DATA SECURITY BY TEXT AND IMAGE BASED ENCRYPTION-DECRYPTION USING AES

[1]Jyoti R Maranur, [2] Pooja S Honnutagi,
[1]ASST.Professor, [2]ASST.Professor,
[1]Computer science and engineerring,
[1]Godutai engineering college for women, Kalaburagi, India

Abstract : In recent years, a lot of applications based on internet are emerged such as on-line shopping, stock trading, internet banking and electronic bill payment etc. Such transactions, over wire or wireless public networks demand end-to-end secure connections, should be confidential, to ensure data authentication, accountability and confidentiality, integrity and availability.

***Keywords**: AES,STEGNOGRAPHY*

I. Introduction

In recent years, a lot of applications based on internet are emerged such as on-line shopping, stock trading, internet banking and electronic bill payment etc. Such transactions, over wire or wireless public networks demand end-to-end secure connections, should be confidential, to ensure data authentication, accountability and confidentiality, integrity and availability.

The NIST Computer Security Handbook defines the term computer security as, "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)." Security is the mechanism by which information and services are protected from unintended or unauthorized access, change or destruction. Security in networking is based on Cryptography (a word with Greek origins, means "secret writing"), the science and art of transforming messages to make them secure and immune to attack /Encryption is one of the principal means to guarantee security of sensitive information. Encryption algorithm performs various substitutions and transformations on the plaintext (original message before encryption) and transforms it into ciphertext (scrambled message after encryption). Many encryption algorithms are widely available and used in information security. Encryption algorithms are classified into two groups: Symmetric-key (also called secret-key) and Asymmetric-key (also called public-key) encryption. Symmetric key encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys – one a public key and one a private key. It is also known as public-key encryption.

Digital steganography is a means of hiding the data behind the digital information like images, videos, music etc. The hackers if extracts the packet they would feel that there are only digital information and no data is associated. But complex de-stegano methods can be built to extract the data from the images. The data in the digital information is stored as a noise. By studying the noise behavior the presence of data can be estimated .Where as the cryptography is a method by means of which the original contents of the data is changed either using linear keys of using the matrix keys. Many such algorithms are available like DSA, RSA etc. Decrypting such data is tough but as they are conventional methods, by implementing reverse mathematics, data can be decoded. The work therefore attempts to integrate the facilities of both the above-mentioned methods as a single data protection interface. Data is encrypted first by linear cryptography and then is hidden behind the images. Thus extraction of the data from such model is difficult.

The packet headers will not be encrypted like the other method. Only the data would be protected. Therefore all the intermediate nodes would not require encrypting the packet and decrypting it. Hence routing would not get slow down due to this procedure. Only the end users are required to participate in the procedure.

Linear cryptography would be used in this project where the password would be generated by XORing the bytes of a Key file with the linear password text. This would in terms be XORed with the text message bytes.As this is a method just to demonstrate the encryption integration with the steganography, throughout the work emphasis would be given on steganography

