International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

A Survey on Secured Data Transmission Using RSA Algorithm and Steganography

Rajat Asreddy[1], Avinash Shingade[2], Niraj Vyavhare[3], Arjun Rokde[4], Yogesh Mali[5]

[1,2,3,4] Student, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegoan, Savitribai Phule Pune University, Pune, Maharashtra, India

[5] Assistant Professor, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering, Lohegoan, Savitribai Phule Pune University, Pune, Maharashtra, India

ABSTRACT

Conceptual In the cutting edge world, there is a need of high security of media information. This verified framework ought to give classification, genuineness, respectability and non-disavowal in the system. The private subtleties moved through web are hacked by phishing in an electronic correspondence world. So data security plays a significant job. The Cryptographic calculations are applied over numerous applications for secure transmission of information against dangerous assaults. Steganography is utilized to conceal their reality. Rivest-Shamir-Adleman (RSA) is an awry cryptographic, profoundly verified calculation. Since it is mind boggling to process, extraordinary strategies are applied to build the speed of a RSA calculation. This paper proposed a strategy to upgrade the security of correspondence by consolidating cryptography and steganography strategies. The proposed framework is progressively productive in verifying information from unapproved clients.

Keywords : Cryptography, RSA, Encryption, Unscrambling, Steganography.

I. INTRODUCTION

An expanded interest for exchange of data and internet providers needs security from the interlopers. In this manner, mystery of information move in correspondence media in nearness of programmer, for example, cryptography and steganography are utilized. Cryptography clutters a message to be transmitted with the goal that it can't be perused and get it. Steganography is procedure of correspondence that covers up the nearness of emit message in another message[1]. The two significant advances are beginning one is covering data from unapproved gatherings and second is making information incomprehensible to individuals separated from assumed recipient. Cryptographic calculations are recognized as symmetric and hilter kilter calculations. In symmetric calculations, a solitary key is applied by sender and recipient during conveying called as mystery key. These calculations are otherwise called discharge key and single-key encryption. This procedure have less computational expense. Likewise experience issues while keys being traded, non-renouncement and confirmation. In unbalanced calculations, two separate keys are applied. One is open key used to encode messages. Another is private key used to decode got messages. Here open key is known by both sender and recceiver, where as private key is kept emit. Numerous lopsided calculations are being utilized to slove numerical entanglements to get them in an irreversible state. Figuring Challenge: The huge numbers are utilized in creating RSA keys. The RSA Factoring challenge is the one confronting trouble while figuring these huge numbers. Two huge prime numbers are consolidated to get each number. Modulus of a key pair is additionally created in comparable manner[6]. Figuring of a number is the one getting it as the result of prime numbers. Time to register figuring increments if the size of the number increments. Another test is mystery key test where the key should be exchaged utilizing better encryption calculation safely among sender and proposed receipient without being known to outsider. The basic objective of steganography is to oppose fascination with respect to transmission of covered information.

II. LITERATURE SURVEY

A picture steganography utilizing a Hash-LSB (H-LSB) encoding and unraveling, RSA encryption and decoding what's more, Blowfish calculation is proposed [1]. RSA is utilized to encode the mystery data and after that it is covered up into the spread picture document utilizing Discrete Cosine Transform (DCT) and Hash-LSB method. Reviews different enhancements for RSA calculation by applying alterations so as to improve it [2]. Improved RSA is proposed in [3] where the estimations of x, y and n are known to both sender and recipient, the estimation of d is known as it were to collector. The strategy to upgrade the security of RSA plan disposes of the excess messages which happened in certain estimations of n or in the result of two prime numbers [4]. LSB Replacement system which is a procedure of altering the least noteworthy piece pixels of the spread picture [5]. RSA was picked as an encryption system due to its encryption and decoding speed, and furthermore its base stockpiling necessity for the figure content. An audit around two methods of picture steganography are proposed in 0 produced. Fig.1

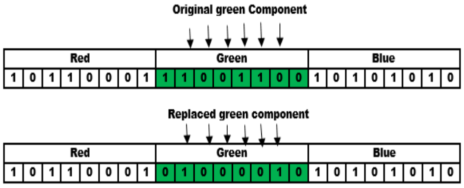

Fig 1.

Green Pixel Replacement Continuing of 2018 IEEE International Conference on Current Trends toward Converging Technologies, Coimbatore, India

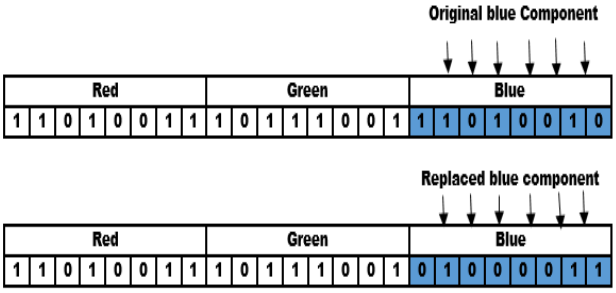

Fig 2.

