International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 1, Issue 3, pp 16-18, December-2017

Encryption of the Data/Image Maintenance and Backup of the Patients Personal Health Information Using Image Steganography

Dr Nelson Jaladanki

Professor, Department of Computer Science and Engineering, Malla Reddy College of Engineering for Women, Hyderabad -500100, Telangana, India

Abstract - Healthcare professionals use video records of a patient. All this data is stored on the healthcare cloud, which provides services like maintenance and backup of the patients Personal Health Information (PHI), for any further studies or legal procedures. The healthcare cloud is constantly under the threat of data theft attacks which are the most serious forms of attacks. Hence the main goal of system is to make these data theft attacks difficult for the attackers. Steganogrphy is the art of hiding the fact where communication is taking place, by hiding information in other information. Steganography becomes more important as more people join the cyberspace revolution. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. Security is provided by encrypting the data that is sent in the image and again encrypting the image that carries the information using AES algorithm. This encryption of the data and image thus provides double security.

Keywords: AES Encryption, Steganography, Healthcare, Cloud, Healthcare.

1. INTRODUCTION

Now a day's the uses of devices like computer, mobile and many more other device for communication as well as for data storage and transmission has increases. Here arise data security problems. To overcome this uses the technology AES and Steganography. Healthcare cloud infrastructure is used to store medical information. It helps in managing and tracking the patient's healthcare information, even if the patient moves across multiple cities. Healthcare cloud has several security issues like privacy protection, absence of security standards, legal and policy issues, lack of transparency, data protection, and licensing. A methodology is proposed to secure the patient's Medical Big Data (MBD) by using the fog computing facility along with the stegnography and also provide a secured healthcare cloud. This security is provided in two layers. First the data that is to be hidden in the image is encrypted using AES algorithm. This encrypted data is then hidden in the image. The image with the hidden data is then encrypted again. Thus the user with the decryption key of both image and data will be able to retrieve the data and image in its original form. De-duplication, which eliminates redundant copies in user provided data, has been widely used to improve storage utilization and reduce communication cost. The saving is significant for cloud storage service provider which stores data from many customers. Typically, storage systems require seeing the client data in plaintext to perform de-duplication, which incurs obvious privacy threat. On the other hand, if every user encrypts their own file using a user-specific key, the effectiveness of de-duplication is drastically reduced since the probabilistic nature of a secure encryption intuitively produces random-looking cipher texts. The first attempt to resolve the seemingly contradicting requirements was convergent encryption. It works by mapping each file into a key deterministically by hashing the file and then encrypting each file using such file derived key. This ingenious solution guarantees that identical files are encrypted to identical cipher texts, enabling efficient de-duplication. Convergent encryption (and its variants) has been used in numerous applications.

Objective

Confidential and sensitive data stored in the cloud is extremely crucial. So the main aim is to protect data sharing using keys and secure to both the data hidden and the image that carries the information in medical field.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 1, Issue 3, pp 16-18, December-2017

Scope

The main scope of this is to provide security and reduce the storage space and avoid problems of discrete data. The proposed mechanism is providing high security to the video data and image data.

2. RELATED WORK

All other works focus on static files, with no support of file update (even with the help of a key-management server). To modify a single bit, the file owner has to download the whole encrypted file, decrypt, update, re-encrypt, and then upload the new cipher text to the cloud. The computation and communication costs of these operations are linear in the file size, which are too expensive for large files

3. PROPOSED SYSTEM

The distributed source coding (DSC) to encrypt image in RDH, by encrypting the original image/media using stream cipher, the data-hider compresses a series of selected bits which is taken from the encrypted image to make the secret data. The original image is encrypted directly by the sender and the data-hider embeds the additional bits by modifying some bits of the encrypted data. Data extraction and image recovery are realized by analyzing the local standard deviation during decryption of the marked encrypted image. The receiver end has both the embedding and encryption key and then the receiver can extract the secret data and recover the original image perfectly using the distributed source decoder. The expected result is lossless image and data. The security of the image can be enhanced by encrypting the data and the image in which the data is hidden. The receiver should have keys to retrieve the data (i.e.) the decryption key of the data, the retrieving key of the data from the image and lastly the decrypting key of The Image.

Encryption of Video

Here use AES encryption technology for encrypt the single video and decrypt the video in this way it can assure the security. For encryption purpose four rounds consist of substitute byte, shift row, six columns, add round key. AES specifies a federal information processing standards publication (FIPS) approved cryptographic algorithm that can be used to protect electronic data. It is the reverse process of EDE encryption method. The user can use the same key for encryption and decryption. The sequential order is changes but the key remains the same.

