International Journal of Applied Engineering and Technology ISSN: 2277-212X (Online)
Online International Journal Available at http://www.cibtech.org/jet.htm
2020 Vol. 9, pp.141-148/Suganya
***Research Article** (Open Access)*

SECURE FILE STORAGE PLATFORM USING HYBRID CRYPTOGRAPHY AND STEGANOGRAPHY

P. Suganya[1] AP
Department of Computer Science Engineering
St. Joseph's College of Engineering and Technology

ABSTRACT
The proposed software product is liable to meet the required security needs of data center of cloud. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. The idea of splitting and merging adds on to meet the principle of data security. The hybrid approach when deployed in cloud environment makes the remote server more secure and thus, helps the cloud providers to fetch more trust of their users. For data security hybrid algorithm is used. cryptography and stenography is combined to strong encryption. For cryptography triple DES and RSA algorithm is used and for stenography Blind hide, Battle steg technique is used to encryption and decryption. Cryptography technique translates original data into unreadable form. Stenography translates encrypted data into image format. So that Data could not be threatened and So only authorized person can access data from cloud server.

***Keywords*:** *Network Security, Data Transmission, Cryptographic Security, Data Exchange, Hybrid Cryptography, RSA, Triple DES Steganography, Blind hide, Battle steg.*

INTRODUCTION
The art of preserving information by transforming it (encrypting it) into an unreadable format (for human eyes), called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code-breaking, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important [1]. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is Pretty Good Privacy because it's effective and free. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient. public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses [2].There are a number of applications available now in these days by which the private and sensitive data is transmitted using untrusted network. Basically most of the time user sends the data from a trusted network to a trusted network. But between source and target host the network remains unsecure. Therefore, Most of the applications are consumes the cryptographic techniques for providing the security and confidentiality in data [3]. In this presented work the main aim is to find the efficient and optimum solution for color image cryptography [4]. Efficiency concerned with the minimizing the computational resources in terms of memory consumption and execution time and the solution optimization is leads to modifying the cryptographic technology using hybrid approach with their integrity check. Thus the desired cryptographic system required to work in less time and less memory consumption. In order to develop such approach simple mathematical techniques and lightweight cryptographic standards are required to employ with the system.
The proposed work is intended to provide an efficient and a complex cipher generation technique using the hybridization of different techniques. For successfully achieve the desired goal following tasks are included in the study. In proposed system we combine Cryptography and Steganography.

STUDY OF DIFFERENT IMAGE AND VISUAL CRYPTOGRAPHIC SCHEME

In this phase of study various cryptographic approaches are explored in order to find the appropriate solution.

DESIGN AND IMPLEMENTATION OF THE NEW ENHANCED ALGORITHM:

From the previous studies a new cryptographic technique is recovered and the enhancement on the existing technique is proposed. The proposed technique is further implemented using the suitable programming language in this module.

PERFORMANCE ANALYSIS

In this phase the performance of the system is evaluated and the comparative study among traditional algorithm and presented improved technique is performed for finding the computational and storage complexity.

LITERATURE AND SURVEY

In the current years, there is an explosion in the amount of information being exchanged over Network; therefore it becomes very essential to provide proper security measures. In order to provide a secure environment to send data over network, a proper analysis of present security mechanism needs to be done. Recently one of the existing system uses compression based mechanism along with RSA algorithm for light weighted devices such as mobile phones and pda's [10]. This system provides a secure way to send message over the network [8]. This system uses compresses technique to reduce the length of message, then encrypt it by using RSA algorithm and Triple DES algorithm and Triple DES(Data Encryption Algorithm) is a symmetric-key block cipher ,which applies the DES Algorithm three times to each data block . RSA algorithm is an asymmetric algorithm which uses Public Key Encryption method. One of limitation of using asymmetric cryptography is time and space complexity. One another method uses compression based cryptography to transmit medical related information. It uses 26 compression methods like Sequitur for reducing the size of data being sent. The combination of McEliece public-key cryptosystem with compression provides confidentiality in the transmission [9].This system has a drawback as its efficiency drops with increase in data. The proposed system uses symmetric key cryptography hence it is faster than asymmetric key cryptography and uses compression technique to reduce the size of cipher text.

