ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 4, April 2016

Encrypted Image With Hidden Data Using AES Algorithm

Muthulakshmi P, Shathvi K, Aarthi M, Seethalakshmi V

Abstract— **Steganography 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. Steganography include an array of secret communication methods that hide the message from being seen or discovered. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project report intends to give an overview of image steganography, its uses and techniques. In addition to this our project also adds security to both the data hidden and the image that carries the information. 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 layer.**

Index Terms— AES Algorithm, Decryption, Encryption, Steganography.

I. INTRODUCTION

Now a day the sharing of images over network is increasing in large numbers. The network security is becoming more important as the number of data being exchanged on the internet increases. More over the data that is relevant for the image is also send along with it. Therefore, the confidentiality and data integrity requires protecting against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding. Data hiding is a technique that is used to hide information in digital media such as images, video, audio etc. This technique is also referred to as steganography. Here the data is hidden in the image. The data may be the information about the image itself. The data hidden must be recoverable. Since in most of the application hiding of data in the image and the reversible process is essential. Reversible data hiding was first proposed for authentication and its important feature is reversibility, it hide the secret data in the digital image in such a way that only the authorized person could decrypt the secret information and restore the original image. Several data hiding methods have been proposed. The performance of a reversible data embedding algorithm is measured by its payload capacity, complexity, visual quality and security. Earlier methods have lower embedding capacity and poor image quality. As the embedding capacity and image quality is improved, this method became a convert communication channel. Not only the data hiding algorithm be given importance but also the image on which the data is hidden should also be highly secured. 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.

II. ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

AES is a symmetric key block cipher published by the NIST in December 2001. NIST evaluation criteria for AES are [1] Security [2] Cost [3] Algorithm and Implementation Characteristics. AES is a non-Feistel cipher that encrypts and decrypts a data block of 128-bits. The key size can be 128,192 or 256-bits. It depends on number of rounds. The input to the encryption and decryption algorithm is a single 128-bit block. The block is represented as a row of matrix of 16 bytes. AES structure is not a Feistel structure. ***Encryption*** is the process of converting plaintext to cipher-text (had to understand) by applying mathematical transformations. These transformations are known as encryption algorithms and require an encryption key. ***Decryption*** is the reverse process of getting back the original data from the cipher-text using a decryption key. In Symmetric cryptology- The encryption key and the decryption key could be the same as in symmetric or secret key cryptography, The key can different as in asymmetric or public key cryptography.

ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 4, April 2016

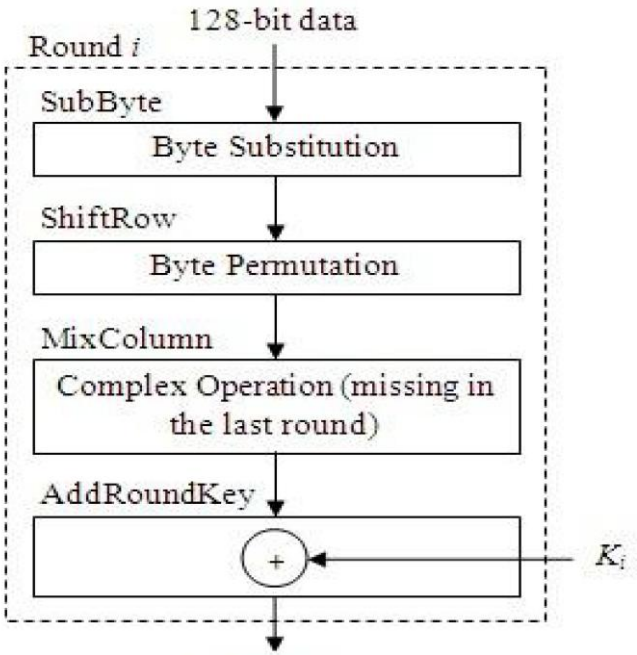

Figure AES Encryption

III. EXISTING SYSTEM

The existing system uses the histogram of the image to embed the data. This method also enhances the contrast of the image. The image enhancement is achieved by histogram equalisation. The highest peaks in the histogram are taken. The bins between the peaks are unchanged while the outer bins are shifted outwards so that each of the two peaks can be split into two adjacent bins. To increase embedding capacity, the highest two bins in the modified histogram can be further chosen to be split, and so on until satisfactory construct enhancement effect is achieved. For the recovery of the original image, the location map is embedded into the host image, together with the message bits and other side information. So blind data extraction and complete recovery of the original image are both enabled. The generation of image histogram is a difficult and a time consuming process. But the contrast of the image is enhanced. The data is only hidden in the image where the security level is simple. Since the data is hidden and if the retrieving process is known the intruder will be able to retrieve the image easily without any effort.

