Secure Transfer of Data with Increased Reliability and Security

Ashok T V
Students, Dept. of E&TE
Sri Siddhartha Institute of Technology
Tumakuru, India

Sumukh Bharadwaj S
Students, Dept. of E&TE
Sri Siddhartha Institute of Technology
Tumakuru, India

Chandana D
Students, Dept. of E&TE
Sri Siddhartha Institute of Technology
Tumakuru, India

Vinay
Students, Dept. of E&TE
Sri Siddhartha Institute of Technology
Tumakuru, India

Dr. K B Shivakumar
Students, Dept. of E&TE
Sri Siddhartha Institute of Technology
Tumakuru, India

Dr. Srinidhi G A
Students, Dept. of E&TE
Sri Siddhartha Institute of Technology
Tumakuru, India

***Abstract* - We live in the world of the Internet, the "Time of Information Technology" where a lot of private and secret data is being put away, handled and transmitted. Such data has gotten helpless to copyright encroachment, listening stealthily, and hacking, cracking and different sorts of unapproved get to. So, it is necessary to keep this information private. This has offered an ascend to the need of mystery correspondence. Thus, another space managing security of information has advanced and is known as "Information Hiding". Our framework utilizes the two information concealing strategies i.e., Cryptography and Steganography that permits the client to pack the Secret-Image.**

Keywords - Steganography ; Cryptography ; Information hiding

I. INTRODUCTION

Steganography and Cryptography are the two strategies used to stow away or secure mystery information. Nonetheless, they contrast in the regard that cryptography makes the information garbled, or conceals the significance of the information, while steganography shrouds the presence of the information. In our model we are clubbing these two advancements to accomplish secure information transmission with more noteworthy productivity.

Steganography is derived from a Greek word meaning ‘disguised composition’. The word steganos means secured and graphical method of writing. Steganography has the capacity of concealing the data and also it will conceal the principle behind the communication of secret data.

It hides the secret data in another document such that only the targeted receiver knows the existence of the secret data. In olden times, the secret data was communicated by concealing it on the rear of wax,stomach of hares etc.

Cryptography is the method of securing data and communications using codes so that only those people for whom the information is intended can understand the secret message.

II. LITERATURE SURVEY

G. Suman And P.Anuradha ,“RSA Algorithm And Least Significant Bit SteganographY’’,International of journal engineering research and technology (ijert), vol. 2 issue 10, october - 2013. In this paper a novel method for encoding a message was proposed for organizing security applications. Both the RSA calculation and LSB steganography technique were utilized for messages to give higher security. This calculation was created utilizing framework C coding and actualized on FPGA. FPGA will give the measured engineering to advancement of an ASIC IC.

Anil Kumar and Rohini Shrama, “A Secure Image Steganography Based On Rsa Algorithm and Hash – Least Significant Bit Technique”, International Journal Of Advanced Research In Computer Science And Software Engineering, VOL. 3, ISSUE 7, 2013.

Anil Kumar proposed another picture-based steganography strategies for mystery information communication. Hash – least significant bit information concealing technique is used in planning the model of this paper. To expand the security level, the cryptographic information encrypting process is alluded. Before information covering up, the model encodes the mystery content information utilizing RSA algorithm with a mystery key. During information concealing an. alteration picture is utilized as a spread article. The spread picture is divided into Red, Green, Blue planes and the content data will be changed over into a parallel piece stream. Three - bit of content data is covered up into Least Significant Bit of Red and Green shading arrangement of the spread picture though another two – bit data is put away in Blue shading segment. Presentation of the model is contrasted and the straightforward Least Significant Bit information concealing methods, result is estimated as far as PSNR and MSE of stego picture.

Salesh Saraireh, “A secure data communication system using cryptography and steganography”, international journal of computer networks and communication (ijcnc), vol. 5, issue 3,2013.

Saleh Saraireh proposed a protected information correspondence model planned by the usage of Cryptography and Steganography information concealing techniques. Channel bank figure calculation is used in order to scrabble the mystery instant data. For spread picture encryption, changes in discrete wavelet are taken into consideration in steganography. Instant messages are changed over into parallel piece streams. Changed over paired data is covered up in the wavelet coefficient of spread picture. HISTOGRAM and PSNR estimation of the Stego picture is used in order to dissect the exhibition of the allied structure. It is presumed that the structured model with channel bank figure calculation and Discrete Wavelet Transform work builds the general information Security over the opened channel and upgrades the framework efficiency.