PROPOSED SYSTEM

The information technology is growing frequently using the internet and communication technologies. The network is secured using various techniques such as the firewall and other anti-virus techniques. But among the two private networks the data is traverse through the public network and the public network is not much secure due to the different kinds of attacks and their security issues. Therefore the cryptographic and steganographic techniques are utilized for improving the security of data during their transmission in the public networks.

On the other hand the different traditional cryptographic and steganographic solution for network data transmission is well known and different techniques that are breakable by hackers. Thus new kinds of techniques for improving the network data security is required to investigated and developed. In this presented work a hybrid technique is developed using two different cryptographic and steganographic approaches. These techniques are modified for improving the key generation and integrity checks by which the security is assured at both the end of network.

The proposed techniques are able to secure the data when the data is transmitted on the public and unauthorized data networks. And during different kinds of outsider attacks are identified is data altered during transmission or not. Thus the presented technique is an effective and essential for the network data security where the two users are communicating in unknown networks.

The proposed working hybrid model for data cryptography and steganography is given using figure 1 and 2. In the figures the encryption process of the system is described and reports the decryption process of the

system. During the encryption process user need to encrypt the file using the hybrid cryptographic model, thus a input file is first produced to the system. The input file is first processed using 3DES algorithm, the 3DES algorithm generates the 168 bit code for the input data.

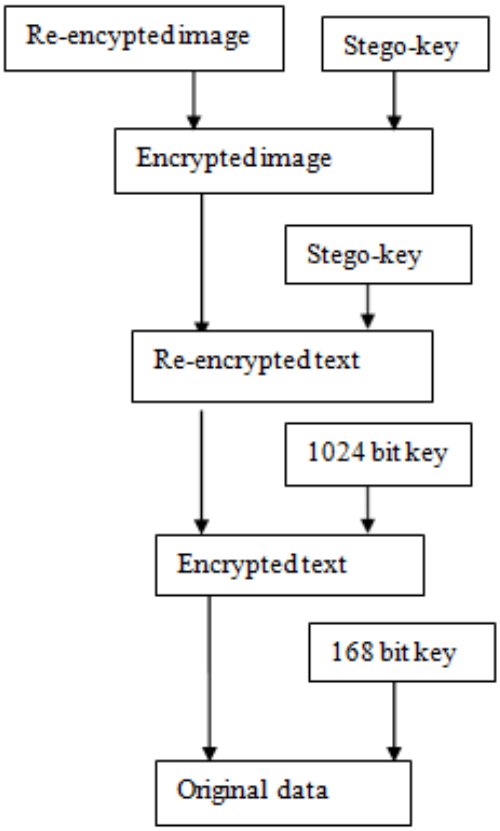


Figure 1

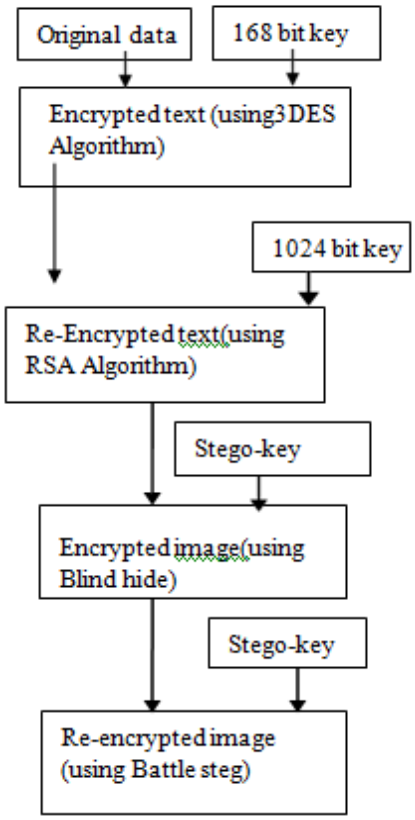


Figure 2: Decryption process

Over the produced 168 bit key the bit discarding process is taken place, in this process the 168 bit code is converted into 16 blocks of the 8 bit data For securing the key more the DES algorithm [7] is used to encrypt the key which generates the cipher 1 which the encrypted key for decryption process. This process generates the cipher 2.In further steps cipher text1 and cipher text 2 is combined. The blind hide algorithm generates stego-key is used to encrypt image 1, which is further encrypted using Battle steg which generates 198 byte stego-key. This process generates image 2. In further steps the image 1 and image 2 is combined and ready to prepare the text for transmission.

