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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

An Approach to Embed Secret Data over Secured Reversible Image Using Lossless Compression Technique

Priya S[1], Dharun Praveen[2], Rohit S[3]

Assistant Professor, Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, Coimbatore, India[1]

UG Scholars, Department of Computer Science and Engineering, Nehru Institute of Engineering and Technology, Coimbatore, India[2,3]

ABSTRACT: Recently, more number of data is paid with the Reversible Image Data Hiding, derived from the original data. The methods can embed the process through the standard of AES algorithm. The protocols which are rooted and a particular portion are been selected from the original image. The traditional RDH algorithm, thus provide the encrypted data values from the reversible data without the key generation. The encrypted data are been processed through the direct flow of bins with the lossless compression technique.

KEYWORDS: Reversible Image, Data Hiding, Lossless Compression, Cipher text, Advanced Encryption Standard, Image-Recovery.

I. INTRODUCTION

Information processing in the encrypted domain has attracted considerable research interests in recent years [1]. In many applications such as cloud computing and delegated calculation, the content owner needs to transmit data to a remote server for further processing. The service provider must be able to do the processing in the encrypted domain. The encrypted images are the redundant of the original image which cannot be used directly after image encryption. Encrypted images since the redundancy in the original image cannot be used directly after image encryption [2]. The hidden data can be completely withdrawn using the embedding key, and the original image can be approximately reorganized with high quality using the encryption key. Many reversible data hiding methods have been proposed recently [5]–[9]. [5] Embeds data bits by expanding the difference of two consecutive pixels. [6] Uses a lossless compression technique to create extra spaces for carry data bits. [7] Shifts the bins of image histograms to leave an empty bin for data embedment. [8] Adopts the difference expansion and histogram shifting for data embedment. The embedded carriers are further encrypted to prevent the carrier from being analysed to reveal the presence of the embedment [10]–[12]. The data hider to embed secret data into an encrypted image without knowing the original image content, where the encrypted image is generated by the content owner [13]. The content owner encrypts the original image for privacy protection, for the cloud provider or administration, he may hope to append some data into the image for labelling or classification, and he has no right to access the original image. Data extraction and image recovering are accomplished by comparing the estimation error. The original image are randomly selected and estimated by their surrounding pixels, secret data bits are embedded into the encrypted estimation errors. Encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission and the typical reversible data hiding approaches to improve the performance [15]–[16].Encryption is an effective and popular means of privacy protection. In order to securely distribute a secret image among others, a content owner may encrypt the image before transmission. The data of original cover are entirely encrypted, and the additional message is embedded by modifying a part of encrypted data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

II. RELATED WORK

The data-hider enters access the image content, and the secret message is held by the data-hider. The idea was first proposed by Puech et al. [3], in which the owner encrypts the original image by Advanced Encryption Standard (AES), and the data-hider embeds one bit in each block include n pixels, meaning that the embedding rate is 1/n bit-per-pixel (bpp).On the receiver side, data extraction and image recovery are actualise by analysing the local standard deviation during decryption of the marked encrypted image. Zhang proposed a practical RDH method for encrypted images in [4], in which the data-hider divides the encrypted image into blocks and embeds one bit into each block by flipping three least significant bits (LSB) of half the pixels in the block. On the receiver side, the marked encrypted image is decrypted to an estimate image. The original block is presumed to be much smoother than interfered block. Thus the embedded bits can be extracted and the original image reclaim jointly. Embedding rate of this method depends on the block size. The data hider then embeds the secret data into the encrypted estimation errors using the data hiding key and scrambles the image using the sharing key [13]. With an encrypted image containing additional data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image.

III. IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving the users confidence that the new system is workable and effective. Implementation of a modified application to substitute an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system. Each program is tested individually at the time of development using the data and has establish that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user.

