IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE IMAGE TRANSFER USING SMTP

[1]Desathi Avinash Babu, [2]Singamsetty GowriShankar, [3]Salapaka Prasanthi,[4] Bantupalli Gayatri Harshitha,

[5]Sachana Prema Divya Swaroopini

[1] Assistant Professor, [2]B.Tech Graduate, [3]B.Tech Graduate, [4] B. Tech Graduate, [5]B.Tech Graduate

[1]Computer Science And Engineering

[1]Satya Institute Of Technology And Management, Vizianagaram, India

Abstract: Confidentiality is major task for every sector, keeping things confidential among the organization is the most important factors. Providing security for information is also 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 intruders. In this paper, we propose Email authentication for encrypted and decrypted image.

In our framework, first, the confidential image will be encrypted using a symmetric key algorithm, Advanced Encryption Standard (abbreviated as AES) by the sender and the encrypted image will be send via Email to receiver. The Cryptographic algorithms provides security to the image, as we proposed AES to our framework it will become more difficult to crack the original image for intruders.

Moreover there are some other encryption algorithms to encrypt and decrypt the image but Advanced Encryption standard has its unique features like it protects from brute-force attack and image takes less rounds to encrypt,etc. that gives more security compare with other symmetric algorithms. And Email provides a secure transmission of encrypted image.

The above results and analysis for crypto system based on AES algorithm give a high performance. So we have reason to believe that use of this method to encrypt and decrypt the image and sending via Email will have a very good prospect in the future.

Keywords **–Image, Cryptography, Encryption, Decryption, AES, SMTP, security analysis**

I. INTRODUCTION

A major issue for computer networks is to prevent important information from being disclosed to illegal users. For this reason, encryption techniques were introduced. Most encryption techniques have an easy implementation and are widely used in the field of information security.During the last decade, the use of computer networks has grown spectacularly, and this growth continues unabated. New networks are being installed and connected to the global internet. The internet is commonly seen as the first incarnation of an information superhighway. Today, the information transmitted over the internet is not only text but also contains multimedia like images, audio, etc. Most images are used. However, the more extensively the images are used, the more important their security will be. For example, it is important to protect military image databases, ensure confidential video conferencing, and protect personal online photo albums.However, with the growth of computer processors processing power and storage, illegal access has become easier. As a result image security has become an important topic in the current computer world.Most traditional or modern cryptosystems have been designed to protect textual data. The original plain text is converted into cipher-text (a hidden form of the message) which is stored or transmitted over a network. Upon reception, the cipher text can be transformed back into the original plain text by using a decryption algorithm. However, the images are different from the text. Although the traditional cryptosystems, such as RSA and DES-like cryptosystems may be used, to encrypt images directly, it is not a good idea for two reasons.One is that the image size is always much greater than that of the text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data.The second is that the decrypted text must be equal to that of the original text. However, this requirement is not necessary for image data. This is due to the characteristics of human perception; a decrypted image containing small distortion is usually acceptable.A digital image is defined as a two-dimensional (2D) rectangle array. The elements of this array are denoted as pixels. Each pixel has an intensity value (digital number) and a location address (row, column). For protecting the stored 2D data, they must be converted to one-dimensional (1D) arrays before using various traditional encryption techniques. The raster sequence of image data can be encrypted into blocks by using a block cipher or a stream cipher. A product cipher can also be used to encrypt a file of image data. However, it is more efficient to encrypt an image after employing some compression techniques. This will reduce the computational requirement and also increases the speed of processing (which is of high importance in a real-time scenario).

II. PROBLEM STATEMENT

The two fundamental issues that emerge in the picture encryption process are regard to the time it takes for its calculation and its security level. For ongoing picture encryption, just those codes are ideal which takes a lesser measure of computational time without compromising security. An encryption plot that runs gradually, despite the fact that many have a more serious level of safety highlights would be of minimal pragmatic use for ongoing cycles. Subsequently a compromise must be made.

Numerous encryption strategies have been proposed in the writing, and the most widely recognized method for safeguarding enormous mixed media documents is by utilizing regular encryption procedures. Confidential Key mass encryption calculations, like Triple DES or Blowfish, are not reasonable for the transmission of a lot of information (like pictures). Because of the intricacy of their inner design, they are not especially quick as far as execution speed and can't be applied for pictures continuously situations. Additionally, customary cryptographic procedures, for example, DES can't be applied to pictures because of the inherent properties of pictures like mass information limit, overt repetitiveness, and high connection among pixels. Picture encryption calculations can turn into an indispensable piece of the picture conveyance process assuming that they point toward productivity and simultaneously safeguard the security level.

