Combination of Cryptography and Steganography

VIPUL WAGHAMODE

Co-author: – Prof. Samitha Khaiyum

PG SCHOLAR, DEPT of MCA, DSCE

CA- ASST.PROF, DEPT of MCA, D.S.C.E

ABSTRACT

People are concerned about the protection of data transmitted over the internet. There are several strategies for preventing data from falling into the hands of unauthorized people.Steganography and cryptography are two commonmethodsfor transmitting sensitive data in a secure manner or in secrete way.One conceals the presence of the message and the other contorts the message without anyone else .In this paper we are centered around the high level LSB(least critical piece) and RSA Algorithm. By coordinating with data to an image or picture, there chance is less of an assailant having the option to utilize steganalysis to recuperate data. Prior to concealing the information in a picture the application

Keywords: Cryptography, Steganography, AES Algorithm, RSA Algorithm, LSB method,LSB Technique

LITERATURE SURVEY

Steganography and cryptography are the two distinct strategies of stowing away data which give secrecy and respectability of information (Raphael and Sundaram, 2011). Li et al. (2011) likewise expressed that steganography procedure expects to communicate a message on a channel, where some other sort of data is now being communicated.The focus of steganography is to cover informations inside the other progressed media in a manner that doesn't allow any person to attempt to recognize the presence of secret message as written in "Secure data transmission using steganography and encryption" (Laskar and Hemachandran, 2012b).

The Information Encryption Standard (DES) calculation has been a mainstream secret key encryption calculation and is utilized in numerous business and monetary applications. In spite of the fact that presented in 1976, it has demonstrated impervious to all types of cryptanalysis. Notwithstanding, its key size is excessively little by current guidelines and its whole 56-digit key space can be looked in roughly 22 hours (Sharma and Kumar, 2013). The Cryptographic examination local area is in a persistent cycle of growing new ways of getting data and distributing assaults showing the shortcomings of existing calculations (Bozesan, Opritoiu and Vladutiu, 2013).

Some steganographic utilities utilize secret keys. In 1996, Pfitzmann analyzed that there are two sorts of keys, i.e., steganographic keys and cryptographic keys. A steganographic key controls the inserting and separating measure. For instance, it can disperse the message to be inserted over a

subset of all appropriate spots in the transporter medium.

Without the key, this subset is obscure, and each example used to distinguish implanting by a measurable assault is a combination of utilized and unused spots (i.e., of all likely places) which ruins the outcome. A cryptographic key is anyway used to scramble the message before it is implanted. For the two applications, the “secret”, which disguises the message, is segregated from the real calculation as a boundary the key.

Picture steganography is the study of concealing mystery messages within pictures. Consider it 21st-century vanishing ink. The easygoing spectator just sees a customary picture; just somebody who realizes what to look like for it will notice or discover the message.

1.INTRODUCTION

To control or conceal the presence of a message or information, cryptography and steganography are the two best procedures. Web clients regularly need to store, send, or get private data, which should be shielded from unapproved access and assaults.

Watermarking, cryptography, and steganography are the three primary strategies for data security right now being used. Watermarking disguises information to pass on data about the cover medium, like possession and copyright. By utilizing symmetric key cryptography and deviated key cryptography is used to encode the first message. While Steganography is gotten from the Greek words "steganos" and "graptos," which signify "covering" and "composing," separately. It is the specialty of inserting a secret message in a medium, typically an image, a sound document, or a video record, so that nobody aside from the sender and the proposed beneficiary knows about the secret message.

2. Proposed System

The proposed's plan will likely make a safer and strong strategy for data trade with the goal that secret and private information can be shielded from assaults and unapproved access. To accomplish the important vigor and security, The utilization of cryptography and steganography is consolidated. For steganography, a picture is utilized as a cover medium, and the RSA calculation is utilized for encryption.