The transmitted text to the network is received by the end user, this text is termed here as the received text. In first process the received text is divided into two different ciphers, cipher 1 which is outcome of key data and seconds the cipher 2 that contains the encrypted data for security. The cipher 1 is treated first to generate the key for data recovery, therefore first the cipher text 1 is produced to DES algorithm for the recovering the original key by which the data is recovered. After recovering key using decipher of cipher text 1 the key is produced to RSA algorithm with the cipher text 2.

The RSA algorithm decipher the original text and can be used with the other application but for authenticating the recovered data on receiver end the integrity check is applied for the data. Therefore first the recovered data is processed through the 3DES key and 168 bit obtained from the data. In further the comparer is implemented, the comparer has two functionalities first using the 3DES 168 bit, regenerate the original key by which the encryption performed. Thus the same operation is performed over the 168 bit to generate key and second the comparison among generated key and the obtained key from network. In

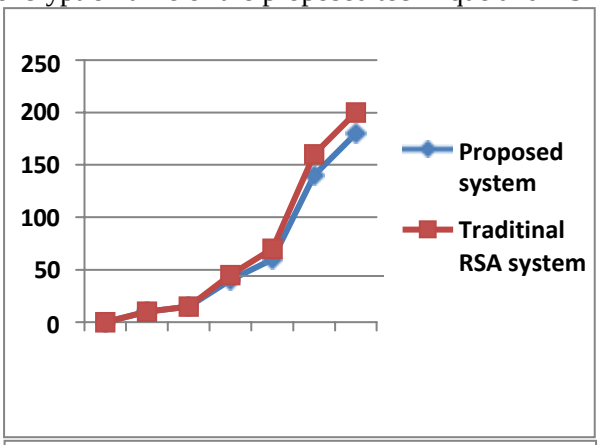
further is both the keys are found similar the data is accepted by the system else the data can be rejected.In steganography image 2 is decrypted using battle steg stego-key and the image 1 is decrypted using blind hide stego-key.

RESULTS AND ANALYSIS

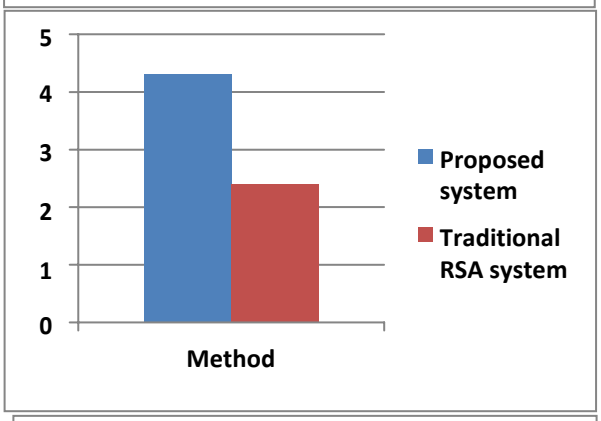
The experimental evaluation and performance is computed and compared with RSA algorithm as described in table. The comparison is performed with the help of some performance factors. This section provides discussion about the obtained results.

Encryption Time

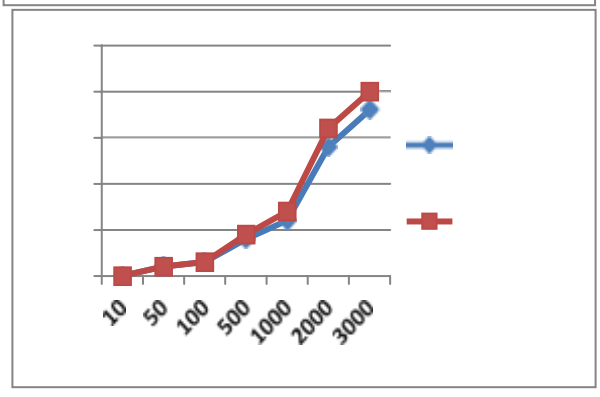
The time required to encrypt data is termed as encryption time of the cryptographic system. The encryption time of the proposed technique and RSA algorithm is given using figure 3 and table 3.