III. RELATED WORKS

Compression and encryption schemes are based on SCAN patterns generated by the SCAN technique. Kuo proposed an image encryption method - image distortion, which obtains the encrypted image by adding the phase spectra of the plain image with those of the key image. This method is safe but the image is not compressed, thus encryption & decryption is inefficient. Here again, security is high but no image compression is considered.
Public key encryption schemes are not suitable for encrypting large amounts of data and archival due to their relatively slow performance. Advances in algorithmic techniques and number theory force us to re-encrypt large databases and archives with a longer key to maintain a sufficient degree of security. Here a chaotic map is first generalized by introducing parameters and is discretized to a finite square lattice of points (image) which represent data items (pixel). The main features of the encryption scheme studied in this paper are a variable key length, a relatively large block size (several kB or more), and a high encryption rate.

Due to the differences between images and text, a wide variety of cryptographic algorithms have been proposed for image security.In the paper 2, Kuo proposed an image encryption method - image distortion, which obtains the encrypted image by adding the phase spectra of the plain image with those of the key image.This method is safe but the image is not compressed, thus encryption decryption is inefficient.In the paper 3, Bourbakis and Alexopoulos developed a new method that performs both lossless compression and encryption of binary and gray-scale images.The compression and encryption schemes are based on SCAN patterns generated by the SCAN technique.SCAN is a formal language-based two-dimensional spatial-access methodology that can efficiently specify and generate a wide range of scanning paths or space-filling curves.Here again, security is high but no image compression is considered.In the paper 4, Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen used one of the popular image compression techniques, vector quantization, to design an efficient cryptosystem for images.The scheme is based on vector quantization VQ, cryptography, and other number theorems.In VQ, the images are first decomposed into vectors and then sequentially encoded vector by vector.Major advantage- simple hardware structure required bit-rate for VQ is also small.In the paper 5, Fridrich demonstrated the construction of a symmetric block encryption technique based on a 2D standard chaotic map.In this paper to encrypt large data files private-key symmetric block encryption schemes are used because public key encryption schemes are not suitable for encrypting large amounts of data and archival due to their relatively slow performance.

3.1 EXISTING SYSTEM

In January, 1997 NIST began its effort to develop the AES, a symmetric key encryption algorithm, and made a worldwide public call for the algorithm to succeed DES. Initially 15 algorithms were selected, which was then reduced down to 4 algorithms, RC6, Rijndael, Serpent and Two-fish, all of which were iterated block ciphers. The four finalists were all determined to be qualified as the AES. The algorithm had to be suitable across a wide range of hardware and software systems. The algorithm had to be relatively simple as well. After extensive review the Rijndael algorithm was chosen to be the AES algorithm.The Rijndael Algorithm For Rijndael, the length of both the block to be encrypted and the encryption key are not fixed. They can be independently specified to 128, 192 or 256 bits. The number of rounds, however,varies according to the key length. It can be equal to 10, 12 and 14 when the key length is 128bits,192 bits and 256 bits, respectively. The basic components of Rijndael are simple mathematical, logical, and table lookup operations. The latter is actually a composite function of an inversion over
Galois Field (GF) with an affine mapping. Such structure makes Rijndael suitable for hardware implementation.

