ISSN:0975-9646

Separable Reversible Data Hiding in Image Using Advanced Encryption Standard with Fake Data Generation

Divyani UdayKumar Singh, Kasturi Mohan Padwal, Madhura Pundlik Jadhav

Department Of Information Technology
Dr. D. Y. Patil Institute of Engineering and Technology
Ambi, Pune, India

***Abstract* – The concept of steganography is used in the paper to transmit the data secretly and safely from one user to another as it hides the data behind image. In this sender encrypt data using AES algorithm, hides encrypted data in image using LSB technique and the system auto generate the hide key. Sender sends the file with the help of existing mailing system. Receiver can perform action based on key like if he is having only data hiding then he can only get the image in original form and if he have data hiding and data decryption key then he will be able to get the original data, it also provides protection for the keys. All these are done with proper login process. The system generates fake data if the user is not authenticated in the process of login. In such a way only the authorized user, who was supposed to get the keys, is able to get the original data.**

Keyword*- Data encryption, *AES, LSB technique.

I. Introduction

The transmission of information over internet is vital and repetitive work in present scenario. Due to the increasing hacking, fraud, data manipulation, forgery, there is need of some extra functionalities to send data bovver internet. The paper introduces the separable reversible data hiding in encrypted image using Advanced Encryption Standard. Cryptography is used to convert the plain text data to cipher text to provide data security. The algorithms used for cryptography come under the Advanced Encryption Standard. To provide more security to the data, the concept of steganography is used, which helps to hide the encrypted data behind any image. It only acts as carrier of data in network from one user to another. Keys like data hide key and decryption key are auto generated by the system. These keys are generated by the sender while file uploading and transmitting files over internet.

These file uploading by the sender is done when he is properly logged in to the system. The receiver on the other hand, authenticates himself and downloads these files, using the keys provided by the sender in a separate e-mail. If the user is not properly authenticated then he is not allowed to get the original data. There is a fake data generated by the system which misguides the unauthorized user by pretending to be the original one. Proper security is provided by the system along with safe transmission of data over internet. AES algorithm and LSB techniques are used in the system for data encryption and hiding data behind image respectively.

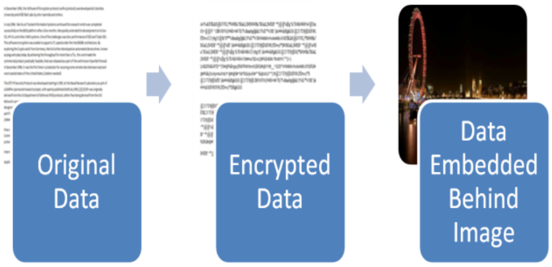

Fig. 1 Cryptography and Steganography

A large volume of data transmitted over internet is private and confidential. Encryption is the desired to transmit the information correctly and safely. The security provided by stegenography is more than the security provided by cryptography alone. Thus due to various similar reasons these concepts are widely used in data transfer through internet now a days. These two concepts are used in the system along with authentication which provides the authorization to the user to use the system with all correct functionalities

Cryptography can protect the data while transmission but when it is decrypted, there is no more protection left. To provide more protection and safety information hiding techniques are used now a days and steganography is one of them which allows the user to store a large amount of data behind any image. Cryptography aims at creating data unintelligible for the third person who is not authorized to get the information. Steganography deals with hiding the data from the third person behind any image.

II. Literature Survey

Previously, data to be transmitted were encrypted using the algorithms like DES, Triple DES, Blowfish. They provided the data protection but up to certain extent.. The Protective measure of highly confidential data is on demand in the market. DES algorithm consumes least decryption time. It is a secret key based algorithm which experiences problems like key distribution and key agreement but provide throughput in less power intake. On the other hand, AES algorithm uses least memory usage. Cryptographic methods do not hide the secret data. On the other hand data can be protected by using information hiding techniques. Information hiding techniques embeds the data into cover objects like texts, images, audios, videos. For more security, cryptographic techniques can be applied to an information hiding scheme to encrypt the private data. Stagenography can be used to increase the chances to hide the data so that the intruders are not able to get the data as it will be hidden behind the image.