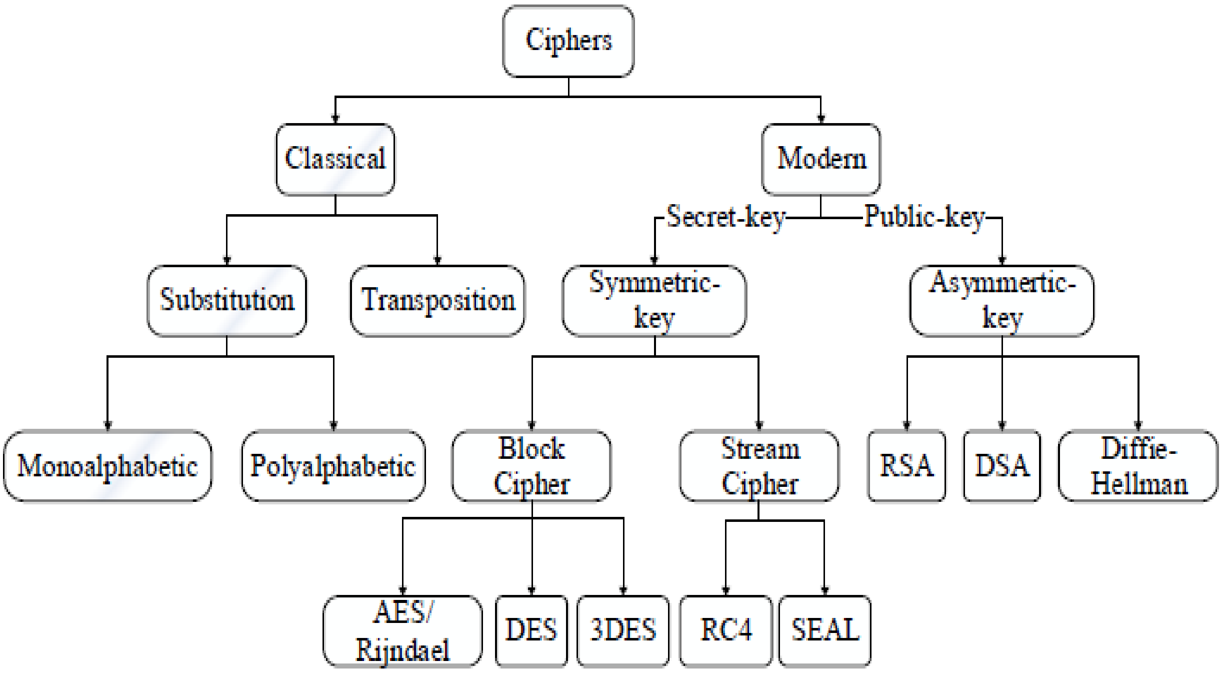


Fig1. Tree view for data steganography techniques

II. LITERATURE SURVEY

Mayanak Mishra et.al[1] In the era of digital transaction, in order to transact the data in a more secured manner the need for a cryptographic algorithm is inevitable. There are numerous numbers of cryptographic algorithms which makes the system invulnerable from the attacks of intruders and eavesdroppers.RivestCipher4 algorithm is one such cryptographic algorithm which is very well known for its performance and simplicity. In this paper, we propose a software toolkit for increasing the key strength so that it will be very hard for the intruder to break the key and this technique will act as black box so that intruder will have no idea about the key formation. So it will lead to increased key complexity which obviously results the intruder nothing else than confusion and frustration.

Vikas Agarwal et.al[2] On considering the current scenario, Most of the existing systems which offer security to a network or web or to a data are vulnerable to attacks and they are breached at some point of time by effective cryptanalysis, irrespective of its complex algorithmic design. In general, today's crypto world is restricted to a practice of following any one single encryption scheme and that too for a single iteration on a single file basis. This is evident in the 99% of the encryption-decryption cases. So, A need for "practically strong and infeasible to get attacked" technique becomes vital. In this paper, we propose a Software tool which involves Cryptographic enciphering and deciphering along with File Splitting and Merging mechanisms. We used modified Blowfish algorithm for Encryption and Decryption of data. Though we use only one algorithm, we differentiate the cryptographic scheme by varying the key for varying file slices. Our results clearly justifies that our tool serves as a better solution both in terms of performance as well as security.

In Recent times, we are facing various challenges in security related issues during data transfers. There are various security models following different enciphering techniques for the betterment of secured data transfer. Though there exist many complex cryptographic encryption algorithms, which provide high level of security, vulnerability of those algorithms increases day after a day. It is to be worth saying a point that modification of existing complex algorithms will obviously intensifies to the enhancement in security of algorithm as well as the data ,provided the modification should not be eavesdropped easily than the original algorithm. In this paper, we proposed a software tool which considerably enhances the security by following an iterative approach depending upon sender's need. Our experiments show that the use of iterative approach enhances the security provided by the algorithm when compared to the non-iterative approach.

