ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Survey, Comparison and Discussion on Reversible Data Hiding Techniques

Megha Mohan[1], Anitha Sandeep[2]

M. Tech Student, Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Trivandrum, India[1]

Associate Professor, Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Trivandrum, India[2]

ABSTRACT: As the requirement of securing data (both image and text) has increased, novel approaches like reversible data hiding have been developed. Reversible data hiding is one among the many methods to securely store message into a cover image which cannot tolerate deformities. Separable reversible data hiding is an improvised method in which there are two key players: the content owner and the data hider. The former encrypts the original image with an encryption key while the later exploits the spatial correlation of the natural image to create an additional space to accommodate data. At the receiver side, receiver having the data-hiding key, can extract the data but not the original image. At the same time, the receiver with the encryption key, can extract the image but not the data. If he has both the data-hiding and the encryption keys, he can extract the data and the original image content. The efficacy of this method can be enhanced if the keys too can be secured. This can be done using a key-exchange algorithm like the Diffie-Hellman Key Exchange Algorithm. Also use of multiple encryption methods would make the system compatible with different applications. An authentication system and attack prevention measures, integrated along with the current version makes Separable Reversible data hiding a formidable method for data security.

KEYWORDS: Reversible data hiding, Separable reversible data hiding, Symmetric keys, AES, DES, Diffie Hellman key exchange.

I. Introduction

As we know the growth of data and its security are major research areas under consideration. There is a tremendous growth in the size of data being processed and also it is a tedious process for handling them. There are various methods used for securing the data which is transmitted through the shared medium. One such method is hiding the data into a cover media. The cover media may be of type text, image, audio or video. As the requirement of securing data (image and text) has increased, novel approaches like reversible data hiding have been developed which is an example for data securing method using image as the cover media. The method is reversible in nature as the original cover image can be recovered as such after the hidden message has been retrieved [3].

Reversible Data Hiding system is a non-separable method that is, the image and the data cannot be extracted independently. This results in less flexibility. In order to overcome limitation of previous system a new system was proposed which was both separable and reversible in nature.

Separable reversible data hiding is one in which there are two key players, the content owner and the data hider [1]. The former encrypts the original image with an encryption key while the later exploits the spatial correlation of the natural image to create an additional space to accommodate data. At the receiver side, receiver having the data-hiding key, can extract the data but not the original image. At the same time, the receiver with the encryption key, can extract the image but not the data. If he has both the data-hiding and the encryption keys, he can extract the data as well as the original image content. [1] Separable reversible data hiding technique can also be used by incorporating certain efficient algorithms like AES for encrypting both the image as well as the data. In this method, the data is given higher priority than the cover image used for embedding [2]. It uses Lossy compression technique to compress the image and hide the data within it.

DOI: 10.15680/IJIRCCE.2016. 0409096

The efficacy of this method can be enhanced if the keys too can be secured. This can be done using a key-exchange algorithm like the Diffie-Hellman Key Exchange Algorithm. Also use of multiple encryption methods would make the system compatible with different applications. The system, in its working environment, would come across various actors with different privileges. In such a situation, having an authentication system would ensure that the data is received at the right hands. An authentication system and attack prevention measures, integrated along with the current version makes Separable Reversible data hiding a formidable method for data security. In the following section, section II, a brief about the existing Reversible data hiding technique is given. Followed by is section III in which the Separable reversible data hiding technique is explained and then is section IV, dealing with Separable reversible data hiding using AES algorithm. Then is Section V, which is a discussion about how to improve the existing techniques and finally the conclusion which is Section VI.

II. REVERSIBLE DATA HIDING

Reversible data hiding (Fig 1)is one among the many methods used to securely store message into cover image which cannot tolerate any deformation, like sensitive images - military images or remote sensing images or medical images. This technique is to implant message into some cover media provided. After extracting the hidden message, the original cover image can be retrieved back perfectly [3]. Recently various types of reversible data hiding methods are advised. In Differential Expansion method, the deviation between a pair of nearby pixels are used to produce a new sparse space using the least significant bit (LSB) technique, this provides space for incorporating data which is to be stored securely.

