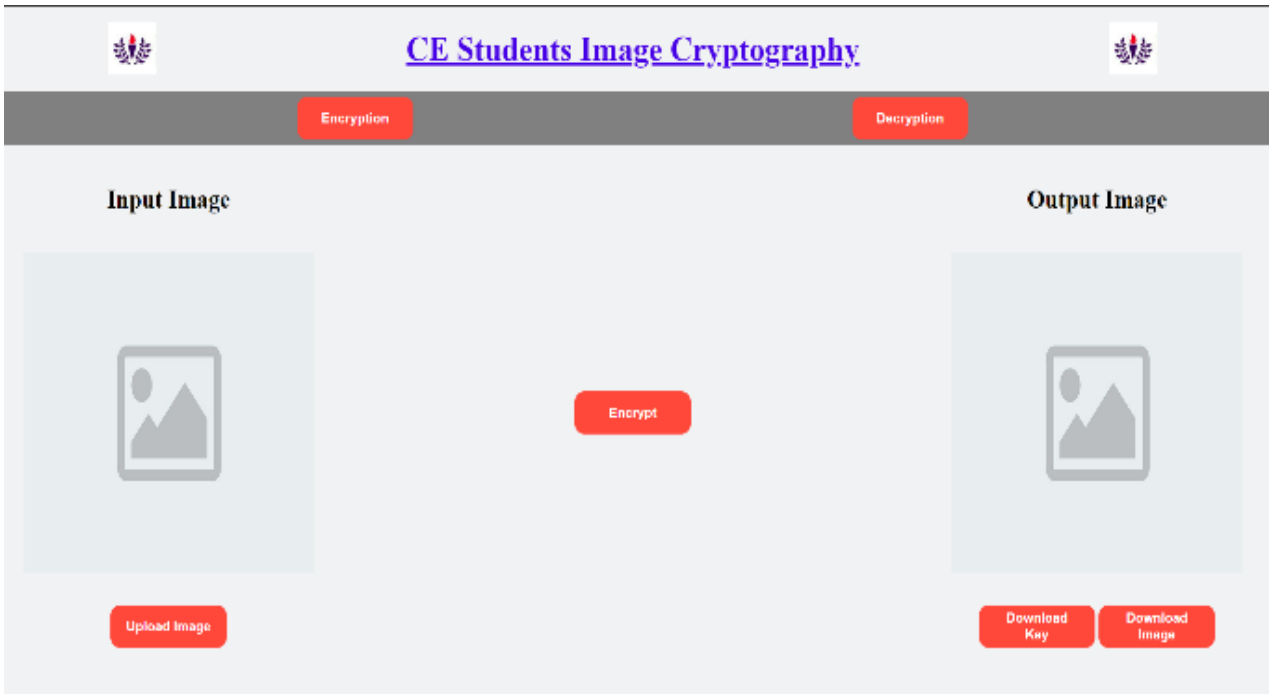

Fig 3: Input original image before encryption

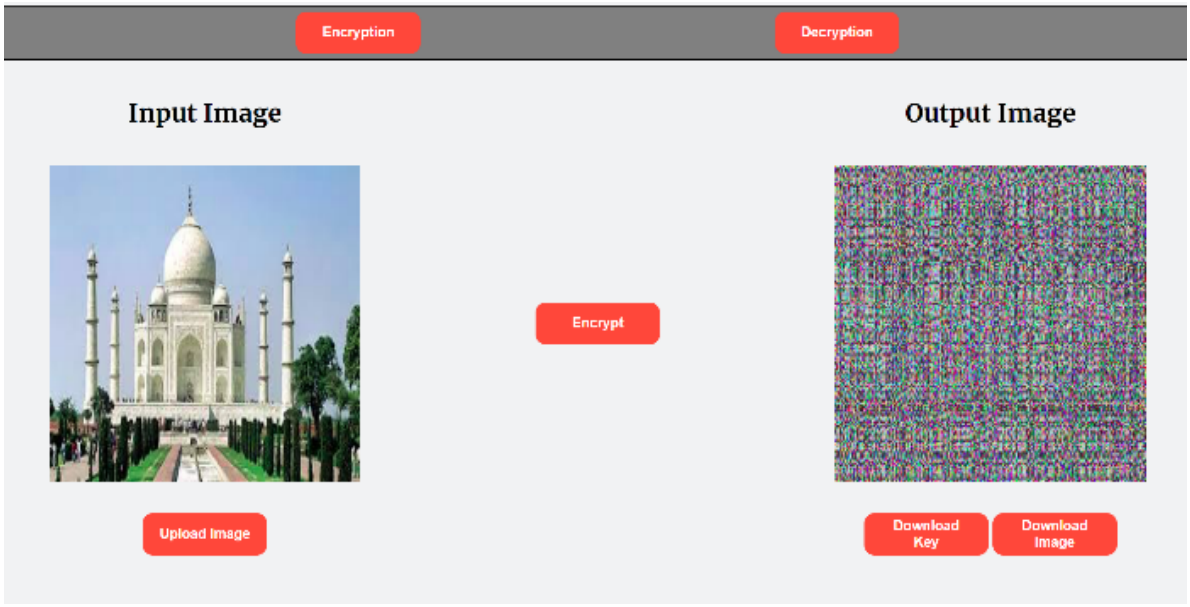

Fig 4: Successful of Encrypted image

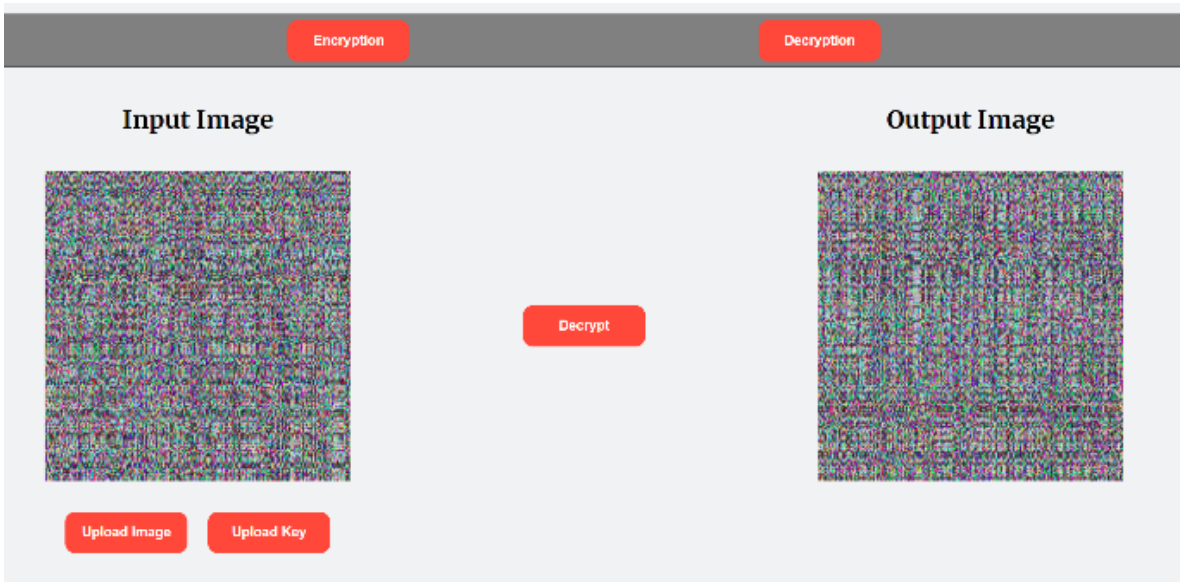

Fig 5: Encrypted image after decryption

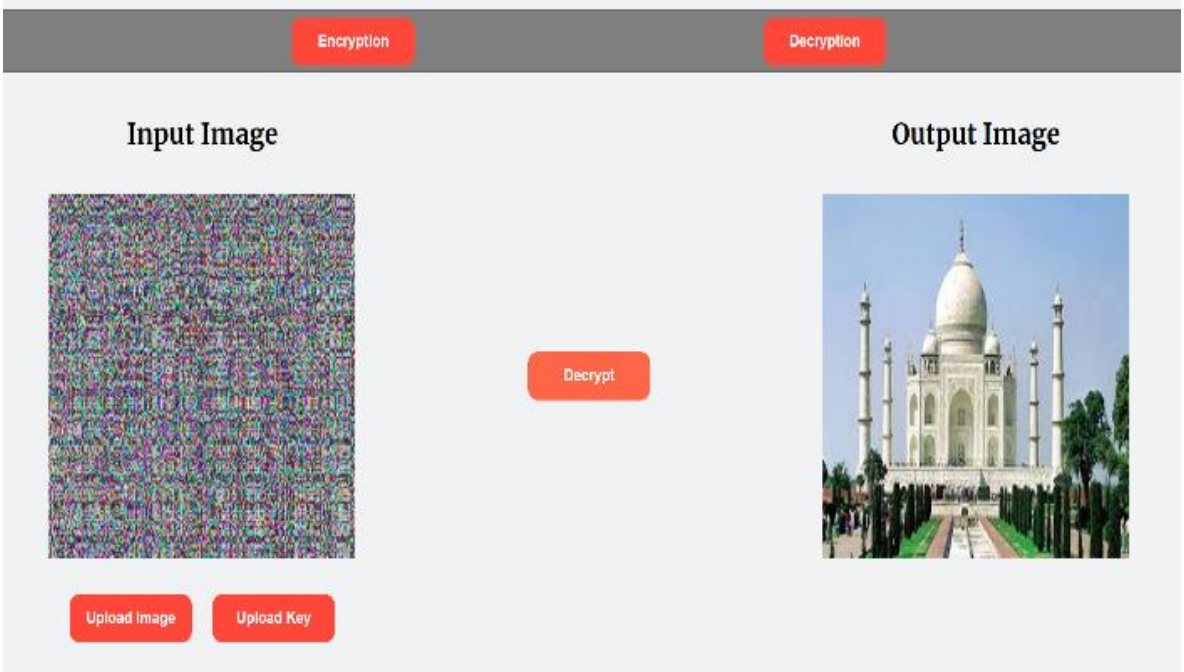

Fig 6: Successfully image decryption.

`

Fig 7: Original image.

The image is encrypted and decrypted using AES algorithm with 128 bit of key. The original image with key is given

where it is converted into a blank form and send to the receiver where receiver will convert back into original image using key. It provides the security form inducer and widely used.

V. REFERENCES

[1] Jui-Cheng Yen and Jim-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption",2000. [2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki , "A Modified AES Based Algorithm for Image Encryption" ,2007 .

[3] P. Radhadevi, P. Kalpana , "Secure Image Encryption Using Aes",2012 .

[4] Roshni Padate, Aamna Patel, "Image Encryption And Decryption Using Aes Algorithm" ,2014.

[5] Jose´ J. Amador, Robert W. Green, "Symmetric-Key Block Cipher for Image and Text Cryptography", 2005. [6] Philip P. Dang and Paul M. Chau, "Image Encryption For Secure Internet Multimedia Applications", 2000.

[7] Sanjay Kumar, Sandeep Srivastava, "Image Encryption using Simplified Data Encryption Standard (S-DES) ", 2014.

[8] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption Using Advanced Encryption Standard", 2014

[9] P.Karthigaikumar, Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm", 2011. [10] B.Subramanyan, Vivek.M.Chhabria, T.G.Sankar babu , "Image Encryption Based On AES Key Expansion", 2011