In this study we propose a new hybrid technique of combining "the twins" cryptography, Steganography along with the compression techniques which results in a new extreme of providing informational security. The importance of information not only depends upon its contents but also upon its safety arrival to the receiver. Nowadays, eavesdropping one's personal messages and exposing it to the air becomes passion of showing one's technical expertise to the world. There are numerous occurrences of breaching of message contents even where the data equipped with the techniques of Steganography and cryptography. So, a need for "practically unbreakable and non suspicious systems" becomes vital. Our experimental results shows that our system is unique in its design and as well as in its performance when compared to a specific steganographic or a cryptographic technique.

III.METHODOLOGY

Steganography Technique

The word steganography comes from the Greek Steganos, which means covered or secret and -graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected. A secret information is encoded in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data . It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect there is secret information in a carrier medium, then the method has failed.

The basic model of steganography consists of Carrier, Message and Password. Carrier is also known as a cover-object, which embeds the message and serves to hide its presence. Basically, the model for steganography is shown in Fig. Message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a hit stream such as a copyright mark, a covert communication, or a serial number. Password is known as a stega-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object.

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. There are several suitable carriers that can be used as the cover-object as listed below:

- Network Protocols such as TCP, IP and UDP.
- Audio that use digital audio formats such as way, midi, avi, mpeg, mpi and voc.
- File and Disk that can hide and append files by using the slack space.
- Text files such as html and java.
- Image files such as bmp, gif and jpg, where they can be both color and gray-scale.

In general, the information hiding process extracts redundant bits from cover-object. The process consists of two steps.

- Identification of redundant bits in a cover object. Redundant hits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-object.
- Embedding process. It selects the subset of the redundant bits to be replaced with data from a secret message. The stego-object is created by replacing the selected redundant bits with message bits.

STEGANOGRAPHY TECHNIQUES

Information hiding techniques are receiving much attention today. The main motivation for this is largely due to fear of encryption services getting outlawed, and copyright owners who want to track confidential and intellectual property copyright against unauthorized access and use in digital materials such as music, film, book and software through the use of digital watermarks.

There are many ways to hide information in digital images. Each of these techniques has varying degrees of success. We look at the following approaches:

- least significant bit insertion
- masking and filtering
- algorithms and transformations
- Least significant bit insertion

LSB is a simple approach to embed information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not .result in human-perceptible difference because the amplitude of the change is small.