A. Disadvantages in existing system

- High Computation time.
- Algorithm Complexity and distortion is high.
- Security is less because single key is used for the whole process.
- Generation of histogram is a difficult and time consuming process.

IV. 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. Thus in our project 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 three 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.

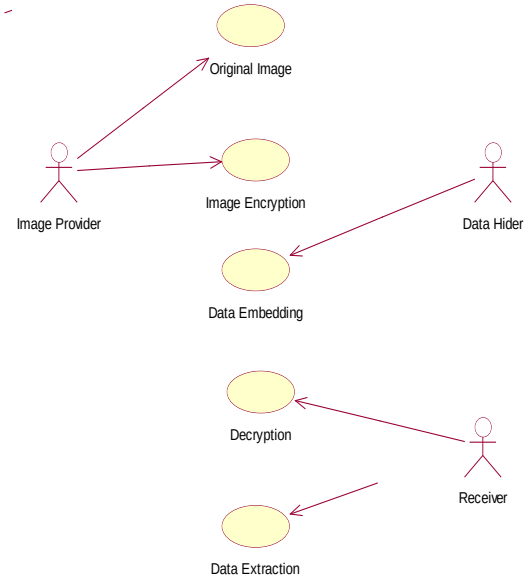

Fig. 1: Overall diagram of Image Encryption with hidden data

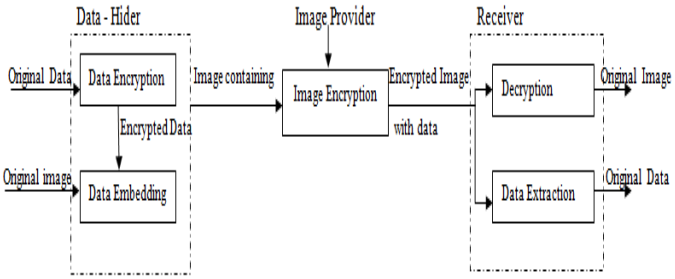

Fig. 2: Architecture diagram of proposed system

A. Collaboration Diagram

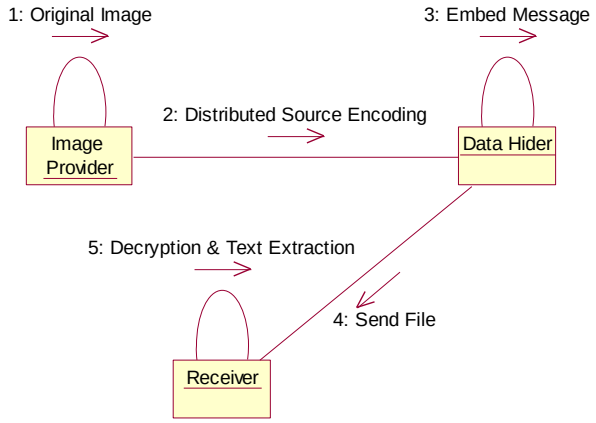

Fig. 3: Collaboration diagram

B. Advantages in proposed system

- 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.

C. Modules involved

1) Data Encryption and Hiding: In this module the user has to select the data which has to be embedded and the image in which the data is hidden. The data is encrypted using AES algorithm. Once the Embed button is clicked the data is encrypted and embedded in the image.

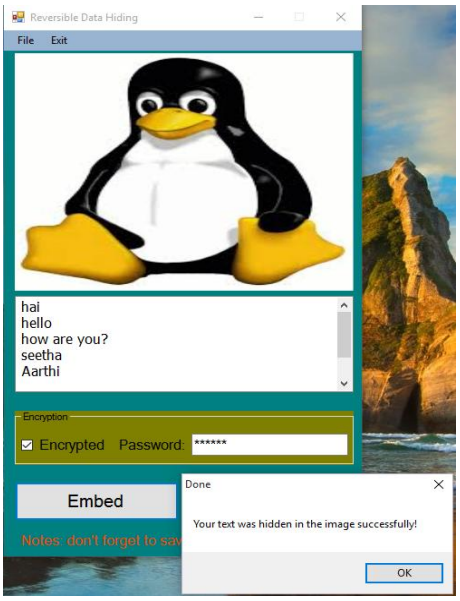

Fig. 4: The data is encrypted and hidden in the image.

