" A REVIEW : CRYPTOGRAPHY AND STEGANOGRAPHY FOR DATA HIDING IN IMAGES"

PRAGYA [1]
M. Tech. CSE Scholar
Greater Noida Institute Of Technology, Gr. Noida

DR. YATIN KUMAR AGARWAL[2]
Asso. Prof., CSE Deptt.
Greater Noida Institute Of Technology, Gr. Noida

Abstract: Now a day's cloud computing is used in numerous domain like business, social network website, YouTube, colleges etc. to store enormous quantity of data. We can retrieve data from cloud on demand of user. To store data on cloud we have to face numerous issues. To afford the resolution to these problems there are quantity of ways .Cryptography and steganography approaches are currently used for data security algorithms measured for fusion decryption and encryption can be implemented to improve security over the cloud computing. The objective is to construct ultra-compact transactional data storage to achieve data storage such that the execution time and communication overhead for encoding and decoding are reduced. To Design and implementation of Security of Data in Cloud computing environment we are using Fusion level Algorithm. Our fusion level approach is based on Cryptography with row and Column level encryption which has been accomplished by integrating ECC.

Keywords: Fusion level Algorithm cloud server (CS), Encode, Decode, Delay, Integrity

1.INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and steganography methods into one system for better confidentiality and security.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganography methods will not. However, steganography and cryptography differ in the way they are evaluated: steganography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the

steganography medium. The disciplines that study techniques for deciphering cipher messages and detecting hidden messages are called *cryptanalysis* and *steganalysis*. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages. The aim of this paper is to describe a method for integrating cryptography and steganography through some media such as image, audio, video, etc.

Cryptography and Steganography are often interrelated and share the common goals and services of protecting the confidentiality, integrity and availability of information; which are some of the most important fields in computer security. Cryptography and steganography are methods of transferring private information and data through open network communication, so only the receiver who has the secret key can read the secret messages which might be documents, images or other forms of data. Cryptography and steganography also contribute to

Computer Science, particularly, in the techniques used in computer and network security for access control and information confidentiality. They are also used in many applications encountered in everyday life. Despite the differences between Cryptography and Steganography systems the requests for them have increased recently for the fast development of the Internet publicly.

2. LITERATURE REVIEW

Ahmed AL-Shaaby, TalalAlKharobi et al Digital communication witnesses a noticeable and continuous development in many applications in the Internet. Hence, secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide network security. In this paper, we survey a number of methods combining cryptography and steganography techniques in one system. Moreover, we present some differences between cryptography and steganography. The aim of this paper is to develop a new approach to hiding a secret information in an image or audio or video, by taking advantage of benefits of combining cryptography and steganography. In this method first, the message is encrypted by using AES algorithm and hashed the key using SHA-2 to prevent from attacks. After that, we performed some modifications on LSB algorithm by adding a key to make hiding process non sequential. Results achieved indicate that our proposed method is encouraging in terms of robustness and security [1].

HAYFAA ABDULZAHRA, ROBIAH AHMAD Cryptography and Steganography are the two popular methods for secure data hiding and transmission available broadly. The techniques used information in order to cipher or cover their

existence respectively. Cryptography is the science of using mathematics to encrypt and decrypt data; the data are converted into some other gibberish form, and then the encrypted data are transmitted. While Steganography is the art and science of hiding communication, a stenographic system, thus embeds hidden content in the unremarkable cover media so as not to provoke an eavesdropper's suspicion. In steganography the secret message embeds in a harmless looking cover such as a digital image file, then the image file is transmitted. The primary purpose of this paper is to improve a new method of hiding secret messages in the image, possibly by combining steganography and cryptography. A new encryption technique is used in order to lower the space of representing the characters. LSB method is used to hide the encrypted message into images. PSNR and MSE are used for measuring the quality of images; the results showed that the proposed method gives better results than simple LSB with higher PSNR lower MSE [2].

G. Naveen Samuel et al A new technique proposed with the combination of cryptography and steganography enhanced with powerful algorithms for generating a new security system can be called as Crypto Steganography System. It consists of both cryptographic functions and steganography functions. Here in this paper a security system is enhanced by ensuring data hiding operation using steganographic function. The message to be transferred is encrypted using an AES algorithm which is modified for steganography to occur. Encrypted message is encouraged with a text and a key. Now to make the transfer to be more secured we introduce another two keys with the encrypted message where the message is made to be hidden in an image. Image bears the message in which it needs both keys for viewing the text message behind it. A Steganography function makes the message detection process much harder for the hackers who interrupt between the sender and receiver. This kind of system is to be introduced in applications such as transferring secret data that can be authentication of various fields. This system ensures a secure data transferring option between the source and destination stations [3].