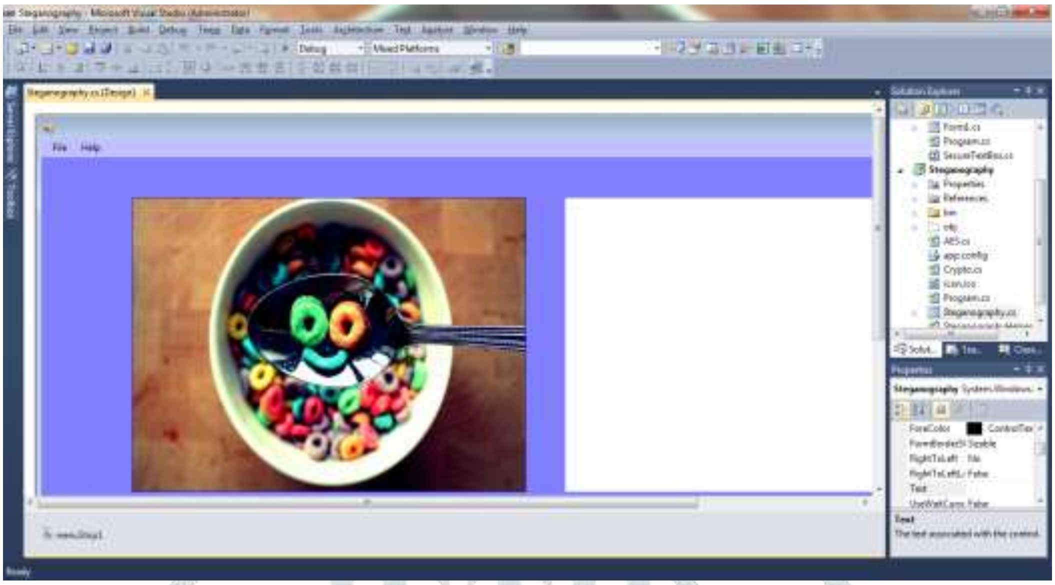
- Masking And Filtering

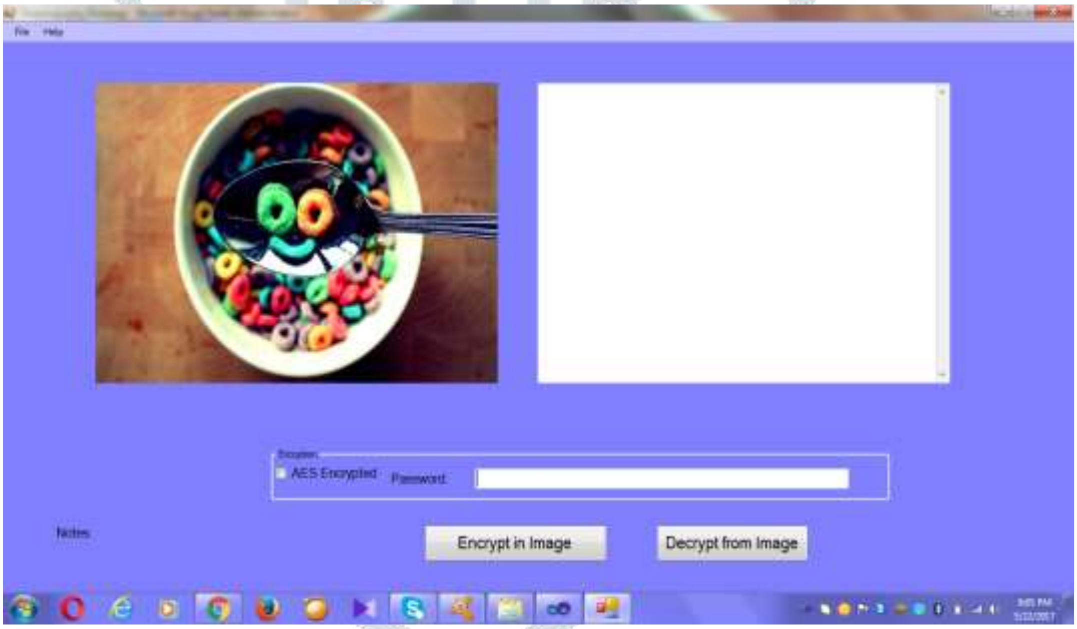
Masking and filtering techniques, usually restricted to 24 bits and gray scale images, hide information by marking an image, in a manner similar to paper watermarks. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover-image than just hiding it in the noise level.