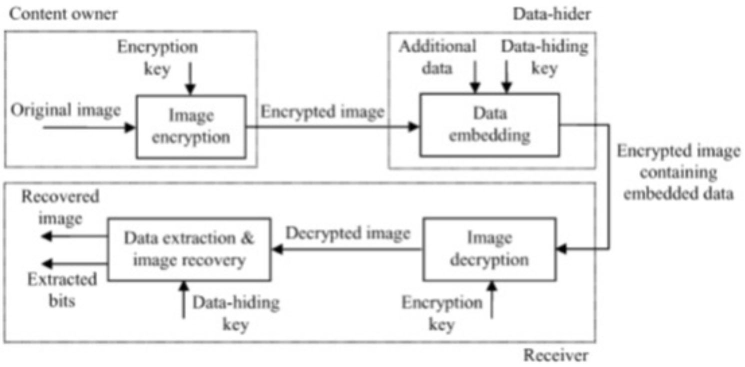

Fig.1. Reversible data hiding [3]

The person who intent to hide the data can use different methods like reversible data hiding which make use of histogram shift processes, which makes use of the zero as well as the peak points of the generated histogram of the image. There are also methods in which the redundancy in the cover image is utilized by carrying out lossless compression to generate the space required to accommodate the secret message. Also, different accomplishments have been introduced into the distinctive reversible data hiding method to increase the efficiency.

Advantages of Reversible data hiding technique is that, it helps to securely hide data within encrypted images and also security of the cover image is also considered. Disadvantage is that, this method is not separable i.e. both keys are required to retrieve the embedded data as well as the original cover image with desired resolution. Though various novel changes have been made in the reversible data hiding technique, due to some major drawbacks, another improved method was considered, which is Separable reversible data hiding [5].

III. SEPARABLE REVERSIBLE DATA HIDING

The term separable means something that is possible to separate [1]. In this concept, the separation of actions: decryption of the actual cover image and retrieval of secret (data which was embedded) takes place independent of each

other. The separation of actions is done based on keys available(Fig 2). At the destination, there are three different cases chanced during extraction : (a) cover image only, (b) payload only, (c) both payload and cover image [1].
Advantages of using this method is that, data and image can be separately recovered as this method is separable unlike basic reversible data hiding. Also it is more efficient, flexible and secure than reversible data hiding. Disadvantage is that, it do not consider about the security of the secret key used in the encryption and embedding of data.

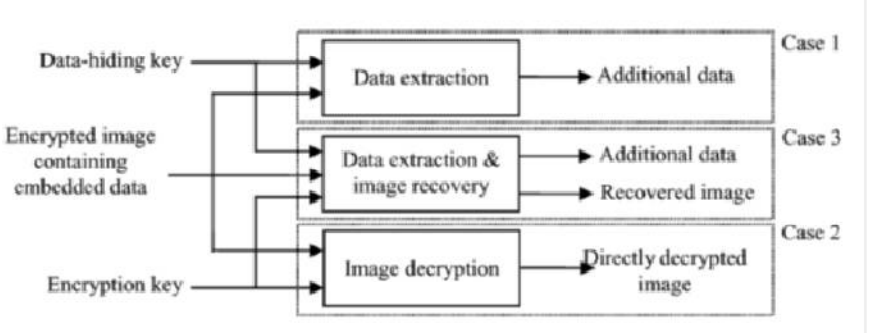

Fig.2. Separable reversible data hiding [1]

IV. SEPARABLE REVERSIBLE DATA HIDING USING AES ALGORITHM

In this method, the sender encrypts the data and may be hidden in any type of cover media like audio, video, text, document or image. First the data is taken and is encrypted using AES algorithm [2]. The image system would automatically generate the keys for encrypting the data as well as the image. The least significant bits (LSB) of the encrypted image is compressed to provide space for embedding the data. This is done using Lossy compression technique.

At the receivers end, the encrypted image, containing the encrypted data is obtained and is processed. If the receiver have both the data encryption key as well as the data embedding key, he can successfully extract the data but cannot get the image(Fig 3). If the receiver has the data embedding and the image encryption key, he would get the image as same as the original one with accuracy of about 80 percent, but cannot get the additional data [2].