The previous method is made of image encryption, data embedding and data extraction/image recovery phases. The sender encrypts the original image using an encryption key to produce an encrypted image. Afterward, the data hider compresses the least significant bits (LSB) of the encrypted images using a data hiding key to create a sparse space to adjust the extra data. At the receiver side, the data embedded in the created space can be easily recovered from the encrypted image containing additional data with the help of data hiding key. Since the data embedding only influences the LSB, a decryption with the encryption key can result in an image analogous to the original image. When using both of the encryption and data-hiding keys, the embedded additional data can be extracted and the original image can be perfectly restored by taking advantage of the spatial correlation in natural image. If the lossless compression approach in is used for the encrypted image containing embedded data, the additional data can be even now also extracted and the original content of the encrypted image that contains embedded data. On the other hand, the lossy compression method in well-matched with encrypted image produced by pixel permutation is not suitable here since the encryption is done by bit-XOR operation.

A. *Image Encryption*

The original image in uncompressed design and each pixel with gray value coming under[0,255], denoted by 8 bits. In encryption stage, the XOR results of the original bits and pseudo-random bits are calculated.

B. *Data Embedding*

In the data embedding stage, some parameters are embedded into a small number of encrypted pixels and the LSB of the other encrypted pixel are compressed to create a space for inserting additional data and the original data at the location occupied by the parameters.

C. *Data Extraction and Image Recovery*

In this stage, the three cases are taken into account that a receiver has only the data-hiding key, only encryption key, and both the data hiding and encryption keys, respectively.

The first reversible data embedding scheme was put forwarded in Barton, 1997. The algorithm to achieve the reversibility encounters the underflow and overflow problem. The majority of the work on reversible data hiding is done on the data embedding/extracting on the plain spatial domain. But in a number of applications, a low-grade associate or a network administrator desires to add on some additional message like the origin information, image details or authentication data, within the encrypted image even if he does not know the original image content at the side of receiver.

Recently, we have observed that there are numerous system which have non separable data hiding in encrypted image which have so many limitation and compulsion like user is bound to have all keys to get the data, there is less security for the data. This type of systems cannot be taken in to account while transferring confidential data. To overcome limitation of previous system other new system proposes the separable and reversible data hiding technique in which data is going to be embedded in normal form as data have high security compare to image also because data have more priority than image. To overcome these problems, we propose the new system separable and reversible encrypted data in image using AES algorithm. AES algorithm provides the best security to the data to be encrypted as it includes various rounds during decryption. Both hardware and software implementations are faster while using the AES algorithm. Using separable reversible data hiding in image, the security can be increased and overhead can be decreased.

III. Proposed System

A secure method of data hiding will be used in the paper which provides authentication, data integrity and confidentiality. The combination of encryption and data hiding can solve these types of problems by using reversible data hiding method for images. It will be able to embed data in images. First encrypting data then compressing where compressor does not have knowledge of the encryption key. The system will provide user authentication and authorization to give more security to data while transmission. Fake data generation for unauthorized users and eavesdroppers will be there. The Encrypted data will be stored at database server by the sender.

There are various stages which will come under the processing of the data from one user to another.

A. *Sender Side*

It contains the overall processing of data in sender side. The steps for these are as follows:

1) *Data Encryption* - The sender selects the particular data or file such as word file or pdf and by applying the encryption algorithm he encrypts the data. Here, the algorithm used for encryption is AES.

2) *Data hiding* – The sender, after encrypting the data, hides this data behind any selected image to transmit it to the other user. Any image can be selected for processing like PNG, JPEG, BMP.

3) *Data Sending* – The information is send to the particular user after the data is successfully hidden behind the image.

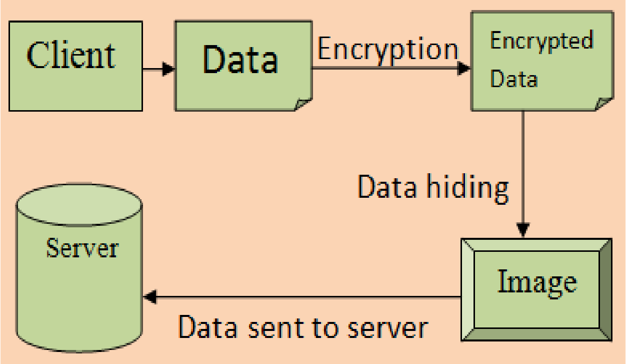

Fig. 2 Data uploading on sender side

This data is stored on the server for further processing along with a link to the receiving is separately sent to the receiver on his mail. Hide key is auto generated by the system which is mailed to the user.