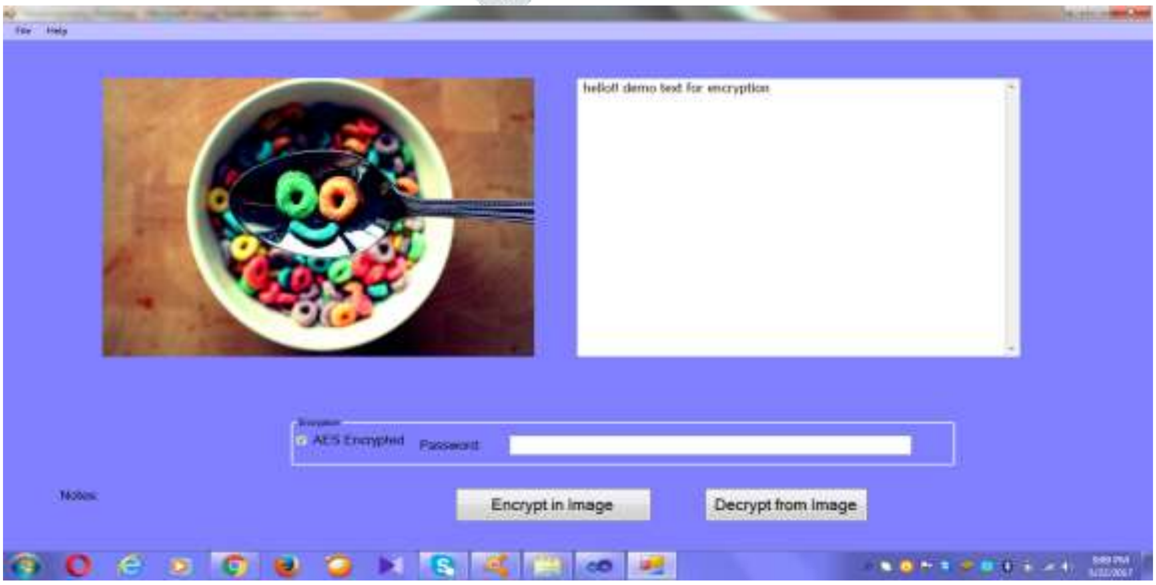
- Algorithms And Transformations

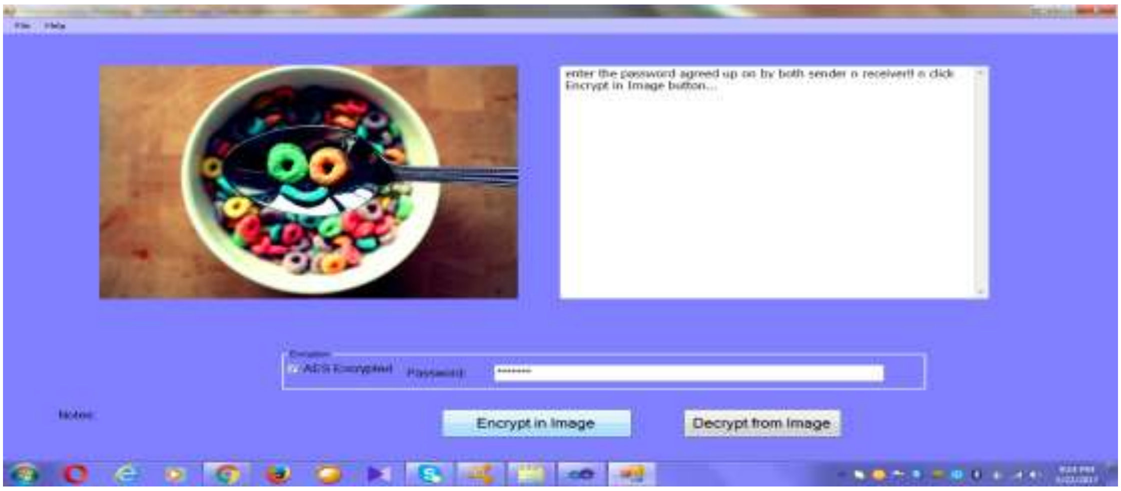
Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in PEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods bide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variants.

