IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DATA HIDING ON SHARED DATA IN CLOUD USING ENCRYPTION WITH PRIVACY MODE

[1] M.Masilamani,

[1]Assistant Professor,
[1]Information Technology,
[1]Hindusthan college of Engineering and Technology, Coimbatore, India.

Abstract: *The Army record maintenance is sensitive and crucial task in Military Sectors. The Soldiers records are stored in a huge data set; it can be stored, maintained and traced every day. The objective of this project is to store soldiers reports safely.* In Existing, Cryptographic-based encryption is to encrypt data into unreadable code; it is more likely to attract the attacker's attention. Once these ciphertext is intercepted, the attacker will try to decrypt these ciphertext to obtain some useful information, so as to carry out some illegal activities. Some Military information not only have high requirements for privacy protection, but also want to be able to express their preference in the decision-making of privacy protection, so they may want to define what information is sensitive to them and what is not. The proposed model can classify the data into sensitive data and non-sensitive data according to the user's preferences with SVM (Support Vector Machine) based machine learning classification. Since non-sensitive data pose no threat to user privacy, it can be transmitted directly on ordinary channels without being processed. While, sensitive data need to be processed before it can be transmitted. In terms of sensitive data processing, here proposes a method of combining data encryption with information hiding. Sensitive data are encrypted using Advanced Encryption Standard (AES) encryption algorithm before it can be transmitted, making it to unreadable code. Then, a novel information hiding method proposed, named the Modified LSB (MLSB) information hiding method is used to provide a second guarantee for the security of sensitive data. In other words, the sensitive information is hidden in the multimedia carrier, so that the adversary cannot notice the existence of sensitive information.

Keyword - Privacy protection, data encryption, information hiding

I. INTRODUCTION

We are hiding the secret messages using steganography within every day. The receiver can understand the information is hidden on the image then the receiver use particular steganography method to recover the hidden text to stego text. The goal of steganography is allow the sender and receiver to communicate each other but the Third party cannot identify the hidden text. Hidden information can seem as encrypted data. It was decrypted by the receiver using the decrypt key. The key was generated by AES advanced encryption standard algorithm. Steganography can replace different bits with unused bits in the computer files. When the encrypted file is deciphered then also we cannot see the hidden information because the encrypted file is still hide information using steganography. The image using top three most significant bits for hiding the data.it gives better security for hiding the information**.** The admin can maintain the entire database. In this project we are hiding the information in admin page and in database also. The only possibility is the user want to send request to the admin then the admin verify the request and give approval. The admin gives approval means two keys are automatically generate to there requester mail one key is unhide key and other key is decrypt key. The mail will send using SMTP simple mail transfer protocol. On the requester page first we want to view the image then we want to use the unhide key to unhide the hidden information on the image. On the final stage we want to use the decrypt key to decrypted and view the information that is hidden on the image using steganography. Before transmitting the information to the server, they are classified into sensitive data and non-sensitive data according to the preference of users. For the classification purpose here utilize machine learning based SVM (Support Vector Machine) algorithm. At first, users label the dataset according to their own preference, and

then the classifier trains the classification model. In order to reduce the complexity of the classifier and give consideration to the universality of the classifier, this paper decides to adopt SVM as the classify model.

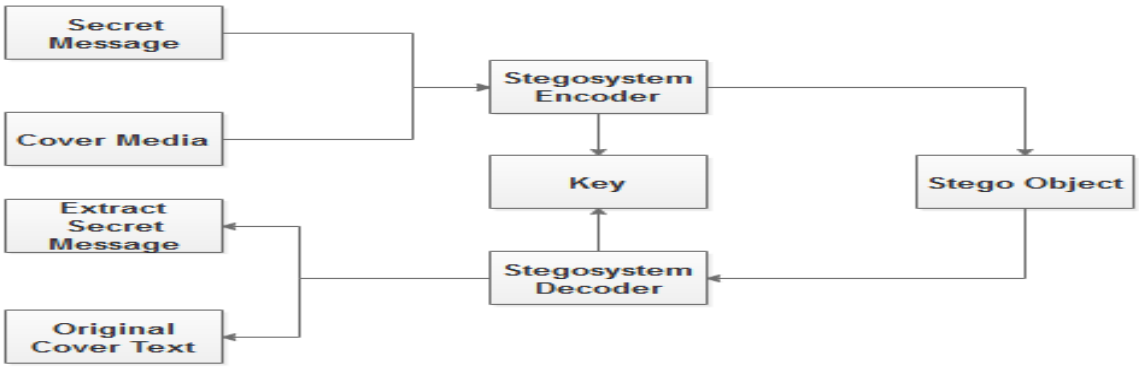

Figure 1.1 Processing steps for Steganography.