Shailesh Nana Kumavat, Pavan Patil, Ashwini Yeole And Yogesh Patil, “Highly Secure Steganography Using Crossover Algorithm And Unbreakable Cryptosystem”, International Journal Of Scientific Engineering And Technology Research, Vol. 4, issue 8, pp. 1499 – 1501, 2015. Shailesh Nana Kumavat has proposed an irregular secret phrase based cryptographic procedure. Then Model is partitioned into 2 modules for example in the principal module discharge information encryption utilizing secret key or secret word. In Steganography the content data is covered up into spread picture LSB procedures. Further Crossover calculation is conducted to change over stego image. The Crossover calculation mixes the segment and line pixel data. The model is planned by utilizing java devices.

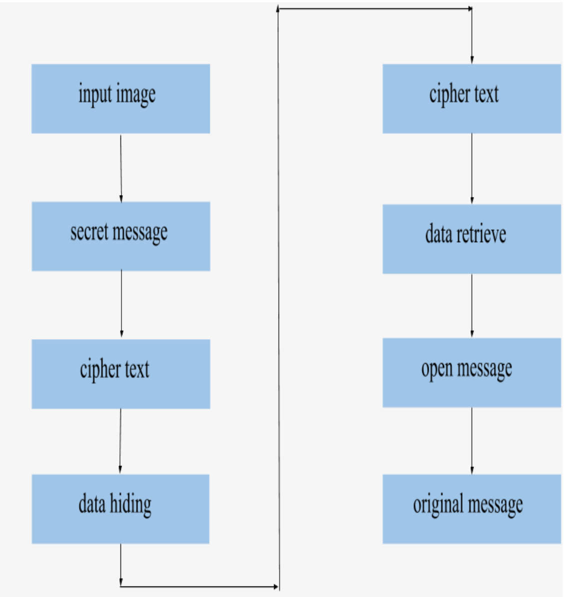
Ya– Lin Lee and Wen – Hsiang, “A New Secure Image Transmission Technique Via Secret – Fragment – Visible Mosaic Images By Nearly Reversible Color Transformation”, Ieee Transactions On Circuits And Systems For Video Technology, vol. 24, issue 4, 2014.Ya LIN LEE proposed a steganographic technique based on picture. In this model a delicate picture is covered up by utilizing the spread item. The information picture is changed over to a mosaic Picture with a similar size. The presentation of the alluded model is dissected by a measurement of the mean auxiliary closeness (MSSIM), root mean square blunder and the transmission bitrate with picture square.

III. PROPOSED METHODOLOGY

In the proposed framework, RSA ALGORITHM and LSB ALGORITHM are utilized. The Project targets diminishing the evil impact of pictures with the goal that the security and unwavering quality of the proposed strategy would be expanded.

This proposed model has mainly two different parts. They are: -

1. **Secured Transmission of Data**
2. **Secured Extraction of Data**



In this proposed system, we used RSA ALGORITHM and LSB ALGORITHM.

A. RSA ALGORITHM: -

RSA Algorithm is one of the asymmetric cryptography algorithms. Asymmetric actually implies that it chips away at 2 unique Keys. For example, open key and private key. The public Key is given to everybody and the private key is kept hidden. RSA is a calculation which is utilized to give the encryption and verification framework.

Ron Rivests, Adi Shamir, and Leonard Adelman introduced the RSA algorithm in 1977. This algorithm is most commonly and normally used for encryption and check counts. The RSA count is a chief open key cryptosystem, and it is commonly used for the secured data transmission. In such a Cryptosystem, the Encryption key is an open one and the unscrambling key fluctuates which lets sleeping dogs lie. In RSA, this asymmetry relies upon the after effect of two colossal prime numbers, thinking about the issue. The RSA scramble key encodes the image, with the objective that it changes over into a ciphertext course of action and it will be taken care of as a substance record. The opposite system for encryption, the opposite methodology is figured by another interpreting key of RSA estimation and it unscrambles the image from the figure content. Finally, it will locate the resultant picture by the unscrambling techniques.

