High-capacity reversible data hiding in encrypted images based on extended run-length coding and block-based MSB plane rearrangement

Mahesh Sanjay Chavan

Professor.Shrawani Pawar Mam

Bharti Vidyapeeth Institute of Management and Information Technology ,Cbd Belapur,Navi Mumbai

***Abstract*— In this paper, we propose a different scheme which attains real reversibility by reserving room before encryption with a traditional RDH algorithm, and then encrypting the data and embedding the data in the encrypted image, We used some solid encryption techniques which is efficient. We also removed the data hider from the image process. The proposed method can achieve real reversibility that is data extraction and image recoveries are free of any error.**

***Keywords*— RDH, Image Partition, Watermarking. embedding capacity**

1. INTRODUCTION

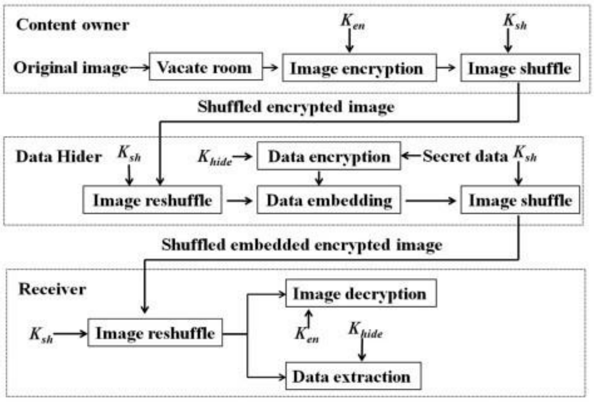
Reversible data hiding in images is a technique by which he original cover can losslossely recovered after the embedded messages are extracted. This important technique is widely used in medical imaginary, military imaginary and law forensics ,where no distortion of originalcover is allowed. since first introduced, RDH has attracted considerable research interest.

2. Existing system

Existing system proposed design a block-based MSB plane rearrangement (BMPR) scheme which transforms the MSB planes of the original image into high compressible bit streams, and an extended run-length coding which compresses the transformed bit streams at a high compression ratio.

1. Based on MSB plane compression, they present anRRBE RDHEI method. The method can achieve high embedding capacity and high quality of the marked decrypted image. Data extraction and image recovery of the method are separable and error-free.
2. Based on BMPR scheme and the extended run-lengthcoding, the joint-embedding, room-vacating scheme can be performed to vacate room in LSBs for embedding data. The procedure of the joint scheme. Based on the joint embedding-room-vacating scheme, the data owner can make room for the data hider to embed data in encrypted images.

1. Encryption and decryption process is describe is the below figure.



3. Proposed Reversible Watermarking Scheme

SchemeIn the existing system, they hadn't specified any encryption techniques which is robust and efficient and they also didn't specified any key size. In this advanced reversible data hiding method, encrypted data can be embedded and extracted from both encrypted images.The data is encrypted using AES algorithm and image is encrypted using the Blowfish algorithm. It inserts authentication information in multimedia data which can be used as proof of ownership.The proposed work includes: generation of encrypted data, generation of encrypted image, data embedding, data extraction and image recovery.

3.1. Generation of Encrypted data: The secret data is encrypted using the AES algorithm. Run length encoding is performed to compress the secret information and then this information is encrypted using AES algorithm. This table may be derived from the input itself or from data which is representative of the input. AES is based on a design principle known as a substitution permutation network, combination of both substitution and combination, and is fast in both software and hardware.

3.2. The key size used for an AES cipher

Specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the finaloutput, called the ciphertext.The proposed work utilizes the 128-bit key size of the AES algorithm. Each round consists of four processing steps in which the first step is the substitute byte step and next is the shift row transformation, third is the mix column transformation and last step is the addroundkey transformation step.A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

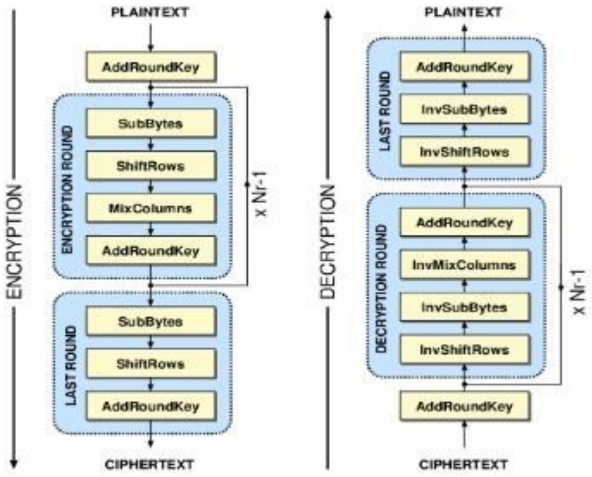


Fig 1: AES Encryption and Decryption

3.3. Generation of Encrypted image: The next step after data encryption is image encryption which is done using Blowfish algorithm. Blowfish is a 64-bit symmetric block cipher that uses a variable-length keyfrom 32 to 448-bits (14 bytes). The algorithm was developed to encrypt

64bits ofplaintext into 64-bits of cipher text efficiently and securely. The operations selected for the algorithm were table lookup, modulus, addition and bitwiseexclusive-or to minimizethe time required to encrypt and decrypt data on 32-bit processors. Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified unlike DES which only modifies the right 32-bits to become the next round's left 32-bits. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation

4. CONCLUSION

An advanced RDH scheme with encrypted data has been presentedin this paper. This work combines data encryption with image encryption. The two main algorithms implemented for data encryption and images encryption are the Advanced Encryption Standard (AES) algorithm and the Blowfish algorithm.

5.FUTURE SCOPE

The RDH technology is quite useful for some special applications in which images are not allowed to be disturbed, such as military, medical, and law forensics applications.

6.REFERENCES

[1]Kede Ma, Weiming Zhang, Xianfeng Zhao, Member,IEEE, NenghaiYu, and Fenghua Li"Reversible Data Hiding in Encrypted Images byReserving Room Before Encryption" ieee transactions on information forensics and security, vol. 8, no. 3, march 2013.

[2] M. Goljan, J. Fridrich, and R. Du, "Distortion-free data embedding," in Proc.4th Int. Workshop on Information Hiding, Lecture Notes inComputer Science, 2001, vol. 2137, pp. 27–41.

[3] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[4] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in Proc. Security and Watermarking of MultimediaContents IV,Proc. SPIE, 2002, vol. 4675, pp. 572–583.

[5] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003

[6] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," IEEE Trans. Image Process., vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[7]Ratinder Kaur, V. K. Banga "Image Security using Encryption based Algorithm" International Conference on Trends in Electrical, ElectronicsandPowerEngineering (ICTEEP'2012) July 15-16, 2012 Singapore. [8]Pia Singh Prof. Karamjeet Singh "Image encryption and decryption

using blowfish algorithm in matlab" International Journal of Scientific & Engineering Research, Volume 4,Issue 7, July-2013 150 ISSN 2229-5518.

[9]Prachi V. Powar , Prof. S.S.Agrawal "Designof digital video watermarking scheme using matlab simulink"PRACHI V POWAR* et al ISSN: 2319 1163Volume: 2 Issue: 5 826 830 IJRET, MAY 2013.