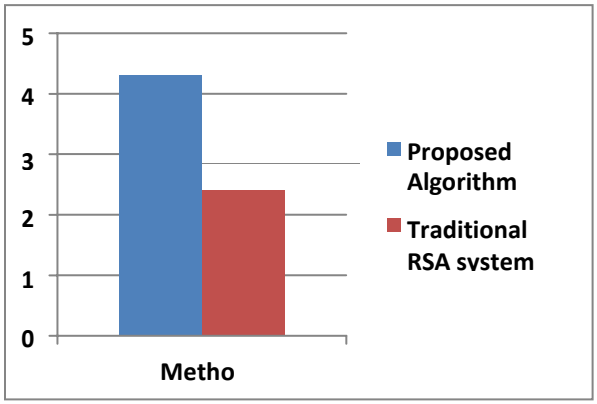


File size	Proposed system	Traditional RSA system
10	0.93	1.47
50	2.47	4.38
100	7.29	10.37
500	31.42	36.53
1000	59.32	67.37
2000	122.39	154.63
3000	158.35	188.54



File Size	Proposed Algorithm	Traditional RSA System
10	0.673	0.947
50	2.92	3.98
100	5.89	7.16
500	21.46	27.81
1000	39.87	47.88
2000	74.56	92.53
3000	125.94	147.22





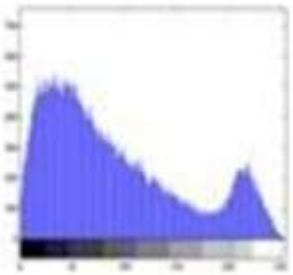
The diagram contains data of different file size in X axis by which experiments are conducted. Similarly Y

axis contains amount of time in milliseconds. The blue line shows the performance of proposed technique and RSA algorithm is denoted by red line. The results show proposed algorithmconsumes less time as compared to RSA algorithm. The amount of time depends on data. To approximate comparative performance figure 4 provides mean performance of algorithms. According to mean performance proposed technique consumes less amount of time with respect to RSA algorithm. DECRYPTION TIME
The time to recover original data from cipher is known as decryption time. Figure 5 shows comparative performance of RSA and proposed algorithm. In this figure X-axis contains file of different size for experiments and Y axis contains time required. The decryption time of the proposed algorithm is efficient as compared to RSA algorithm.
The memory consumption of proposed and RSA algorithm is demonstrated in figure 7. To show advantage of proposed algorithm over RSA algorithm mean space complexity is computed and given using figure 8. The diagram includes memory consumption in kilobytes in Y axis and methods are given in X axis. The performance of proposed technique is efficient as compared to RSA algorithm.

3. STEGANOGRAPY APPROACHES

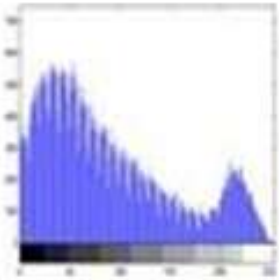
The steganography approaches can be divided into three types [11]:
*1) Pure Steganography:*it is a technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.
2) Secret Key Steganography: it uses the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message by secret key technique and then hide the encrypted data within cover carrier.
3) Public Key Steganography; it is the combination of the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier. The
Difference between Cryptography and Steganography [8, 11]:
Cryptography prevents unauthorized party from discovering the content of communication but Steganography prevents discovery of the existence of communication (i.e., Cryptography makes data gibberish and known the message passing while Steganography tends to conceal presence of hidden data and unknown the message passing).
Cryptography alters the structure of secret message while Steganography does not alter the structure of secret message.
Cryptography is more common technology than Steganography technology. The most algorithms of Cryptography are well known, but the algorithms of Steganography are still being developed by certain formats. In Cryptography, the strong algorithm depends on the key size, the more key size; the more expensive computing power is required to decrypt ciphertext. In Steganography, once the hidden message is detected, the message is become known.
Cryptography can provide all security objectives by implementing the public and private key(s) with hash functions or authentication codes or digital signatures. Steganography cannot provide most of security objectives (Integrity, authenticity, non-repudiation) by itself without using the cryptographic techniques. However it provides confidentiality by itself because mostly, the concerning person knows that the message is hidden in what kind of medium [12].
In this paper, the secret Key steganography approach is used to improve security by using modified AES and method in [1] which includes PVD_MPK and MSLDIP-MPK methods to encrypt and hide the message in cover image. Therefore, if an attacker doubts about the stego image and tries to detect the message from the stego image, he would still require the key to decrypt the encrypted message.
The rest of this paper is organized as follows; related work will be discussed in section 2 and the proposed method will be presented in section 3. Then experimental results of the proposed method will be given in section 4. Finally, section 5 concludes the paper and future work.

a. Cover Image "Baboon"