4. SYSTEM MODEL

The data hiding and image encryption are done by using two different keys. That is encryption key and the data hiding key. The receiver who has the data hiding key can retrieve the data embedded. The receiver who has the encryption key can retrieve the original image without removing or extracting the data embedded in the encrypted image. The receiver who has the both the keys can retrieve the hidden data and the original image from the encrypted image. The Fig-1 illustrates the details about the model.

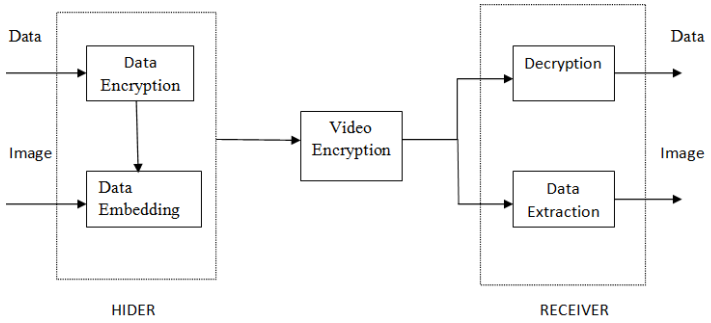

Fig – 1: System Architecture

Steganography

Image steganography used to hiding the data such as text, image, audio files into another image. Here used this technique is to secure the user password. In this way we can prevent the hackers attack. The hidden information decoding through a proper

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 1, Issue 3, pp 16-18, December-2017

decoding technique. Fig – 2 shows the working model of the steganography technology. There is no difference between the original file and the file with the message embedded into it. This is accomplished by storing the message using LSB (Least Significant Bits) in the data file.

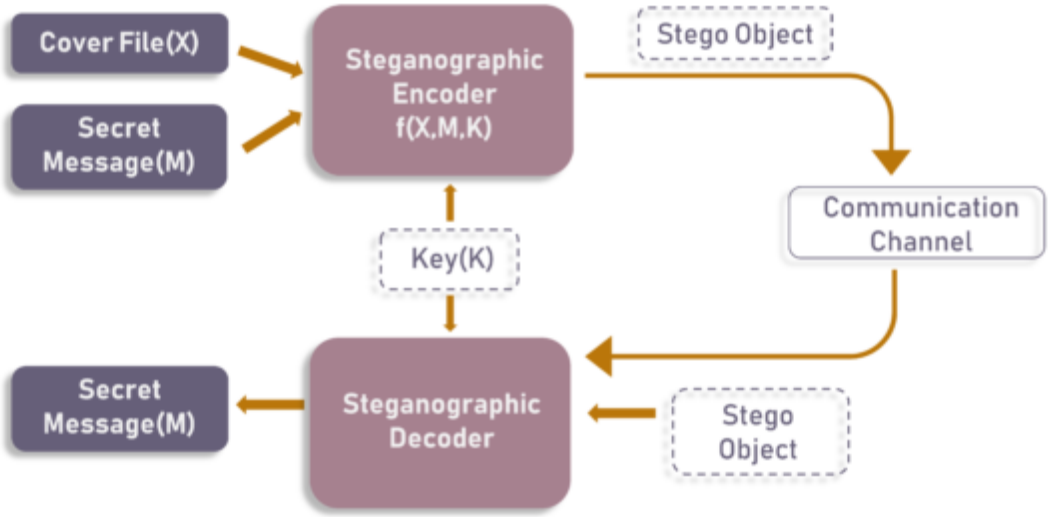

Fig – 2: Working model of steganography

5. CONCLUSION

The system provides high level security since the intruder does not know about the data that is hidden in the image. Thus the intruder will only be able to retrieve the image may be by using his technical knowledge. But he won't be able to know about the data since there will be no traces of data that is hidden in the image. Only the person with proper authentication will be able to retrieve both the original data and the image. Thus this system can be used in various fields where the image and its relevant data have to be transmitted in a secured way. In the medical field where the patient report with its measures has to be sent to the hospital authority securely this system can be used. This technique of hiding a particular video file in the image hide it securely with minimum mean square error and hence gives maximum peak signal to noise ratio. So it helps to transmit data securely by embedding it in a image file and without disclosing to the unintended receiver and without any alternation in secret message.

REFERENCES

[1] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in EUROCRYPT, 2013.

[2] An image encryption and decryption using AES algorithm- Priya Deshmukh.

[3] R. Chen, Y. Mu, G. Yang, and F. Guo, "BL-MLE: block-level message-locked encryption for secure large file deduplication," IEEE Trans. Information Forensics and Security, vol. 10, no. 12, 2015.

[4] D. T. Meyer and W. J. Bolosky, "A study of practical deduplication," TOS, vol. 7, no. 4, 2012.

****