II. EXISTING SYSTEM

RDH could be utilized in various fields like military, healthcare image processing, and Forensics.In existing, information is embedded by increasing. the contrasts between two neighbouring pixels. Data Encryption Standard (DES) encryption algorithm used for converting sensitive data into unreadable code. Top Three Most Significant Bit plain (TTMSB) information hiding method is used to provide a second guarantee for the security of sensitive data.

III. PROPOSED SYSTEM

To implement secret data encryption with data hiding approach. Sensitive data are automatically classified with the help of SVM classification. Then sensitive data are encrypted using AES Encryption Technique. Hide the encrypted sensitive information in cover image using Modified LSB Technique. The receiver can extract secret information and decrypt the marked image to get a image that is similar to the original image.

IV. SYSTEM ARCHITECTURE

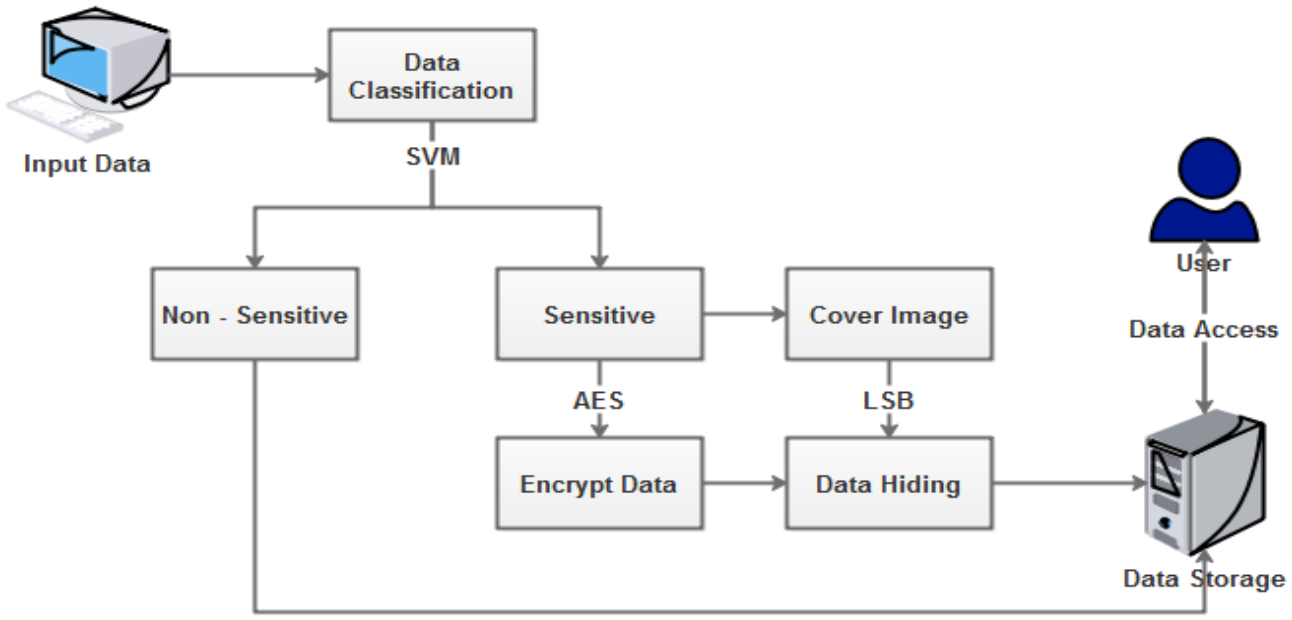

Figure 1.2 Architecture of the Data Hiding.

V. ADVANTAGES:

To eliminate human intervention and to enhance the effectiveness of the distributed computing system. Enhance security with image encryption algorithm. Reduce the data loss during data hiding and retrieval process. Make ease of key generation and key sharing process.

VI. DISADVANTAGES

Attacker can predict the secret data during transmission. Low embedding capacity during data hiding. Does not provide image encryption process, so image can be easily accessible by unauthorized users. DES provide less security comparable with advanced encryption techniques.