In this proposed technique our high level LSB bit control strategy is utilized for implanting the message in the picture document and the message is itself encoded utilizing the current RSA encryption strategy. To begin with, both the content and the picture document should be inserted in the picture record. In the wake of changing over picture documents to paired reciprocals, the content is encoded with RSA. The encoded text is then inserted into the picture document utilizing our high level LSB calculation.

3.Cryptography

Cryptography, in like manner called cryptology is a word from Old Greek words: Kryptos (concealed mystery), Graphein (creating), and Logy (study) [1]. It depicts the methodologies of scrambling data from the outcast called sneak.That is, it is basically the encryption of information with the end goal that it is hard to make importance of it if not the planned recipient.It is the study of math that utilizations calculations like Hash Capacities, Public, or Private Keys to scramble and unscramble information. Cryptography is the workmanship and study of accomplishing security by encoding messages so that they are not, at this point clear. Cryptography can likewise give

validation to confirming the personality of a person or thing. Cryptanalysis is the figuring out of cryptography.

3.1Cryptography consists of two types:

3.1.1. Symmetric Key Cryptography :

A Same key is used for both encryption and unscrambling, at that point that is called as symmetric key cryptography and furthermore called as open key cryptography.

For example:-Information Encryption Standard (DES), AES, Triple DES.

3.1.2. Asymmetric Key Cryptography : IN this type both key are unique that is one key used for encryption and another key is for decoding, at that point that is called as lopsided key cryptography and furthermore called as private key cryptography..

E.g. RSA algorithm.

3.Hash Function :

A Hash function is any function that can be used to map data of arbitrary size to fixed size-values

The values returned by a hash function are called as a hash function

Hash codes,digests or simply hashes . The values are used to index a fixed size of a table is called as Hash Table

A few phrasings utilized in Cryptography are :-

Plaintext: - It is the original text message.

Encryption: - It is the process of encoding the contents oforiginal message so that attacker or any outsider does notunderstand the real message.

Decryption: - The process of retrieving backs the originalmessage.

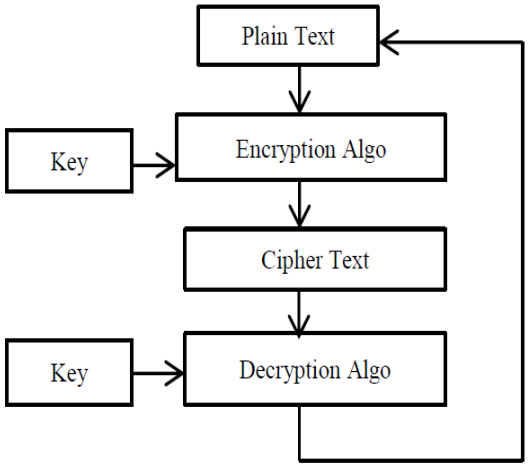

Fig .1 Basic Encryption and Decryption Process of Cryptograph

3.2RSA Algorithm

The estimation was given by three MIT's Rivest, Shamir and Adelman. The RSA estimation is a digressed cryptography computation; this infers that it uses a both key. As their names suggest, a public is shared uninhibitedly, while a private is hidden and ought not be granted to someone. The calculation [3]:

1. Produce any two unpredictable prime characteristics x and y so much that m= x*y is comparable to key piece length. For instance, x=5 and y=7 consequently, m = (7 * 5) = 35

2. Set m=x*y& (phi)=(x-1)(y-1). That is, (phi)= (7-1)* (5-1)== 24, and m=(5*7) = 35 .

3. Leave f alone and whole number with the end goal of 1<f<(phi) and f and m are co-prime. isf=7

```
int x = 61, int y = 53;
int n = x * y;
// n = 3233.

// compute the totient, phi
int phi = (x-1)*(y-1);
// phi = 3120.

int e = findCoprime(phi);
// find an 'e' which is > 1 and is a co-prime of phi.
// e = 17 satisfies the current values.

// Using the extended euclidean algorithm, find 'd' which satisf
ies
// this equation:
d = (1 mod (phi))/e;
// d = 2753 for the example values.

public_key = (e=17, n=3233);
private_key = (d=2753, n=3233);

// Given the plaintext P=123, the ciphertext C is :
C = (123^17) % 3233 = 855;
// To decrypt the cypher text C:
P = (855^2753) % 3233 = 123;
```

3.3AES Algorithm

The High level Encryption Standard - AES calculation (otherwise called the Rijndael calculation) [4] is an even square code calculation that converts plain content into ciphertext utilizing keys of 128,192, and 256 pieces. Since the AES calculation is viewed as secure, it has been received as a worldwide norm.

