



Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES Algorithm and BPCS Algorithm

Bhushan Sakate., Harshal Patil, Rohit Rakshe

Department of Computer Engineering,
Pune University, India

Abstract— Steganography basically was defined for the sending secrets message which hides in the image. The secrets message transmitted from one user to another user safely. In the previous system of hiding data in image uses the AES algorithm and Lossy techniques. But instead of this we use the AES algorithm and the BPCS technique. This gives security to the encrypted data which is embedded in the image. In this user encrypt the data and encrypt the image then embedded that data into the image and sends to the receiver very secretly we provide 2 keys at the time of image encryption and for data encryption. The both keys are uses same for Decryption process. User can decrypt the both image and data.

Keywords— Image encryption, Data encryption, Data decryption, Data extraction, AES and BPCS Algorithm.

I. INTRODUCTION

The steganography was basically used to hide the data into the image message. In the Secret communication the data get encrypted and the system auto generated the key. The encrypted data send to the receiver and the key send it privately. Steganography is the way of hiding the data into the message and cryptography was used to convert the normal data into the cipher form. But the steganography was more secure.

In the existing system the separable reversible data hiding in image having some limitations like less security to data and key. To overcome this limitations system proposes the separable reversible encrypted data hiding in the encrypted image using the AES algorithm and the BPCS Algorithm. BPCS algorithm was used instead of the lossy technique which was more powerful to hide the content into the image without changing the meaning of the image

Proposed system gives two keys for basically one for encrypted data and other for encrypted image. The encrypted data get embedded into the encrypted image using the BPCS technique. To overcomes the limitations of the previous system in new system we proposes the separable reversible encrypted data hiding in the encrypted image using AES algorithm and BPCS algorithm.

II. RELATED WORK

We currently use the AES algorithm for encryption process and the better security and it easily implemented on both the software and hardware. Previously system uses the DES triple DES algorithms for Data Encryption. DES algorithm consumes least time for decryption and provides security to the certain extent. So the AES algorithm overcomes on these limitations. AES uses the least memory for all this encryption process.

To overcomes the limitations of the previous system new system proposes the separable reversible encrypted data hiding in the encrypted image using AES algorithm. Which data having better security because it's to confidential. AES provides the better security and its uses the less memory at the time of encryption and decryption also.

The hardware implementation was to faster in the case of the AES algorithm. At the time of decryption it takes low memory time to decrypt. We can decrypt both image and data also. After decryption not 100% original image can get but it's sufficient to understand to the user.

The data which was hidden inside that image was decrypted with using the keys which provides at the time of the decryption. So using the separable reversible encrypted data hiding in the encrypted image improves the security to the data.

III. PROPOSED SYSTEM

Due to many limitations in existing system it provides less security to the data. So the in the proposed system we use AES and BPCS Algorithm for Better protection. We provide to keys basically two keys one for Image Encryption and the Second is For Data Encryption. In proposed system

In Proposed System at Sender side

A. Data Encryption

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

Recommended font sizes are shown in Table 1.

B. Image Encryption

The Data get selected which we want to encrypt using the AES algorithm. At that time Key provided by the user to that encrypted data for protection.

C. Embedding

Then encrypted data get embedded into the encrypted image using BPCS algorithm. Then the File was send to the Receiver and the both keys were sending privately to the receiver. If any third parties like hacker hack the conversation and get the image but without the Private keys it is impossible to decrypt the image and Data. The diagram shows the architecture of proposed system.

In Proposed System at Receiver Side:

A. Image Decryption

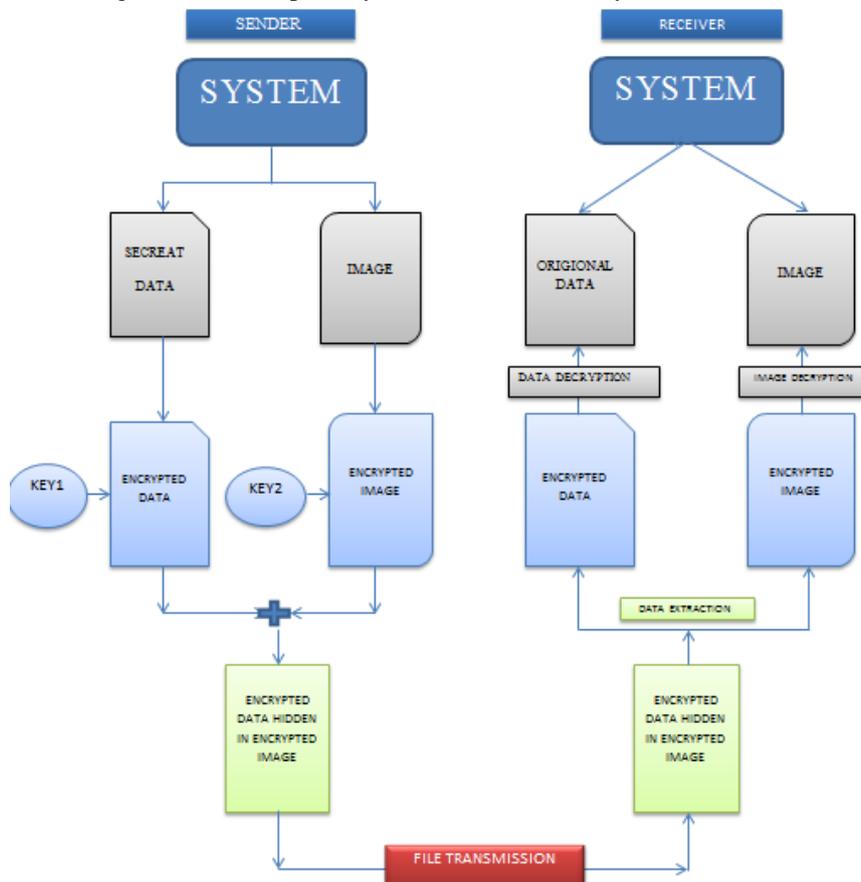
At the receiver end the user can decrypt the image with using key which is privately send by sender.

B. Data Decryption

User decrypts the data with using private key send by the sender.

C. Image or Data Decryption

User can decrypt either image or the data separately if he have both the keys.



IV. ALGORITHM USED

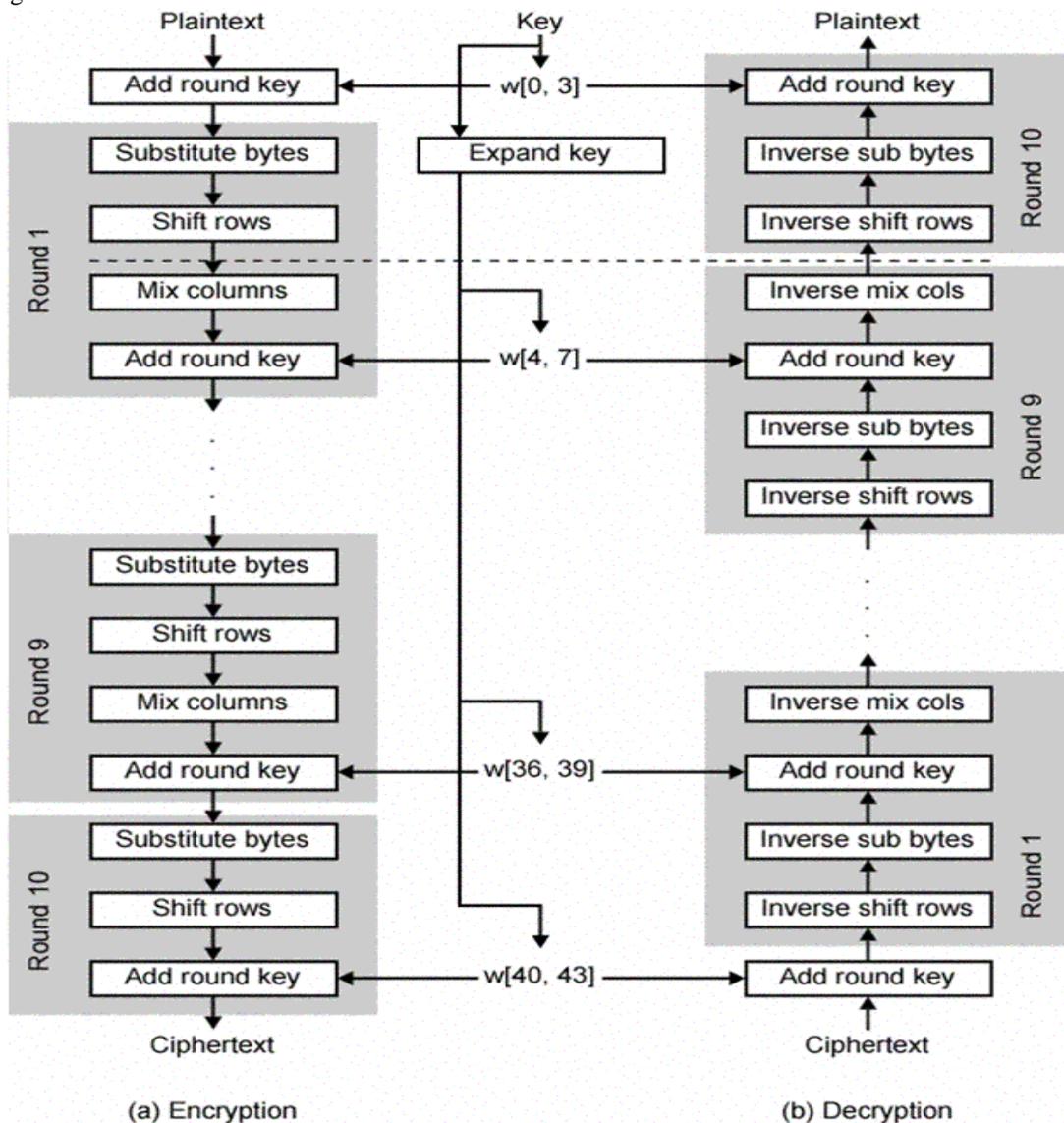
Following are the algorithms used in proposed system:

A. AES Algorithm

The AES is basically used for encryption. AES has key size 128 bit and key sizes 128 bit key, 192bit key and 256 bit key. This gives the better security to data with using advance encryption technique.

- 1) *Sub byte transformation:* In the subtype transformation the each byte get substitute with the lookup tables. Lookup table was standard taken here which contain the value of specific byte.
- 2) *Shift rows transformation:* In this each rows on the matrix gets shifted as its level cyclically. This was not the bitwise shift. The second byte after shifting it was in third position. The forth byte after shifted one space it comes to the first position in same row.
- 3) *Mix rows transformation:* In mix columns each columns the four bytes are added. The multiplication is performed one matrix row at a time against each value of a state column.

4) Add round key transformation: At the end of the round the round key get added to it. to make the encryption more complex. So it cannot get easily decrypted. In the final round of the AES add round key transformation was neglected



B. BPCS Algorithm

- 1) In the proposed system, the BPCS algorithm is used to hide the encrypted data into the Encrypted image. At the time of steganography separate each pixel RGB bit and then create the 8*8 matrix and calculate the alpha value known as Complexity.
- 2) Calculating the alpha value shows that given matrix is capable of hiding some bit or not. The standard alpha value is 0.3 taken here. For calculating alpha we use Formula = (Horizontal transitivity * vertical transitivity) / max transitivity. If the alpha value is less than 0.3 then we don't hide bits in this matrix just neglecting that.
- 3) If alpha value is greater than the 0.3 then we simply hide the in that matrix and calculate again the alpha value. If the alpha value is less than 0.3 then changing the first bit as 1 otherwise its 0. So finally we get the Encrypted Stegano Image.
- 4) At the time of Desteganography we just check the first bit of the 8*8 matrix if it is 0 then we take data as it is. If it's 1 then we EXOR this matrix with the standard chessboard to get the decrypted image.

V. SYSTEM FEATURE

The proposed system features are as follows

A. Two keys For Security

One key for the Data Encryption data and the other for the Image Encryption. Both Keys are required for decryption.

B. User Defined Key

System does not auto generate the key. User can give the key as he wants which is able to recall or easy to remember.

C. User Defined Extension to file

Its prevents the file from the external attack like hacker attack. User gives the extension like .abs or .xyz

VI. CONCLUSIONS

The study helps to prevent the secure data transmission. The algorithm which is used in the proposed system gives the better security to the secret data. Instead of lossy technique BPCS Algorithm is used for better security. The BPCS algorithm is used because of this it is more difficult to extract the data from the Image. Without both keys it is impossible to get decrypt the image and data. AES Algorithm was Provide more security that's why we uses for encryption. In the future be we can use audio and video to hide our secret data.

ACKNOWLEDGMENT

We deeply thank our HOD Prof. Babar for his useful guidance. We also thank our Project Guide Prof. N.K. Patil without whom this project would have been a distant reality. We also thank them for giving us support, timely guidance and discussion in all phases of the project.

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] Hoang Trang and Nguyen Van Loir HoChiMinh City, VietNam- "An efficient FPGA implementation of the Advanced Encryption Standard algorithm" (IEEE 2012) Shrihari Ahire, Vishakha Panjabi, Rahul.
- [3] X. Zhang, "Reversible Data Hiding in Encrypted Image" IEEE signals processing letters, vol. 18, no. 4, pp. 255-258, April 2011.
- [4] Kawaguchi, Eiji; Eason, Richard (1999). "Principle and applications of BPCS-Steganography" (<http://www.eece.maine.edu/~eason/steg/SPIE98.pdf>). Proc. SPIE 3528, Multimedia Systems and Applications, 464. Conference Volume 3528, November 01, 1998. doi:10.1117/12.337436 (<http://dx.doi.org/10.1117%2F12.337436>). Retrieved 3 April 2013.