VII. Module List

- Framework Creation
- Data Categorization
- Encrypt Sensitive Data
- Sensitive Data Hiding
- Data Extraction

Framework Creation

Army data sharing is the process share soldier information to the requester. Here create an application for secure soldier information sharing using data hiding and encryption approach. Before accessing application user should enroll in this application. User enrolment is the process of registering with application to make communications. Authenticated users are only allowed to access application. Otherwise the system shows invalid access message.

Data Categorization

Before transmitting army information to the server, they are classified into sensitive data and non-sensitive data according to the preference of users. For the classification purpose here utilize machine learning based SVM (Support Vector Machine) algorithm. At first, users label the dataset according to their own preference, and then the classifier trains the classification model. The non-sensitive data can be transmitted directly on the ordinary channel without being processed. While, the sensitive data is firstly encrypted, and then the ciphertext that present with garbled code state is hidden into the cover image.

Encrypt Sensitive Data

Data encryption is the process of converting the plain text information into unreadable form. Here sensitive information could be encrypted using AES algorithm. Because the army system focuses on lightweight, in order to reduce the complexity of data encryption operation and take the security of encryption into consideration, the scheme decides to use AES data encryption algorithm. This will enhance the security of shared secret image.

Sensitive Data Hiding

Data hiding is the process of hiding secret message into cover file. The encrypted sensitive soldier information was hidden within the image to create stego image. Generate key for securely sharing the information to receiver. In the process of embedding, the cover image is divided into non-overlapping pixel blocks of 3x3 pixel blocks. Block levels are based cardinality of the cover image. If secret bit is 1 and LSB of stego pixel is 0 or vice-versa, then 1 is added or subtracted to the stego pixel.

Data Extraction

Data extraction is the process of extracting the original data. Receiver gets the sensitive information with cover image. Specific key is generated and shared to the receiver during the process of data sharing. After receiving the stego image, the receiver extracts the ciphertext from the stego image with the extraction key. Then decrypts the ciphertext with the decryption key to obtain the plaintext data.

Conclusion

This paper proposes a reversible data hiding technique for sensitive information hiding using SVM classification technique. The data hiding capacity and speed is increased by combining Modified LSB with AES Encryption. Encryption helps to enhance the security in communication domain.

REFERENCES:

[1] Patel, Arpit, and Tushar A. Champaneria. "Fuzzy logic based algorithm for Context Awareness in IoT for Smart home environment." In 2016 IEEE Region 10 Conference (TENCON), pp. 1057-1060. IEEE, 2016.

[2] Mehrotra, Sharad, Alfred Kobsa, Nalini Venkata subramanian, and Siva Raj Rajagopalan. "TIPPERS: A privacy cognizant IoT environment." In 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), pp. 1-6. IEEE, 2016.

[3] Keshavarz, Mahsa, and Mohd Anwar. "Towards improving privacy control for smart homes: A privacy decision framework." In 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1-3. IEEE, 2018.

[4] She, W. E. I., Zhi-Hao Gu, Xu-Kang Lyu, Q. I. Liu, Zhao Tian, and Wei Liu. "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving." IEEE Access 7 (2019): 62058-62070.

[5] Zhou, Zhili, Huiyu Sun, Rohan Harit, Xianyi Chen, and Xingming Sun. "Coverless image steganography without embedding." In International Conference on Cloud Computing and Security, pp. 123-132. Springer, Cham, 2015.

[6] Bilal, Muhammad, Sana Imtiaz, Wadood Abdul, Sanaa Ghouzali, and Shahzad Asif. "Chaos based Zero-steganography algorithm." Multimedia tools and applications 72, no. 2 (2014): 1073-1092.

[7] Singh, Siddharth, and Tanveer J. Siddiqui. "A security enhanced robust steganography algorithm for data hiding." International Journal of Computer Science Issues (IJCSI) 9, no. 3 (2012): 131.

[8] Zheng, Shuli, Liang Wang, Baohong Ling, and Donghui Hu. "Coverless information hiding based on robust image hashing." In International Conference on Intelligent Computing, pp. 536-547. Springer, Cham, 2017.

[9] Zou, Liming, Jiande Sun, Min Gao, Wenbo Wan, and Brij Bhooshan Gupta. "A novel coverless information hiding method based on the average pixel value of the sub-images." Multimedia tools and applications 78, no. 7 (2019): 7965-7980.

[10] Chen, Min. "Towards smart city: M2M communications with software agent intelligence." Multimedia Tools and

Applications 67, no. 1 (2013): 167-178.