B. Receiver side

In this Phase, The receiver authenticates himself and downloads the data sent by the sender to him.

1) Authentication – The receiver first authenticates himself while logging in to the system using his id and password. He will be able to download the contents which are sent to him by the particular sender.

2) Verification- The user is verified by the system whether he is authorized or not. If he is authorized then he gets the data by providing hide key and decryption key which is separately sent by the sender to his mail. If he only provides the hide key then he will be getting only image and if he provide decryption key also then he wiil be able to get the original data.

3) Fake Data Generation – If the user is not authorized by the system and during login if the username or password is found to be wrong then a fake data is generated by the system. This data is generate only to misguide the intruder and this data is not having any resemblance with the original data .

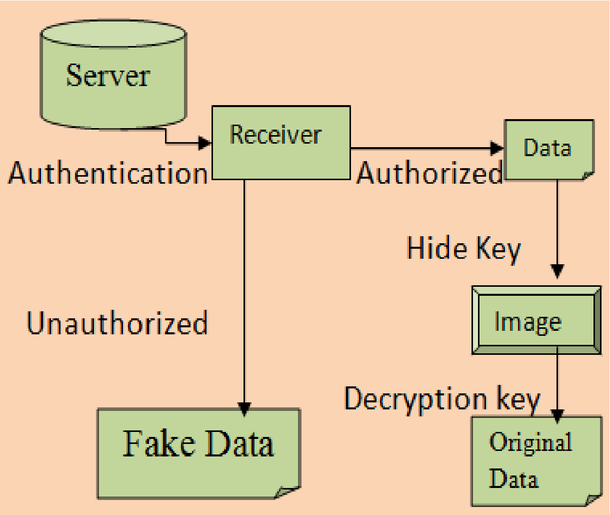

Fig: 3 Data downloading by the receiver

Completing these two stages, the secret and safe transmission of data is done without any extra overhead. The overall system overview can be represented by combining these two stages as a single stage from the point of view of both sender and receiver.