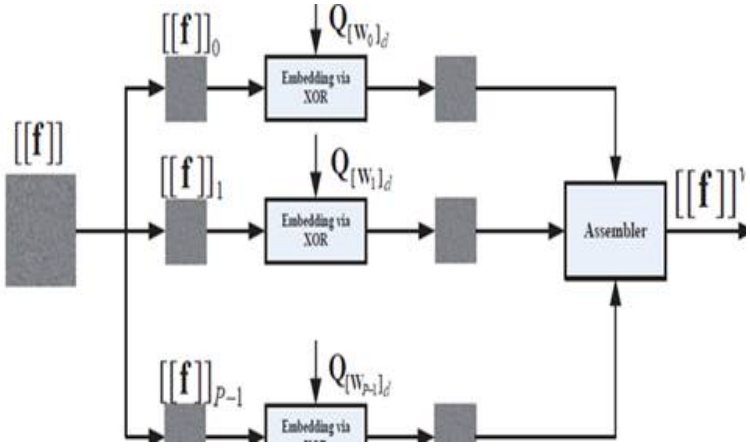

Fig. 1 Architecture

And so the system is going to be execute very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. Implementation is the stage of the project when the theoretical design is emerge into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The effective phases:

(a)Encryption: In this module the cipher text is generated by the bitwise XOR ing the plain text with the key stream. If this is not suitable means the widely used algorithm AES is used to encrypt the plain text. The original and the encrypted image are taken into account, where the encrypted image acts as the cover to accommodate the message to be hidden. Then the message where embedded over the image blocks.

(b)Feature Selection: In this module the feature selection process takes place on both the encrypted and non-encrypted image block. On comparing the feature sets of both the un-encrypted block of original, the unencrypted block have much more uniform distribution. The feature selection is mainly to identify the original and encrypted image difference. The feature selection allows classification based on their feature sets.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

(c)Data Extraction: The decoder in the data centre has the decryption key and tries to recover both the embedded image and the original image. This is done using the XOR operation. Separating the image and message will be helpful to obtain the original text.

(d)Image Decryption: The decryption is done using the key obtained using the AES algorithm. The cipher text is decrypted using the key to generate the original text. The key used for decryption is the identified public key. This allows the user to read or get the original text.