IV.EXPERIMENTAL RESULT



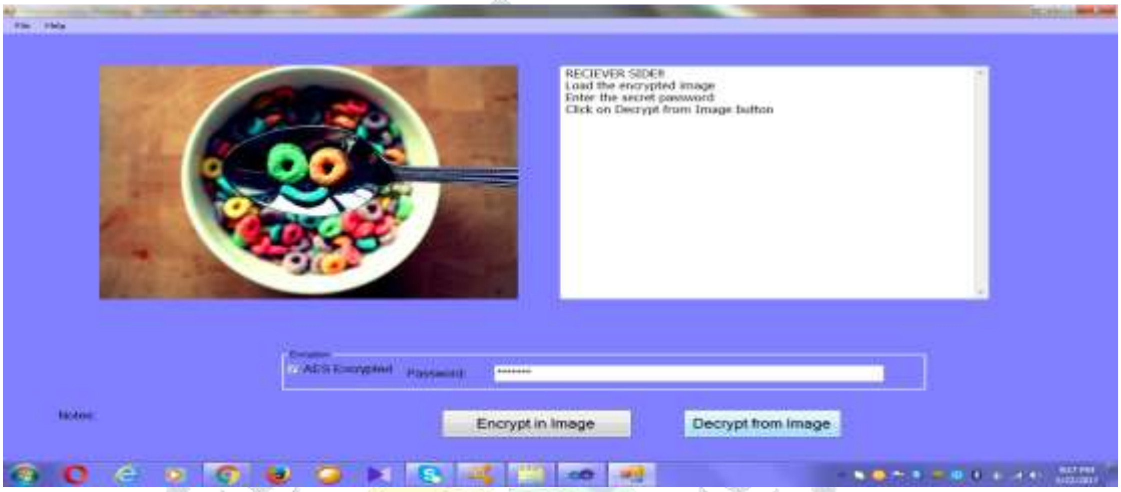



hello!! demo text for encryption



enter the password agreed up on by both sender n receiver!! n click Encrypt in Image button...

☑ AES Encrypted Password: ********



RECIEVER SIDE!!
Load the encrypted image
Enter the secret password
Click on Decrypt from Image button

☑ AES Encrypted Password: ********

FUTURE SCOPE

With the fast progression of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. Information Confidentiality has a prominent significance in the study of ethics, law and most recently in Information Systems. With the evolution of human intelligence, the art of cryptography has become more complex in order to make information more secure. Arrays of Encryption systems are being deployed in the world of Information Systems by various organizations.

CONCLUSION

A new approach for achieving a secured data transmission in an enhanced way. From the experimental results it has been evident that this approach overcomes the traditional methods for encryption. The novelty of this approach is that the original data is divided into two segments by rearranging their positions and then the two segments are combined, which results in a modified numeric data.

The modified numeric data is fed as an input to the encryption algorithm. For better security, we use AES algorithm for encryption and decryption. One major limitation of the system is about the AES key generation part which can be eliminated by strengthening the key generation process. In the future this work can be continued by adding noise.

REFERRENCE

[1] [1] Mayanak Mishra, Prashant Singh, Chinmay Garg "A New Algorithm of Encryption and Decryption of images using chaotic mapping" International Journal of Information and computation technology Volume No.4, Issue No.7, 2014.

[2] [2] Vikas Agarwal ,shruthi agarwal,rajedh deshmukh "Analysis and review of encryption and decryption for secure communication" International Journal of scientific engineering and research, February , 2014

[3] [3] Shetty deepesh sananda,anush karkala "Image encryption and decryption using image gradient technique" International Journal of Emerging technology and advanced engineering" , 2014

[4] [4] Rajindar kaur ,Kanwalpreet singh "Comaparative analysis and implementation of image encryption and decryption" International Journal of Computer science and mobile computing, Volume-2, Issue-4 , April, 2013

[5] [5] Shika kuchhcal and ishank kuchhal " Data security using RSA algorithm in matlab" International journal of innovative research and development, July, 2013.

[6] [6] Pia Sing ,prof.karamjeet singh “ Image encryption and decryption using blowfish algorithm in matlab” Interanational journal of scientific and engineering research ,July-2013

[7] [7] Anju,Babita,Reena and Ayushi Aggarwal “ An Approach to improve the data security using encryption and decryption techniques” , international journal of information and computation technology,2013