If the receiver has all the three keys, i.e. the image encryption key, the data encryption key as well as the data embedding key, the receiver would be able to extract the original data, additional data, and also recover the original image similar to the original one. The various phases of this technique are: Registration, Image encryption, Data encryption, Data embedding, File sending, Image decryption, Data extraction and decryption.

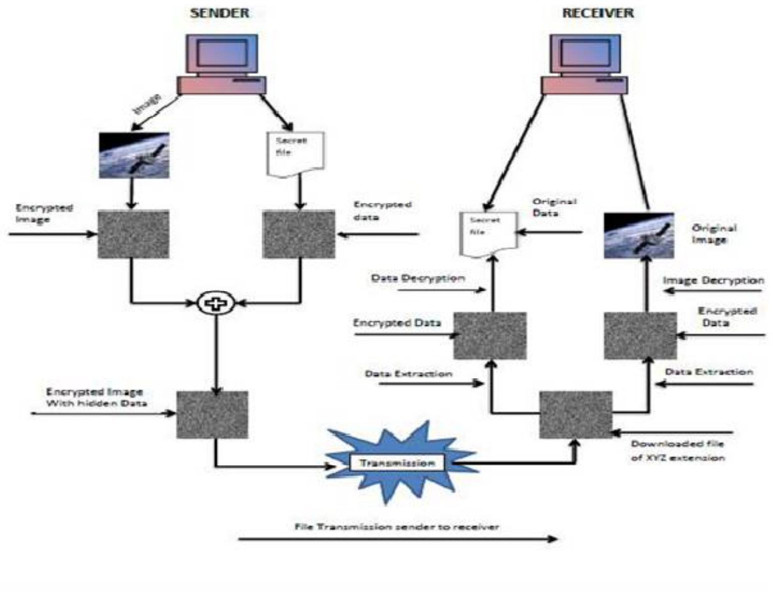

Fig. 3. Seprble reversible data hiding using AES algorithm[2]

V. DISCUSSION

As data hiding is an important activity in most of the highly secure applications like military, remote sensing data analysis and so on, it is important to identify a highly secure method. The method must be simple in its architecture as well as in the algorithms that it uses. More over it must be efficient and must satisfy the requirements of such sensitive applications. Separable reversible data hiding [1] is much more flexible than the reversible technique, and hence it can be used for a better security system.

The basic method does not encrypt the data to be embedded. Encryption standards like DES and AES algorithms can be used to encrypt data and make the basic system even more powerful. This may increase the security level and prevents data from being decrypted by a third person. AES algorithm though complex, it provides better throughput than DES algorithm. So these two algorithms can be used based on the application.

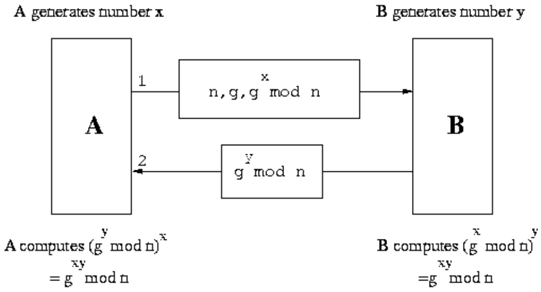
A generates number x
B generates number y
A
B
1
n,g,g^x mod n
2
g^y mod n
A computes (g^y mod n)^x = g^xy mod n
B computes (g^x mod n)^y =g^xy mod n

Fig.4. Diffie Hellman key exchange[8]

In the basic Separable data hiding technique, the symmetric keys used for encryption and the embedding keys used by the sender and the receiver is not shared through a secure way. For secure communication, the total number of keys required for n people is n(n-1)/2 which is equivalent to the number of possible communication channel. To prevent or to control the attacks of an eavesdropper, the keys should be kept safely, changed periodically and also distributed with care to the users. The process of doing the previously mentioned activities is known as key management. Key management is a tedious process as the reliability and security of the keys are at risk.