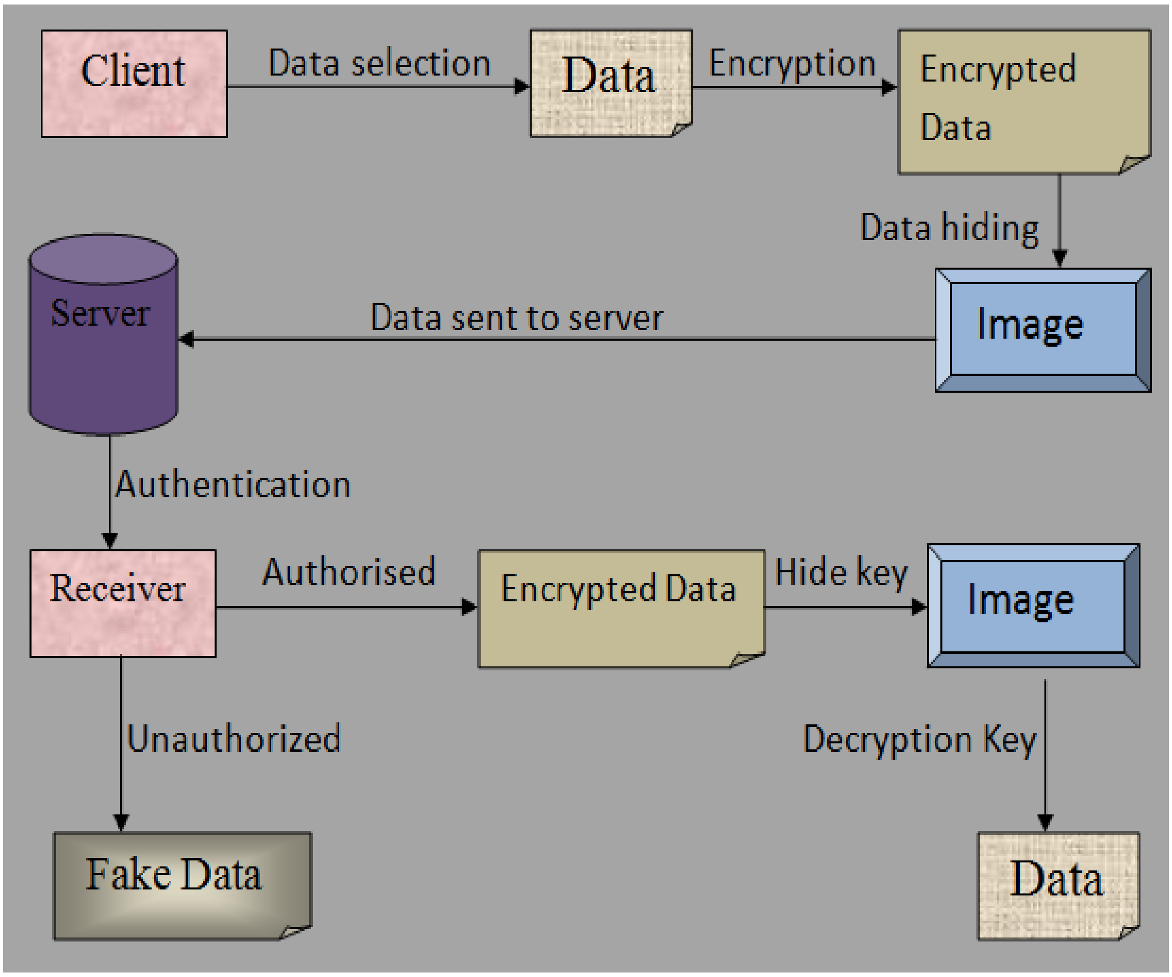

Fig. 4 System Architecture

IV. ALGORITHMS

A. AES Algorithm

AES algorithm, which is an iterated symmetric key block cipher with 128 bit block length which operates on fixed number of bytes which makes it simpler for implementation, is used in the system for data encryption. The algorithm uses same key for encryption as well as decryption of the data that decreases the overhead to manage keys. The size of both cipher text and plain text are same which is considered as an advantage. Internally, AES algorithm's data block is processed sequentially.

1) SubByte – The replacement of each byte is done with the help of S-Box. These are transformed using a non-linear but invertible S-Box. During encryption, each value of state is swapped by the corresponding S-Box value. And during decryption, each value in the state is changed with corresponding inverse of S-Box.

2) ShiftRows- The transformation regularly shifts last three rows in the state. It is a non-bitwise shift. Left shift of number of bytes is equal to the row number. It arranges state in matrix then apply circular shift for each row.

3) MixColumns – This stage contains two steps. The first step describes which part of state is multiplied over which part of the matrix. The second describes how the multiplication is implemented over GF. It is a substitution that used GF(Galois Fields) arithmetic. It considers each column as a vector of 4. Each column of state is replaced by another column obtained by multiplying that column with matrix in particular field.

4) AddRoundKey – Here, there is bit by bit XOR with expanded key. Each of the 16 byte state is XORed against each of the 16 byte of portion of expanded key for the current round. The expanded key bytes are never reused. During decryption, these steps are reversed.

The keys must be expanded preceding the encryption and decryption methods. The expanded key is used in add round key step. Due to a several number of advantages, AES algorithm provides the best way to encrypt any data. It provides high security, flexibility, simplicity and most important it has a reasonable cost. It is resistant to linear and differential cryptanalysis. The attack is not practically possible due to several rounds in algorithm. It is efficient for hardware and software both across various platforms.

B. Algorithm for embedding

1) Consider a Pixel array and store all the extracted pixel of the image in this array.

2) Consider a Character array and store all the characters extracted from the file.

3) Consider a Key array and store hide key and decryption key in it.

4) Store this file containing these details behind the image at any location or a particular location.

5) The image is now opaque, we are not able to see the embedded data behind it.

The embedding of the data behind image can be done in this way to make it transportable on network safely.