Sandeep Kumar U et al Increase in the number of eavesdroppers during information exchange between the source and intended destination has indeed called for a more robust method for securing data transfer. Steganography and Cryptography are the well-known and widely used techniques that manipulate the information in order cipher and hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. In this proposed system, a data hiding,that is based on image steganography, cryptography and water marking is employed to secure data transfer between the source and destination. DWT (Discrete Wavelet transform) method is used to compression of image in steganography and a ECC (Elliptic Curve Cryptography) is employed to encode the message inside the image. the proposed system not only hides large volume of data in an image, but

also limits the perceivable distortion that might occur in an image while processing it, and provide a strong backbone for its security [4].

A. Dhamija and V. Dhaka, et al proposed an encrypting technique by combining cryptography and steganography techniques to hide the data. In cryptography process, they proposed an effective technique for data encryption using one's complement method, which we called as SCMACS. It used a symmetric key method where both sender and receiver share the same key for encryption and decryption. In steganography part, we used the LSB method that is used and mostly preferred [5].

P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz et al authors proposed a highly-secured steganography technique by combining DNA sequence with Hyper elliptic Curve Cryptography. This approach executes the benefits of both techniques to afford a high level of security communication. Also, it uses the benefits of both DNA cryptography and Steganography. This algorithm tries to hide a secret image in another cover image by convert them into DNA sequence using the nucleotide to the binary transformation table. On the sender side, the embedding method includes three steps. First, they convert the values of a pixel of both the cover image and secret image to their respective DNA triplet value utilizing characters to the DNA triplet conversion. Secondly, they convert the triplet values to binary values format. In the final stage, apply the XOR logic between binary values of both secret image and cover image to generate a new image which called stego image [6]

S. S. Patil and S. Goud et al , authors presented a new technique called multi-level secret data hiding which integrates two different methods of encryption namely visual cryptography and steganography. The first step of this method thy used a method called halftoning which is used to reduce the pixels and simplify the processing. After that visual cryptography is performed that produces the shares which form the first level of security and then steganography in which thy used the LSB method to hide the shares in different media like image, audio, and video [7].

3. Proposed Methodology

One of the major problems in enforce entrance control via discriminating encryption is the figure of secret keys that every user must keep securely. In our approach, every user requirements simply to preserve one secret key to get access to all of her authorized resources, which is quite an advantage. This advantage is a result of using a shared value for each resource's secret value which is stored next to every resource there by the allowed user can calculate the resource's secret value effortlessly [8].

Competence of operation particularly policy update operation is one more famous feature. Growing the number of users does not impress any additional attempt to the system. Moreover, the time complexity for grant and retract is remain polynomial as Garner's algorithm imply, which help the scalability of the resolution. Theorem

resolution, according to an resourceful algorithm in. furthermore, the total complexity of yielding or revoke constitutional rights is precious by the complexity of the secret value encryption which is perform for every authorized user. Thus, using a linear encryption technique, a grant or retract operation has a time complexity compare with the approach in our technique the user does not have to get a lot of keys to contact her allowable resources. So, access the resources is additional competent here and does not require a number of interactions with the server to drive the suitable keys. In our approach, privacy of security policies ispreserved beside both the server and users as extended as theusers are anonymous. The server, common users, authorizedusers, and some subject access the server cannot recoveror close several owner approve access control policy [9].

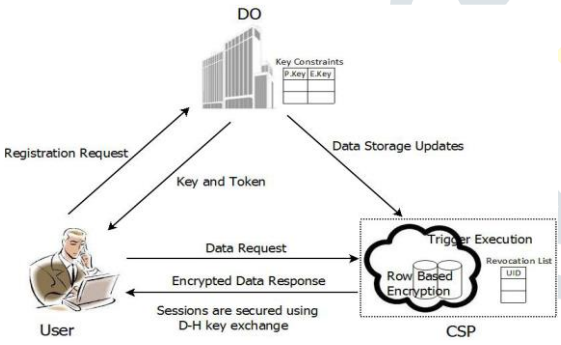

Figure 1 Proposed Database Outsourcing Model

This is theoutcome of the with joint values in its put of key beginning method in our technique delegation of access control enforcement to the server is feasible via key beginning by the user. Our proposed methods, be appropriate to share a secret value between authorized users, and users simply decrypt the shared values to get the suitable secret values. No information is showing even subsequent to decryption. Every user or a number of other internal or external party, simply in the case of theauthorized users' keys ownership will be capable to recognize acceptable users from. Though, in our technique the users' secret keys are indefinite to be private and accordingly the beyond information leakage is impossible.