4. Steganography

Steganography derived from Greek word, Steganos, meaning of Steganosis "Covered" and graphiameans "Communicating" Accordingly, steganography is hiding creation. It is the method of hiding data in other carrier with the ultimate objective that its transmission isn't suspected [6].

Covering media can incorporate computerized pictures, sound, recordings, text documents, and other PC documents.

These mediums are called Transporter Articles or Cover Items.

In the wake of inserting a mysterious message into the cover-picture, a socalled stegano picture is acquired. Steganography's essential inserting and extraction model comprises of a Transporter Item, a Mysterious Message, an Installing Calculation, an Extraction Calculation, and a Stego key.

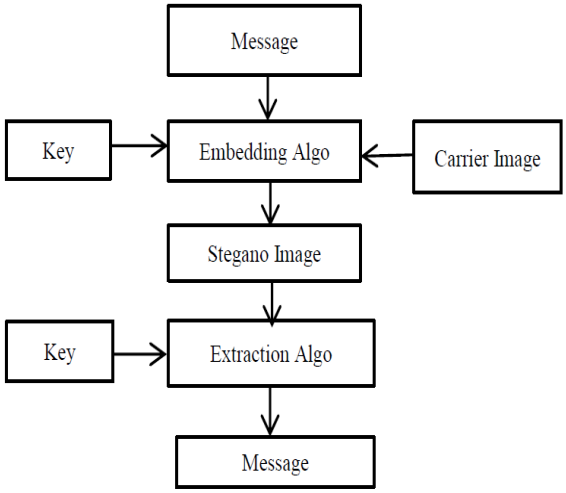

Fig 2:Basic Model of Steganography for Embedding andExtracting Message

4.1 Types ofsteganography :

There are 4 types of steganography according to their carrier type:

Text, Audio, Image and Video

4.2 LSB Technique

The most well-known and famous strategy for current steganography is to utilize LSB of picture Pixel data.

The procedure works perfect when the document is longer than the data record and if picture is grayscale.

While adding LSB procedure to single byte of a 24-bit picture can be encoded into each single pixel.

A touchof every 1 of the red, green, and blue segments can be utilized in a 24-digits shading picture, taking into account, sum of three pieces to be put away in every pixel.

(00100111 11101001 11001000)

00100111 11001000 11101001)

(11001000 00100111 11101001)

At the point the character A, which double worth equivalents 1000001, the accompaning matrix result:

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

For this situation, just three pieces should have been changed to effectively embed the character. Therefore, the progressions made to the most un-huge pieces are excessively little for the human visual framework (HVS) to perceive, and the message is successfully covered up.