C. Algorithm for extraction

1) Consider the three array – Pixel array, Character array and Key array.

2) Extract the data behind the image using the hide key and decryption key.

3) If key does not matches the key in key array then generate fake data.

4) If only hide key matches the extract only image and if both hide key and decryption key matches then provide the original data.

5) Extract the data from the Character array.

In this way by following these algorithms, proper working of the system can be achieved. Operations from data uploading from sender to data downloading by receiver can be done efficiently

V. IMPLEMENTATION

The system is can be implemented on any Microsoft Windows environment. It can be operated on any web browser and will have conformity with Internet Explorer, Mozilla, Opera, Netscape Navigator. SQL Server 2008 and .NET 4.0 is used as a base for the system implementation. The system specification contains 500 GB hard disk capacity, 4 GB RAM, Intel processor 3.0 GHz. Using all these components, the system is executed successfully.

VI. SYSTEM FEATURES

A. Login

By providing proper login for users, it became a benefit for the system as sender and receiver will be verified before sending or receiving any of the data.

B. Keys

Keys are generated to provide extra security while downloading the information. Hide key is used to retrieve image then decryption key to get original data behind the image.

C. Fake data generation

To misguide the intruder who is basically not authorized to use the system get a fake data if he attempt to download the data with a wrong identification during login.

D. Keys send through mail

To provide more security for the time if any how some hackers get to know the receiver login details, the hide key is send separately by the sender to the receiver which is used at the time of downloading the information.

E. More security

The system provides more security without any overhead due to the verification and validation done at many stages during whole process.

VII. CONCLUSION

The system aiming to provide high security to the user does the same in various stages. At sender's side it encrypts the data then hides it behind any selected image. This data is sent to a particular receiver who is authorized to get the data. A separate hide key is also sent to that very receiver separately through e-mail. At the receiver's side, the user logging in first of all authenticates him-self from the system then after he is authenticated then he applies the hide key and decryption Key in order to get the data back. Receiver can get only image if he applies only hide key. In order to get the original data he needs to provide the decryption key also. If he fails in this then he gets a fake data. Due to these phases of security, the system can be considered for transmitting secret data over internet.

VIII. FUTURE SCOPE

The system can be extended to multimedia files transmission over internet secretly. Audio and video file format can also be used for secret communication between users.

ACKNOWLEDGMENT

We are grateful to our project guide Prof. Silkesha Thigale for her remarks, suggestions and time. Also the Head of the Department Prof. Amol Jadhao And Principal Dr. R. J. Patil for providing all the vital facilities like for providing the required facilities, Internet access and important books, which were essential. We are also thankful to all the staff members of the Department of Information Technology of Dr. D. Y. Patil Institute of Engineering and Technology.

REFERENCES

[1] Zhang, “Separable Reversible Data Hiding in Encrypted Image” IEEE Trans.Inform. Forensics Security, vol. 7, no. 2, pp. 826-832, April 2012.

[2]Mazhar Tayel, Hamed Shawky, Alaa El-Din Sayed Hafez, “A New Chaos Steganography Algorithm for Hiding Multimedia Data” Feb. 19 22,2012 ICACT2012.

[3] Akash Mandal, Chandra Prakash, Mrs. Archana Tiwari, “Performance Evaluation of Cryptographic Algorithms: DES and AES,” IEEE Trans.on Electrical, Electronics and Computer Science, 2012.

[4] Lokesh Kumar, “Novel Security Scheme for Image Steganography using Cryptography Technique”, Volume 2, Issue 4, April 2012.

[5] Komel Patel, Sumit Utareja, Hitesh Gupta, “A Survey of Information Hiding Techniques”, Volume 3, Issue 1,Jan 2013, IISN: 2250-2459.

[6] B. Padmavathi, S. Ranjitha Kumari, “A survey onPerformance Analysis of DES, AES and RSA algorithm along with LSB Substitution Technique”, Volume 2, Issue 4, April 2013, ISSN: 2319-7064.

[7] P. Mohan Kumar, Dr. K. L. Sunmuganathan, “A Reversible High Embedding Capacity Data Hiding Technique for Hiding Secret Data in Images”, vol. 7, No. 3, March 2012.