4.RESULTS AND DISCUSSION

Login page for cloud replication with valid IP address, email id and password.

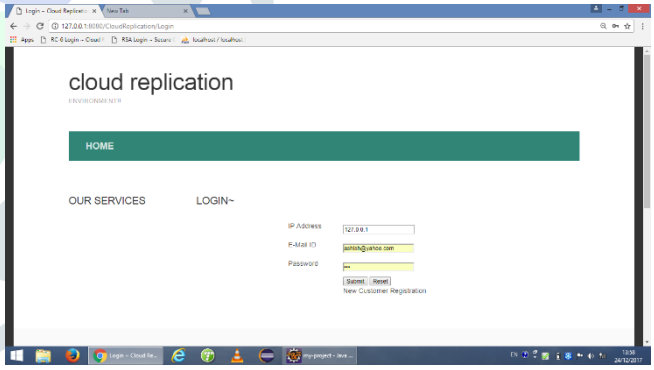

Figure (2) Login Page (Cloud replication).

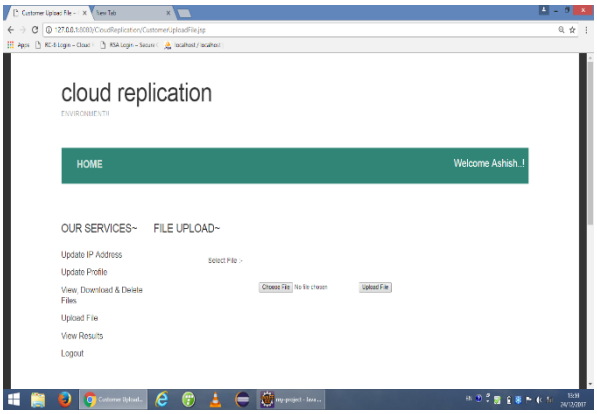

Fig (3) Home Page (Cloud replication).

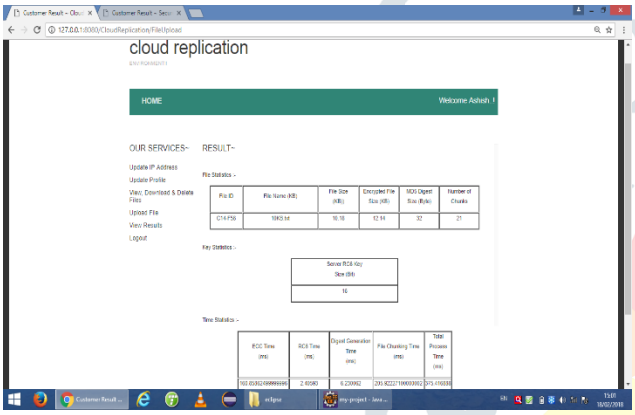

Figure (4)Result for all File size (Cloud replication)

Table 4.1 Representing RSA Computation Time

File Size (KB)	RSA Computation Time (ms)
10	3739.03
20	6721.64
50	17223.12
100	34155.75
150	47893.74

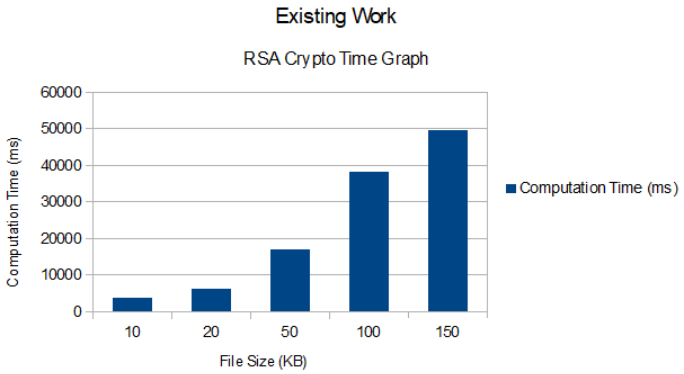

Figure (5) Graphs for Existing Work

Table 4.2 Representing Hybrid encryption Computation Time

File Size (KB)	Hybrid Encryption Computation Time (ms)
10	375.41
20	687.51
50	1274.06
100	2718.38
150	4532.11