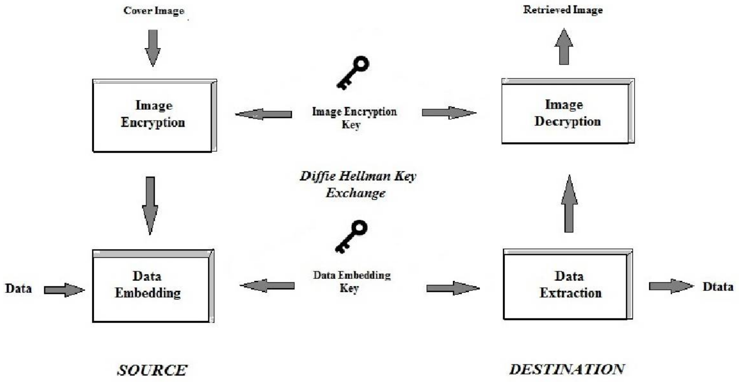

Fig.5. Block diagram of novel method

A Key exchange method like Diffie-Hellman key exchange can be used to share the symmetric key being used. This was chosen based on the survey considering the limitations of RSA key exchange method, [5] and it was found to be a better option for securely sharing the secret key as it is simple and efficient than RSA key exchange mechanism. The figure Fig.4 shows how the symmetric key required for encryption and embedding can be exchanged between the source A and the destination B using Diffie Hellman concept. Figure 5 is a basic block diagram of the enhanced system. It includes modules for encryption of image, embedding of data, extraction of data and decryption of image. A cover image and the data to be secured is given as input to the system and the data is recovered at the destination along with the cover image. Keys used for encryption and embedding are secured using a key exchange algorithm.

VI. CONCLUSION

Cryptography is the implementation and study of methods for the safe and reliable communication when there are threats and issues such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Using a method like reversible data hiding would help in secure transmission of data but they are not separable and hence not flexible.

Hence new methods like separable reversible data hiding can be used to make the system more easy to use and efficient. Integrating these systems along with some key exchange technique like Diffie -Hellman to secure the keys used for encryption and embedding, would help in secure transmission of data. Use of these would provide a mechanism which is much more secure and reliable compared to other existing methods.

Enhanced methods like Seperabale reversible data hiding using AES algorithm for encryption of data as well as image are secure but are computationally difficult. So they can be used as a trade-off between security and efficiency.

REFERENCES

1. Zhang, Xinpeng. ”Separable reversible data hiding in encrypted image.” Information Forensics and Security, IEEE Transactions on Vol.7.2 (2012): pp.826-832.
2. Kadam, Parag, et al. ”Separable reversible encrypted data hiding in encrypted image using AES Algorithm and Lossy technique.” Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on. IEEE, 2013.
3. Zhang, Xinpeng. ”Reversible data hiding in encrypted image.” Signal Processing Letters, IEEE Vol.18.4 (2011): pp.255-258.
4. Mithun Varghese and Teenu S Jhon. A Survey on Separable Reversible Data Hiding in Encrypted Images. International Journal of Computer Applications (0975 8887), Advanced Computing and Communication Techniques for High Performance Applications, 2014.

5. Bhatia, Ronak, et al. ”Separable Reversible Data Hiding In Encrypted Image.” Imperial Journal of Interdisciplinary Research 2.6 (2016).
6. Khader, Aqeel Sahi, and David Lai. ”Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol.” Telecommunications (ICT), 2015 22nd International Conference on. IEEE, 2015.
7. Anuradha, C., and S. Lavanya. ”Secure and Authenticated Reversible Data Hiding in Encrypted Image.” International Journal of Advanced Research in Computer Science and Software Engineering 3.4 (2013).
8. Deshmukh, Punam, and Reema Patil. ”Separable Reversible Data Hiding in Encrypted Image.”
9. http://www.cs.virginia.edu/evans/cs1120-f11/problem-sets/problem-set- 4-constructing-colossi.
10. http://www.howtogeek.com/howto/33949/htg-explains-what-isencryption- and-how- does-it-work.
11. https://en.wikipedia.org/wiki/Diffie
12. https://technet.microsoft.com/en-us/library/cc962035.aspx
13. http://all4ryou.blogspot.in/2012/11/network-securitycontd-part-2.html