The steps of RSA algorithm are shown below: -
step 1: we have to select any two different large random Prime Numbers p and q.
step 2: calculate n= pq. where n is modulus for Public key and Private key.
step 3: calculate Ø(n)= (p-1) (q-1).
step 4: choose an e such that 1<e<Ø(n). and e is co-prime to Ø(n) share no factor other than 1;
gcd(e , Ø(n))=1. e is released as a public key exponent.
step 5: compute d to satisfy the de(mod Ø(n)) =1 i.e. m=e’^d mod(n). d will be kept as a private key exponent.

RSA algorithm is utilized in cutting edge PC condition to encode and unscramble the information in change. The RSA algorithm is likewise called an unbalanced cryptographic calculation. Awry cryptosystem implies two distinct keys are utilized in the encryption and unscrambling.

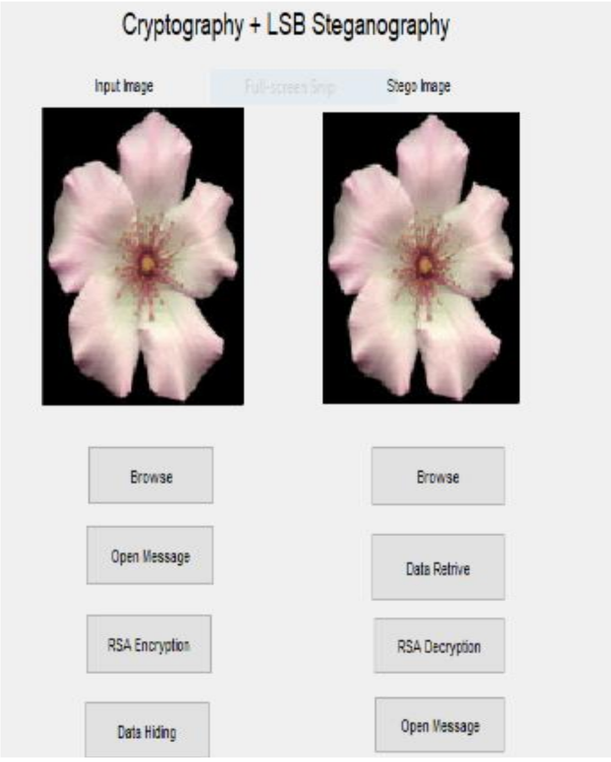
In the two keys, one key will be used for encryption and the subsequent key will be used for decoding. This RSA algorithm is also called Open Key Cryptography. Since one of the Secret Keys can be given to everybody which implies open, the other key must be kept hidden.

2.LSB ALGORITHM: -The LSB is most commonly used data hiding methods. LSB pixel of the cover image will be replaced by the secret data.

1 0 0 1 1 1 1 0	1 0 0 1 1 1 0 1

Before applying LSB operation and After applying LSB operation.

IV. RESULTS



The Stego image contains secret data that we sent through the input carrier image.
Mathematical values: -
PSNR value of the image is 68.0302
MSE value of the image is 0.0103

V. CONCLUSION

The proposed algorithm is best appropriate for content-based steganography, where the secret information in content configuration can be covered up in any spread picture of any goals and organization.

Obtained PSNR values are promising to the point that we can have a mystery correspondence between the two imparting substances.

The general framework is executed utilizing the MATLAB apparatus wherein execution is estimated as far as nature of secret picture and MSE.

REFERENCES

[1] G. Suman and P. Anuradha “RSA Algorithm and LSB Steganography”, International of Journal Engineering Research & Technology (IJERT), vol. 2, no. 10, 2013.

[2] A. Kumar and R. Sharma, “A Secure Image Steganography Based on RSA Algorithm and Hash – sLSB Technique”, International Journal of Advanced Research in Computer Science and software Engineering, vol. 3, no. 7, 2013.

[3] N. Shailesh, P. Patil, A. Yeole and Y. Patil, “Highly Secure Steganography Using Crossover Algorithm and Unbreakable Cryptosystem”, International Journal of Scientific Engineering and Technology Research, vol. 4, no. 8, pp. 1499 – 1501, 2015.

[4] Salesh Saraireh, “A Secure Data Communication System Using Cryptography and Steganography”, International Journal of Computer Networks and Communication (IJCNC), vol. 5, no. 3, 2013

[5] L. Ya – Lin and W. Hsiang, “A New Secure Image Transmission Technique via Secret – Fragment – Visible Mosaic Images by Nearly Reversible Color Transformation”, IEEE Transactions on Circuits and Systems for Video Technology, vol.24, no. 4, 2014.