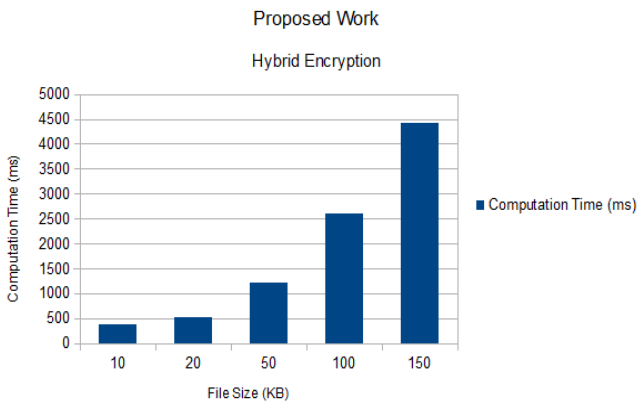

Figure (6) Graphs for Proposed Work

Below graph represents the comparison of proposed work and existing work, computation time is calculated on the basis of different file size. Time is taken in mille second, whereas file size in KB.

Comparison graph shows computation time is reduced in the proposed work as compared to existing work.

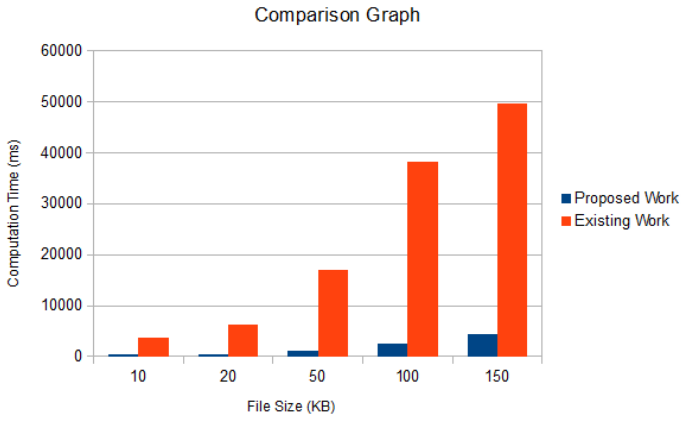

Figure 7 Comparison Graph for Proposed Work and Existing Work

CONCLUSION

though approximately a decade of explore on secure data outsourcing, available approaches have not been report to have a lot achievement in process due to initially, they overcome security challenge with rigid limitations on data types or query support, each now and then with important overheads, and secondly, they gratify different necessities such as accuracy and privacy based on unrelated or even opposing assumption. The potentially unstable enlargement of database outsourcing is disadvantaged by security concern: privacy and integrity. Though privacy in outsourced databases has been at extent researched, there still does not exist a sensible system that can give absolute integrity guarantees before this work. Security is the big requirement in the field of computer science. In the depth analysis everything is thoroughly analyzed in rapid way. In the proposed work security is observed and implemented for the purpose of secure replication. It mainly focuses on the originality of replicated by calculating its integrity and verifying its content. Here, hybrid security algorithm using RC6 and ECC is used for secure data. RC6 lowers the computation overhead while ECC as the asymmetric key reduces the computation time.

REFERENCES

[1] A. Dhamija and V. Dhaka, “A novel cryptographic and steganographic approach for secure cloud data migration,” in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 346–351.

[2] P. Vijayakumar, V. Vijayalakshmi, and G. Zayaraz, “An improved level of security for dna steganography
usinghyperelliptic curve cryptography,” Wireless Personal Communications, pp. 1–22, 2016.

[3] S. S. Patil and S. Goud, "Enhanced multi level secret data hiding," 2016.

[4] B. Karthikeyan, A. C. Kosaraju, and S. Gupta, "Enhanced security in steganography using encryption and quick response code," in Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016, pp. 2308–2312.

[5] B. Pillai, M. Mounika, P. J. Rao, and P. Sriram, "Image steganography method using k-means clustering
and encryption techniques," in Advances in Computing, Communications and Informatics (ICACCI), 2016
International Conference on. IEEE, 2016, pp. 1206–1211.

[6] A. Hingmire, S. Ojha, C. Jain, and K. Thombare, "Image steganography using adaptive b45 algorithm
combined with pre-processing by twofish encryption," International Educational Scientific Research
Journal, vol. 2, no. 4, 2016.

[7] F. Joseph and A. P. S. Sivakumar, "Advanced security enhancement of data before distribution," 2015.

[8] B. Padmavathi and S. R. Kumari, "A survey on performance analysis of des, aes and rsa algorithm along
withlsb substitution," IJSR, India, 2013.

[9] R. Das and T. Tuithung, "A novel steganography method for image based on huffman encoding," in
Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on.IEEE, 2012, pp. 14–18.