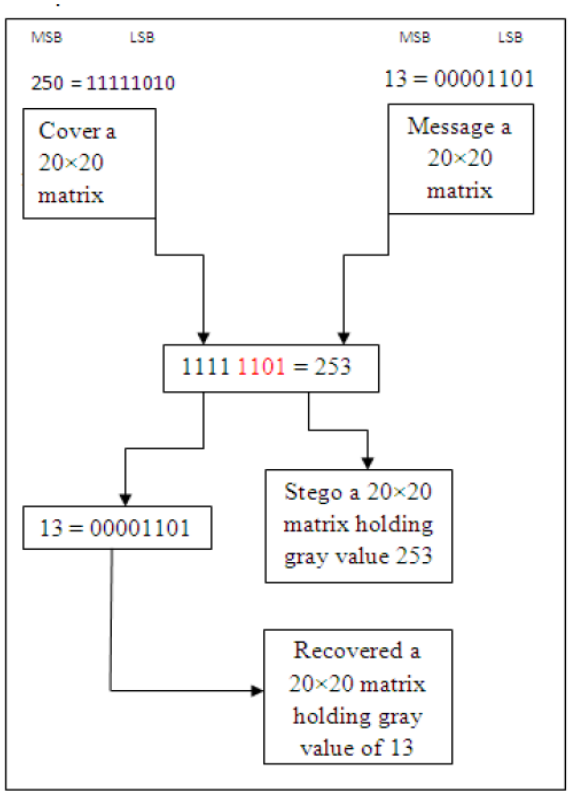

Fig 3: LSB Technique for Steganography

The figure 3 shows how assessment has acted to supplant the pieces of message with the cover. Cover contains a book of 250 qualities with 20x20 lattices and message with 13 qualities. 250 and 13 has been changed over into paired qualities and LSB of cover is utilized and supplanted with secret message. This Stegno record has been shipped off the collector side and recuperated that side again applying LSB to the record.

The figure 4 shows the LSB in picture design where restricted information is supplanted with the LSB pieces of three layers for example red, green and blue.

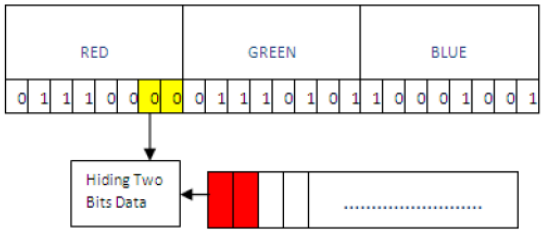

Fig 4 : LSB in RGB Image Format

5. Evaluation Parameters

We have carried out this task utilizing AES with LSB and AES with DWT calculations. To think about our outcomes, we have utilized assessment boundaries like MSE and PSNR. The assessment boundaries are given underneath

5.1 Mean Square Error (MSE)

It is a figure of legitimacy that demonstrates the level of closeness or contrasts between two pictures. Lesser the MSE worth of a picture better is the quality and less twisting from the first.

$$MSE=\frac{1}{M}\times\frac{1}{N}\sum_{i=0}^{M}\sum_{j=0}^{N}(x(i,j)-y(i,j))^2$$

Where:-
x- Original Image
y- Reconstructed Image
m-Total row
n-Total column

5.2 PSNR

PSNR is called as peak-signal-to-noise-ratio. It is the combination between the greatest conceivable force and debasing commotion that undermines the portrayal of the picture. Higher is worth, the better is the nature of the picture.

$$PSNR=10\log_{10}\frac{(2^n-1)^2}{MSE}.$$

6. Comparison between Cryptography and Steganography

Cryptography	Steganography
It alters the message.	It doesn't alter
Key is necessary	Key is optional
Used to encode the message.	Used to hide the message.
In this knownmessage ispassed.	In this unknown message is passed.
In Cryptography mostly text are used.	In Steganography media file like Text, audio, video.
Attack on Cipher text is called Cryptoanalysis.	Attack on Stego object is called Steganalysis.
Output are Cipher text	Output are Stegano File

7. COMBINATIONOF BOTHCRYPTOGRAPHYANDSTEGANO GRAPHY

Steganography could not be mistaken for cryptography, which involves changing a message over to conceal its setting from pernicious interceptors. The expression "breaking the machine" has an alternate significance in this sense. At the point when an assailant can peruse the secret message in cryptography, the framework is broken. To break a steganographic plot, the assailant should initially identify the utilization of steganography and afterward have the option to peruse the inserted message. Steganography, as per, is a technique for

covered up correspondence that can't be removed without significantly adjusting the information where it's installed. Besides, the assurance of a conventional steganography framework is subject to the privacy of the information encoding framework.