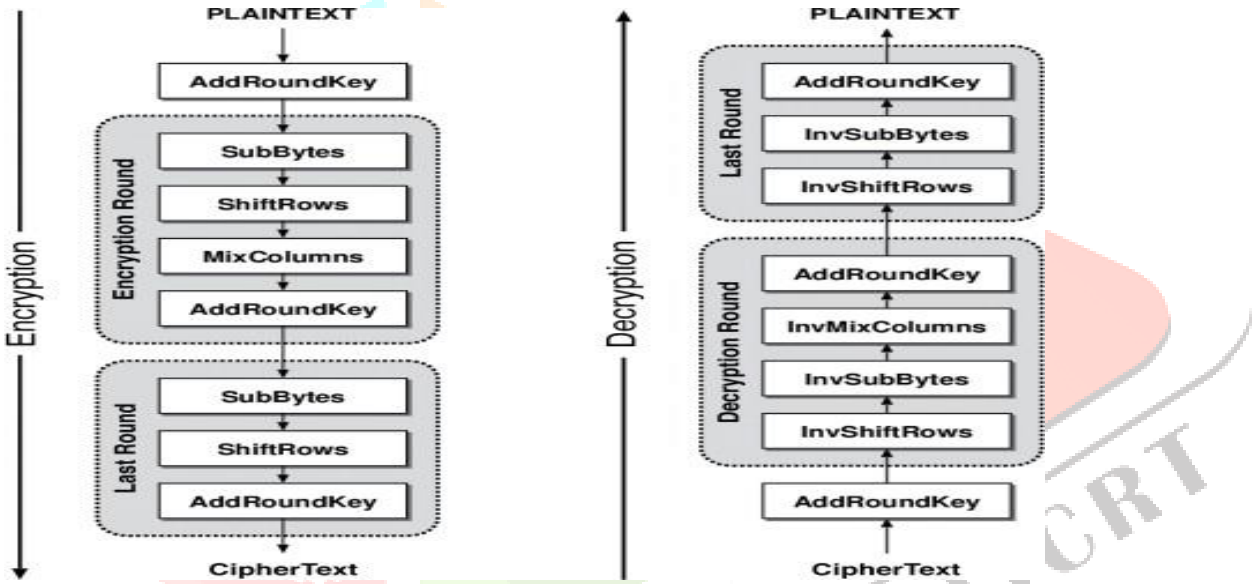
3.2 PROPOSED SYSTEM

As there is rapid growth of using images in many fields, so it is important to protect the private image data from intruders. In this paper, we propose Email authentication for encrypted and decrypted image. Our proposal in this project is extended i.e we designed a very friendly UI which contains different options named encryption, decryption, send email where the process basically starts after the encryption of the image. In this the sender can directly send the encrypted image to a particular email or targeted email very easily without any data leakage. And the receiver can also receive the encrypted image without any data leak and decrypt it on the same frame work. AES or Advanced Encryption Standard, an algorithm used for high-security purposes encrypts the electronic data established by the US National Institute of Standards and Technology. It also happens to be a replacement for the DES or Data Encryption Standard. DES is also the only predecessor of AES.

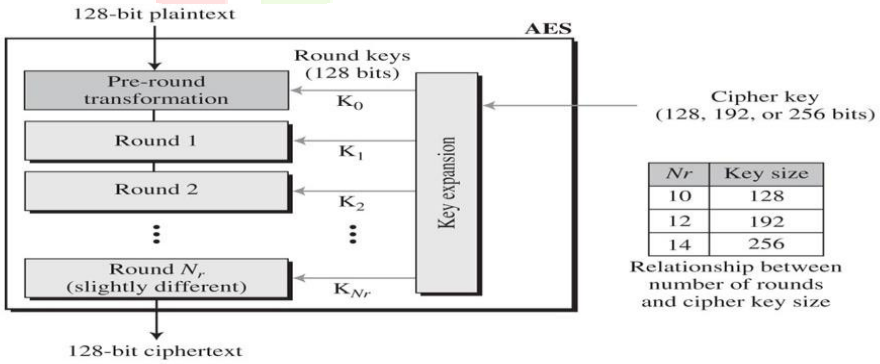
DES was the federal standard for block symmetric encryption in 1977. The DES is a symmetric key block cipher that is published by the National Institute of standards and technology. It is an implementation of the Feistel cipher. DS uses 16 rounds of Feistel structure. The key length of DES is 64 bits but the effective key length is only 56 bits. The remaining 8 bits aren't used by the encryption algorithm. SMTP stands for Simple Mail Transfer Protocol ,is a set of communication guidelines that allow software to transmit an electronic mail over the internet. It is a program used for sending messages to other computer users based on e-mail addresses.

IV. DATA FLOW DIAGRAMS

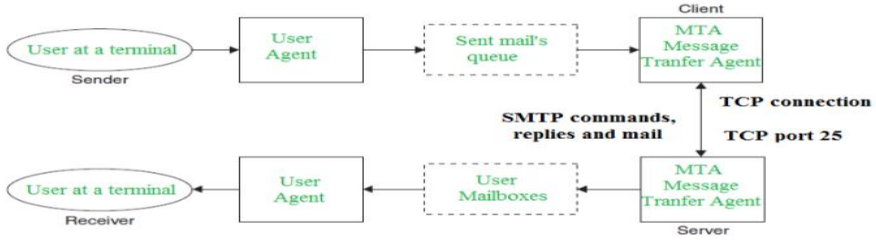
ENCRYPTION & DECRYPTION PROCEDURE AES :



KEY GENERATION :



SMTP PROTOCOL :