III. EXISTING SYSTEM

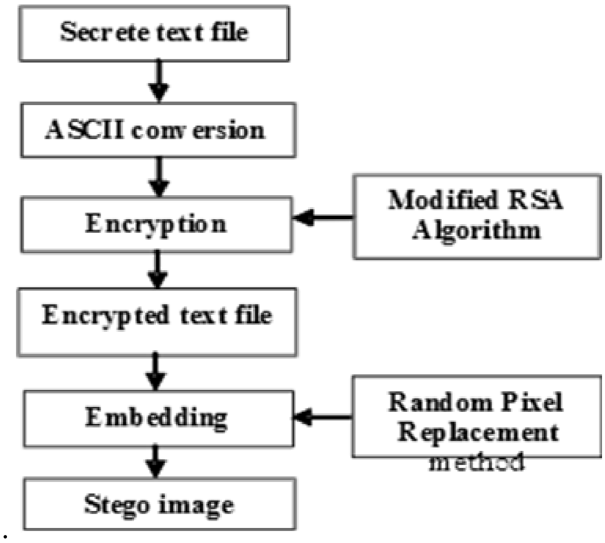

Fig 3. Encoding Process

This stego picture is transmitted in the system to arrive at the goal. The stream chart for disentangling is delineated in Fig.7. Stego picture is gotten at the goal. The initial step is to get the mixed encoded information from the stego picture. This is finished by extraction strategy. The encoded information will be gotten by separating every estimation of pixels based on the arbitrary number produced utilizing pixel substitution strategy. The acquired information must be decoded utilizing the private key from altered RSA calculation. The first mystery content document will be acquired subsequent to decoding the scrambled information.

IV. PROPOSED SYSTEM

In this proposed framework, an altered RSA calculation is actualized to expand security for the mystery message. Without utilizing the key it is difficult to remove the mystery data. An arbitrary pixel substitution method is utilized for inserting. The mix of encryption and inserting in our method gives a two-layer security in the web. Execution examination is assessed by contrasting RSA calculation [14] and altered RSA, which has given a superior MSE and PSNR values for the diverse test pictures. Time taken for encryption and decoding is additionally assessed

Time taken for encryption and decoding is additionally assessed. The future work can be reached out for other information documents like sound, video and furthermore for other picture arrangements and pictures of other size. Some assault investigation can likewise applied for the proposed technique.

System Flow

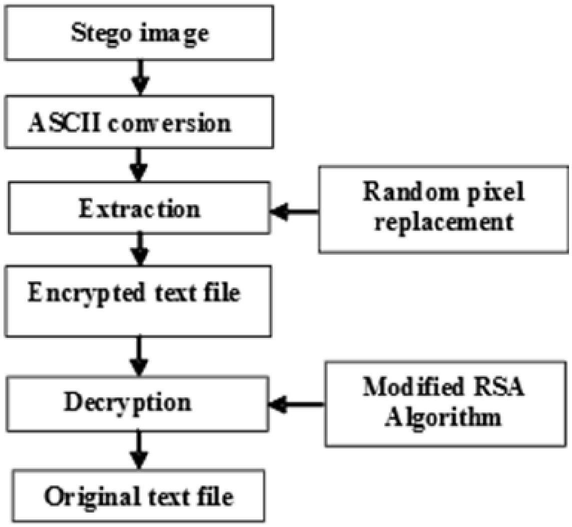

Fig 3. Decoding Process

ALGORITHM

Step 1: Receive a stego image.

Step 2: Find 4 LSB bits of each RGB pixels from stego image.

Step 3: Apply hash function to get the position of LSB's with hidden data.

Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.

V. CONCLUSION

In this proposed framework, an altered RSA calculation is actualized to expand security for the mystery message. Without utilizing the key it is difficult to remove the mystery data. An arbitrary pixel substitution method is utilized for inserting. The mix of encryption and inserting in our method gives a two-layer security in the web. Execution examination is assessed by contrasting RSA calculation [14] and altered RSA, which has given a superior MSE and PSNR values for the diverse test pictures. Time taken for encryption and decoding is additionally assessed. The future work can be reached out for other information documents like sound, video and furthermore for other picture arrangements and pictures of other size. Some assault investigation can likewise applied for the proposed technique.

VI. FUTURE SCOPE

We have compared and analysed existing cryptographic algorithm like DES, AES and RSA along with the same LSB technique for hiding the document in an image file. Our future work will focus on SLSB which replace LSB technique.

VII. REFERENCES

[1]. M.Rajkamal and B.S.E. Zoraida, "Picture and Text Concealing utilizing RSA and Blowfish Algorithms with Hash- LSB Technique",

International Journal of Innovative Science, Engineering and Technology, Vol. 1 Issue 6,August 2014.

[2]. Sarthak R Patel, Prof. Khushbu Shah, and Gaurav R Patel, "Concentrate on Improvements in RSA Algorithm", Worldwide Journal of Engineering Development and Research, 2014.

[3]. Israt Jahan, Mohammad Asif, Liton Jude Rozario, "Improved RSA cryptosystem dependent on the investigation of number hypothesis and open key cryptosystems", American Diary of Engineering Research (AJER), Vol 4, Issue 1, 2015.

[4]. Amare Anagaw Ayele and Dr. Vuda Sreenivasarao, "A Altered RSA Encryption Technique Based on Multiple open keys", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2013.

[5]. Dr. Abdulameer K. Hussain, "A Modified RSA Calculation for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Calculation", International Journal of Innovative Science, Designing and Technology (IJISET), Vol. 2, Issue 1, January 2015.

[6]. E.P. Musa and S. Philip, "Mystery Communication Using Picture Steganography", African Journal of Computing and ICT, Vol. 8, September, 2015.

Cite this article as :

Rajat Asreddy, Avinash Shingade, Niraj Vyavhare, Arjun Rokde, Yogesh Mali, "A Survey on Secured Data Transmission Using RSA Algorithm and Steganography", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 8, pp. 159-162, September-October 2019.

Journal URL : http://ijsrcseit.com/CSEIT194836