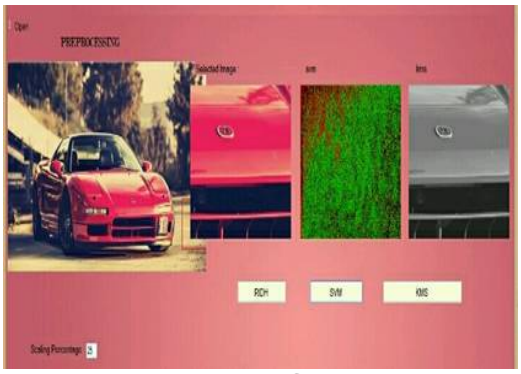

Fig. 2 Image Conversion

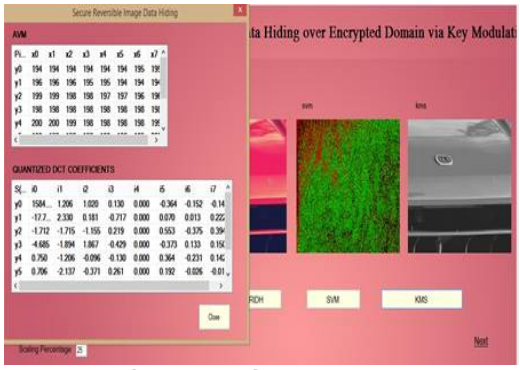

Fig. 3 Decryption Conversion

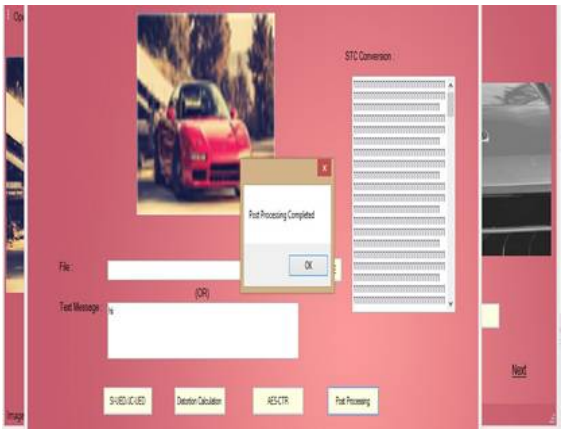

Fig. 4 STC Code

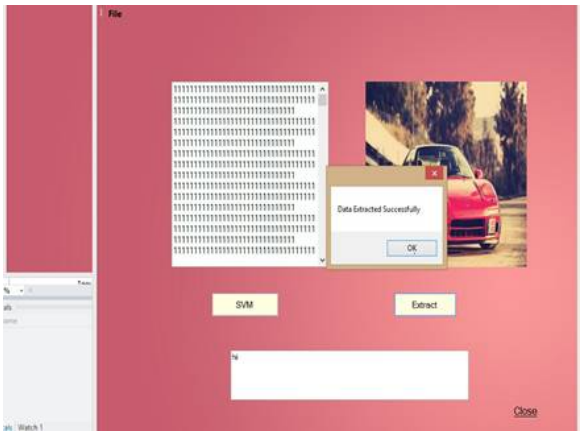

Fig. 5 Output

The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover methods.

IV. CONCLUSION AND FUTURE WORK

After encrypting the original image with a stream cipher, some bits of MSB planes are choose and compressed to make room for the additional secret data. Embedding operations are performed to the encrypted data, the data-hider cannot entry the contents of the original image. That ensures security of the contents in data hiding. The encryption and embedding keys, an adversary is unable to break into the system without these keys and the encoding technique is classified with estimate half of the pixels in the original image to obtain the estimation error values for embedding the secret data, so that the maximum embedding rate can be significantly improved. A novel reversible data hiding scheme for encrypted image with a low computation complexity is proposed, which reside in image encryption, data embedding and data- extraction/image-recovery phases. The data of original image are entirely encrypted by a stream

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

cipher. With an encrypted image carry embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image

REFERENCES

1. Z. Erkin, A. Piva, S. Katzenbeisser, et al., 'Protection and Retrieval of Encrypted Multimedia Content: When Cryptography Meets Signal Processing', EURASIP Journal on Information Security 2007, 2008.
2. ZhenxingQian, Xinpeng Zhang, 'Reversible Data Hiding in Encrypted Image with Distributed Source Encoding', IEEE Transactions on Circuits and Systems for Video Technology, 2014.
3. W. Puech, M. Chaumont and O. Strauss, 'A reversible data hiding method for encrypted images', Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 68191E, Feb. 26, 2008, doi:10.1117/12.766754.
4. X. Zhang, 'Reversible data hiding in encrypted images', IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
5. J. Tian, 'Reversible data embedding using a difference expansion', IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, 2003.
6. 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, 2005.
7. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, 'Reversible data hiding', IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 8, pp. 354–362, 2006.
8. D. M. Thodi and J. J. Rodriguez, 'Expansion embedding techniques for reversible watermarking', IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, 2007.
9. W. Hong and T. S. Chen, 'Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism', J. Vis. Commun. Image Represent., vol. 22, no. 2, pp. 131–140, 2011.
10. D. Kundur and K. Karthik, 'Video fingerprinting and encryption principles for digital rights management', Proc. IEEE, vol. 92, pp. 918–932, 2004.
11. 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, pp. 774–778, 2007.
12. M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, 'A commutative digital image watermarking and encryption method in the tree structured haar transform domain', Signal Process.: Image Commun., vol. 26, no. 1, pp. 1–12, 2011.
13. W. Hong, T-S.Chen, and C-W. Shiu, 'Reversible data hiding for high quality images using modification of prediction errors', Journal of Systems and Software, vol. 82, no. 11, pp. 1833 – 1842, 2009.
14. Xinpeng Zhang, 'Reversible Data Hiding in Encrypted Image', ,IEEE Signal Processing Letters, vol. 18, no. 4, April 2011.
15. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, 'Reversible image watermarking using interpolation technique', IEEE Trans. Inf. Forensics Secur., vol. 5, no. 1, pp. 187–193, 2010.
16. W. Hong, T.-S.Chen, Y.-P.Chang, and C.-W. Shiu, 'A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification', Signal Process., vol. 90, pp. 2911–2922, 2010.
17. C.-C. Chang, C.-C.Lin, and Y.-H. Chen, 'Reversible data-embedding scheme using differences between original and predicted pixel values', IET Information. Security, vol. 2, no. 2, pp. 35–46, 2008.