V. RESEARCH METHODOLOGY

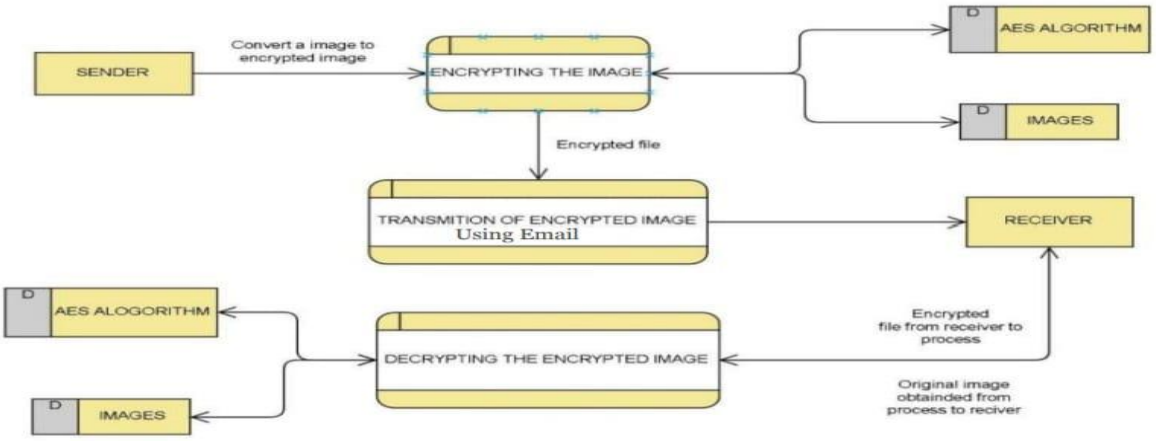
Every encryption and decryption process has two aspects: the algorithm and the key use for the encryption and decryption. Encryption is a wide topic that takes years to fully understand, so we won't take up too much space in this guide to explain the fundamental principles of the practice.
In short, though, encryption generally works by taking a piece of data you want to keep confidential and scrambling it, making it unreadable to anyone who doesn't have the secret key required to unscramble it.
Different protocols go about this differently, with some — such as AES — utilizing a "symmetric-key algorithm," which means that the same key encrypts and decrypts the data.
The opposite of symmetric encryption is (surprise, surprise) "asymmetric encryption," where a publicly available key encrypts the data. However, a separate secret private key has to decrypt it again.
However, it is the key used for encryption and decryption that makes the process of cryptography secure. There are two types of cryptographic mechanisms: symmetric key cryptography in which the same key is use for encryption and decryption. In case of asymmetric key cryptography two different keys are used for encryption and decryption. Symmetric key algorithm is much faster and easier to implement and required less processing power as compare to asymmetric key algorithm. The advance encryption standard (AES) specifies a federal information processing standards publication (FIPS) approved cryptographic algorithm that can be used to protect electronic data.Our Methodology is to realise an image cryptosystem that, besides the above mentioned characteristics, also posses the following characteristics:

1.System should be computationally secure i.e., it should have an extremely long computation time to break. In other words unauthorized users must not be able to read privileged images.

2.Encryption and decryption should be fast enough not to degrade system performance. i.e., the algorithm should be simple enough to be done by users with a personal computer.

3.The security mechanism should be widely acceptable to design a cryptosystem like a commercial product; and should be flexible.

The three basic characteristics in the information security field: privacy (an unauthorized user cannot disclose a message), integrity (an unauthorized user cannot modify or corrupt a message) and availability (messages are made available to authorized users faithfully).A perfect image cryptosystem is not only flexible in the security mechanism, but also has high overall performance. We use AES algorithm to provide more security to the image.The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits and the main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.



VI. CONCLUSION

The proposed algorithm offers high encryption quality with minimal computational time. The key sensitivity and key space of the algorithm are very high which makes it resistant to Brute force attacks and statistical cryptanalysis.The time taken for encryption is relatively less in comparison with the algorithms proposed in the literature. And Email provides a secure transmission of encrypted image.The above results and analysis for crypto system based on AES algorithm give a high performance. So we have reason to believe that use of this method to encrypt and decrypt the image and sending via Email will have a very good prospect in the future.We show that the proposed algorithm is more efficient than other known public key encryption schemes such as ECC, AES-ECB, RSA and DSA.Our proposed method was compared against the existing methods on a number of publicly available benchmark tests such as RC6, RC5, DES

VII. REFERENCES

[1] B.SUBRAMANYAN, VIVEK.M.CHHABRIA, T.G.SANKAR BABU, IMAGE ENCRYPTION BASED ON AES KEY EXPANSION, 2011 SECOND INTERNATIONAL CONFERENCE ON EMERGING APPLICATIONS OF INFORMATION TECHNOLOGY, PAGE 217-220.

[2] C.J.Kuo, Novel image Encryption Technique and its application in progressive transmission. Journal of Electron imaging 24 1993 pp 345-351.

[3] N.J.Bourbakis, C.Alexopoulos, Picture data encryption using SCAN patterns. Pattern Recognition 256 1992 pp567 - 581.

[4] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-91.

[5] Fridrich Jiri, Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurcation Chaos 8 (1998) (6), pp. 1259– 1284.

[6] Mitra, Y. V. Subba Rao, and S. R. M. Prasanna, A new image encryption approach using combinational permutation techniques, International Journal of Computer Science, vol. 1, no. 2, pp. 1306- 4428, 2006.