1) *Image Encryption:* In this module the image with the hidden data is being encrypted. This encrypted image has to be saved in the local disk. A password has to be given manually to encrypt the image while that of data being default. The encrypted image is saved in .png (Portable Network Graphics) file format. When the image is tried to be opened it appears as a blank black image.

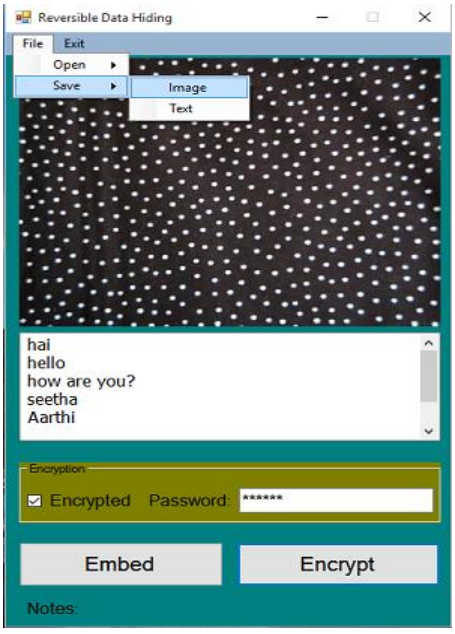

Fig. 5: The image is encrypted and it is saved.

2) *Retrieving Data and the Image:* If the intruder in the middle tries to open the image he may not be aware of the data hidden in the image as there won't be any traces of it in the image. The receiver one who has the data hiding key and the image encryption key will only be able to open the image and retrieve the data. Firstly the image is decrypted and then the data is retrieved from the image.

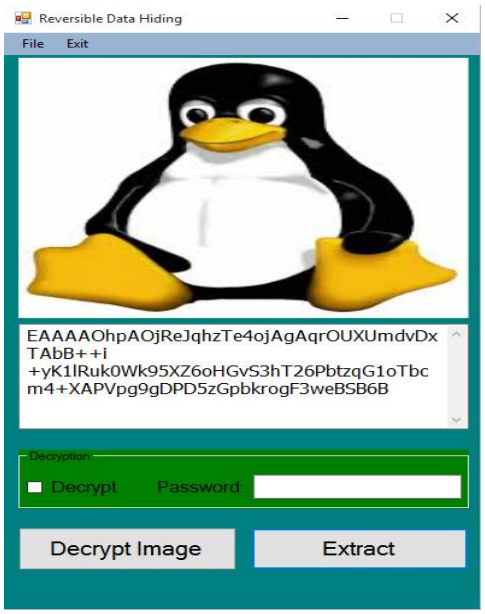

Fig. 6: Decrypt Image and Extract the data from the image.

Fig. 7: Decrypt t data and retrieve the original data.

V. 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. For example in the medical field where the patient report with its measures has to be sent to the doctor securely this system can be used.

ACKNOWLEDGEMENT

We are thankful and would like to express our sincere gratitude for our Head of the Department Mr. S. Venkatasubramanian and our supervisor Mr. P. Dineshkumar for the guidance, support and continuous encouragement in making this project possible. Their guidance from initial to final level enabled us to achieve our objective of final year project. Our sincere thanks to all the Lecturers who helped us in many ways, gave valuable advises and made our journey easy.

REFERENCES

[1] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process, vol. 19, no. 04, Apr 2010,pp. 1097-1102.

[2] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol, vol. 17, no. 6, Jun 2007, pp.774-778.

[3] J. Tian, "Reversible data embedding using a difference expansion," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 13, No. 8, August 2003. pp. 890 - 896.

[4] H. Guo, N.D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme", Multimedia Systems 9 (3) (2003) 249

[5] F. Hartung, J. K. Su, and B. Girod, "Spread spectrum watermarking: Malicious attacks and counter attacks", Proc. SPIE, vol. 3657, pp. 147–158, Jan. 1999.

AUTHORS

P Muthulakshmi
B.E., Computer Science and Engineering,
Saranathan College Of Engineering.

K Shathvi,
B.E., Computer Science and Engineering,
Saranathan College Of Engineering.

M Aarthi,
B.E., Computer Science and Engineering,
Saranathan College Of Engineering.

V Seethalakshmi,
B.E., Computer Science and Engineering,
Saranathan College Of Engineering.