Cryptography encodes messages, which helps in their disguise. A messages content thus, when the substance has been scrambled, There is no real way to see the message. This ensures wellbeing, however The message was deciphered bye the interloper in the wake of figuring out the code .thus, as well as adding another layer of the security cryptography The most ideal decision is steganography.

Be that as it may, consolidating Cryptography and Steganography to add a few layers of safety is frequently a smart thought. Information encryption can be accomplished by a program and afterward the code text can be installed in a sound or some other medium utilizing the stego key. At the point when these two methodologies are joined, the information installed will be safer.

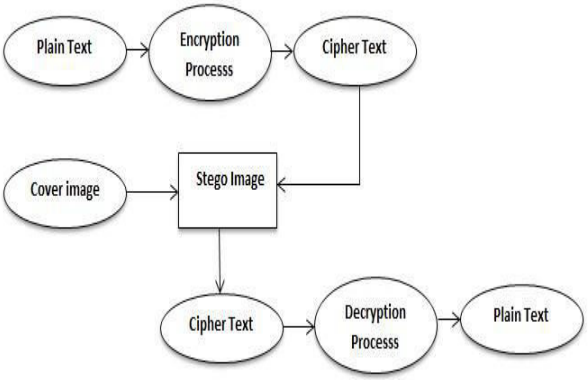

Fig 3:Combination of Cryptography and Steganography

Algorithm of the combination technique:-
1-Sender will provide the plain text and key

2- Then an algorithm is used for an encryption of the message.

3- Then this encrypted a message or a cipher text is embedded in an image with the help of some algorithm to produce a Stegano Image and the key is an option in this process.

4- Then the Stegano image is transmitted for communication.

5- At that point the recipient will play out the converse cycles. a recipient will initially separate the Cipher information structure a picture utilizing extraction calculation.

6- Then receiver will apply a decryption algorithm and will provide key to decrypt the cipher text.

7- The output will be the real plain text message.

8. CONCLUSION

We looked at cryptography and steganography, as well as their combination, in this article. Steganography and cryptography both provide security, but combining the two adds a layer of protection. We encrypt the message first, and then we insert it into the picture. For safe combination, this process improves protection, power, and robustness.

After a dubious assessment, it is difficult to verifiably says that stegano can be used as a substitute to a Cryptography. a crypto offers more secure organizations anyway it in like manner goes with not many issues. In any case, this doesn't structure persuading proof that Steganography will can't be used as opposed to Cryptography. Thusly blend of cryptography what's more, Steganography is used so all security justification existing are tended to

REFERENCE

[1] E. C. Bank, "Third Report on Card Fraud," ECB, Germany,2014.

[2] Vishnu S Babu and Prof. Helen K J,"A study on combined Cryptography and Steganography", *International Journal of Research Studies in Computer Science and Engineering*, Vol. 2, Issue 5, pp. 45-49, May 2015.

[3] B. Padmavathi and S. R. Kumari, "A Survey on PerformanceAnalysis of DES, AES and RSA Algorithm along with LSB
Substitution Technique,"International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Vol.2,Issue.4,pp. 170 - 174, 2013.

[4]. Secure Data Transmission using Steganography and Encryption Technique, Shamim Ahmed Laskar and Kattamanchi Hemachandran, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.

[5] A. Biryukov and D. Khovratovich, "Related-keyCryptanalysis of the Full AES-192 and AES-256," 04 122009. [Online]. Available: http://eprint.iacr.org/2009/317.pdf.
[Accessed 04 12 2015].

[6] R. Kefa, "Steganography-The Art of Hiding Data,"Information Technology Journal , vol. Vol.3, no. Issue.3, pp.245-269, 2004.

[7] Souvik Roya, P.Venkateswaran, "A Text based Steganography Technique with Indian Root" International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) ,pp. 167-171, 2013.

[8] T. Morkel , J.H.P. Eloff , M.S. Olivier, "AN OVERVIEW OF IMAGE STEGANOGRAPHY", Information and Computer Security Architecture (ICSA) Research Group

https://www.educative.io/edpresso/what-is-the-rsa-algorithm