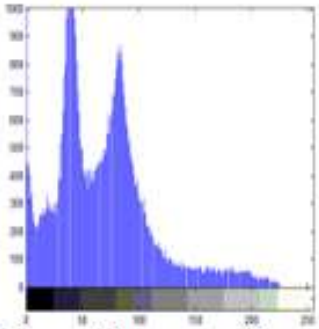
b. Cover istogram"Baboon

c. Stego Image "Baboon"



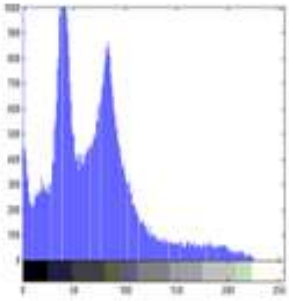
d. Stego Histogram "Baboon"

e. Cover Image "Pepper"



f. Cover Histogram "Pepper"

g. Stego Image "Pepper"



h. Stego Image "Pepper"

Fig. 4. Three cover images and output stego-images used in system simulation with their corresponding histogram

In table I, a comparison between the proposed merg[e1d] method and method in [21] has been made by hiding (18.616, 13.003, and 16.394) secret bytes in 256 x256 cover images (Baboon, Lena, and Peppers) respectively. The results indicate that, the proposed method has higher PSNR values than method in [21], and also the PSNR values are much greater than 36 dB. This proves the suitability of the proposed method. In figure 4, a comparison between the resulting stego images and their histograms with cover images and their histograms has been made. We can see that there is no significant change in stego histograms and visual quality of the resulting stego-image of the three images. Also, the change in histograms is influenced by the properties of image (i.e. the smooth area and edge area), so the larger number of edge areas in the original image, the more change in histogram of stego- image such as Baboon and Lena contrast to Pepper image. This is because the method that is used in hiding in smooth areas is MPK_PVD method.

CONCLUSIONS

In this paper, a new secure communication model has been presented that combines cryptography and steganography techniques to provide two layer of security, so the steganalyst can't reach to plaintext without knowing the secret key to decrypt the ciphertext. Firstly the secret data has been encrypted by using the AES_MPK then the encrypted data has been hidden in gray image by using PVD-MPK and MSLDIP-MPK methods. Due to this combination, the secret data can transmit over open channel because the cipher text does not look meaningless but its presence is concealed by using steganography for hiding cipher text in the images. Experimental results showed that our proposed model can be used to hide much more information than that other existed methods and the visual quality of the stego image is also improved, in addition to it is effective for secret data communication. In the future work, we are looking forward to try applying the proposed method on audio and video. Also, we are looking forward to enhance the proposed method to make the capacity higher than it while keeping the same PSNR or higher.

REFERENCES

1. M.E. Saleh, A. A. Aly, and F. A. Omara"Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad(MPK) Coding, " International Journal of Computer Science and Security (IJCSS), Volume (9), Issue (2), pp. 397 - 397, 2015.
2. FA. P. Petitcolas et al, "Information Hiding-A Survey," Proceedings of the IEEE, special issue on protection of multimedia content, Vol. 87, Issue. 7 PP. 1062-1078, July 1999.
3. K. R. Babu et al, "A Survey on Cryptography and Steganography Methods for Information Security," International Journal of Computer Applications (0975– 8887), Vol. 12, No.2, PP. 13-17, November 2010.
4. R. Oppliger, "SSL and TLS: Theory and Practice," ARTECH HOUSE, 2014.
5. B. Schneier, "Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)," pp. 1–1027, January 1996.
6. K. Nitin K and N. Ashish V, "Comparison of Various Images Steganography Techniques," International Journal of Computer Science and Management Research, Vol 2, Issue 1, PP. 1213 – 1217, January 2013.
7. S. Sharda and S. Budhiraja, "Image Steganography: A Review," International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol.4, Issue 1, PP. 707– 710, January 2013.
8. J. Raphael, and V. Sundaram, "Cryptography and Steganography – A Survey," International Journal , ISSN: 2229-6093, Vol 2 (3), PP. 626- 630, 2011.
9. A. J. Altaay et al, "An Introduction to Image Steganography Techniques," International Conference on Advanced Computer Science Applications and Technologies, PP. 122 - 126, 2012.
10. L. M. Marvel et al "Spread Spectrum Image Steganography," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, PP. 1075 - 1083 AUGUST 1999

11. B. Zaidan, A. A. Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15), PP.1650-1655, 2010.