I J C T A, 9(16), 2016, pp. 7855-7860

Reserving Room before Encryption using Reversible Data Hiding in Images

Neha Mishra and C. Santhana Krishnan

ABSTRACT

Recently additional attention is remunerated to the reversible data hiding (RDH) technique in encrypted images, as it maintains tremendous property that inventive cover can losslessly improved after embedded information is extracted as image protecting content's secrecy. All preceding methods embed information through reversibly vacate room from encrypted image, which can be few errors on image restoration and/or information extraction. We suggest diverse method which achieves real reversibility through reserving room ahead of encryption by traditional reversible data hiding algorithm, and embedding data and encrypting data in encrypted image. This scheme is still improved by encrypt messages with symmetric key technique. This is a cause new security method called RDH arises. The information hiding technique employs adaptive LSB substitute algorithm for covering secret information bits into encrypted image. In data extraction section, secret information will extracted with significant key for selecting encrypted pixels for extract data. Through decryption keys, image along with extracted text information will extracted. Lastly proposal performance in data hiding and encryption will be examined based on data recovery and image. The proposed technique can accomplish factual reversibility that is image recoveries and data extraction error free. The RDH technique utilizes reserving room procedure and it diminishes error and attains real reversibility. Data hiding methods are comparing and discus by reserving room procedure. Experiments demonstrate that novel technique may embed above 10 times huge payloads for similar image quality as previous techniques.

Keyword: RDH, vacate room, reserving room, Image recovery

1. INTRODUCTION

The digital system for storing and transmitting multimedia data are escalating, it is flattering an important concern how to defend their confidentiality, authenticity and integrity of images [1]. By using few encryption methods copying the data require to be controlled. Nevertheless encryption not gives overall security. Once encrypted information is decrypted, they able to freely manipulated or distributed. This issue can be resolved by hiding little ownership information into multimedia information which able to extracted afterward to establish ownership. The majority work on reversible information hiding focus on data extracting/ embedding on basic spatial field. This technique by keeping room before encrypts data with conventional RDH algorithm [2], thus it's simple for hiding information to reversibly implant data in encrypted image. The various works on data activity in encrypted domain are there. The reversible data activity in the image of encryption is investigated. Most work on reversible data activity focus on data extracting / embedding on simple spatial field. This method [3] by reserving room before encrypting with standard RDH decree and consequently it's easy for data hiding to reversibly include data inside encrypted image. Projected method can do valid changeableness that image recovery and information extraction square measure untied as of any error [4]. The data hider will similar to additional area vacant move into before step to form information activity method simple. The projected method will formulate the most ancient RDH method for basic pictures and distribute the goods magnificent performance whereas not secrecy loss. Additionally, this novel method can do valid changeableness [5], separate data extraction and significant improvement on

* Department of Information Technology, SRM University SRM Nagar, Potheri, Kattankulathur, Kancheepuram, Tamil Nadu, *Email: neehaa123mishra@gmail.com*

standard distinct decrypted pictures. Experiments illustrate that this method will include fairly ten times like immense payloads for matching image quality as before strategies [6]. The image recovery and data extraction may be accomplished by investigating the block effortlessness. When encrypting complete associate data extent uncompressed image through stream cipher, extra data embedded into image with varying small quantity of encrypted data [7]. With correlate extent encrypted image enclosing extra data, one may foremost interpret it discrimination encoding key, also decrypted edition is similar to initial image. Observing with information hiding key, through spatial correlation help in normal image, embedded data can be extracted also original image can be completely recovered.

2. RELATED WORK

[8] The Reversible information hiding methods are utilized to protection purpose. Corresponding the secret information from one consign to other consign is very complex, as so several attackers can slash the data. This study mostly compact with security problems in network and different reversible data hiding technique match up with keeping room procedure. The preceding techniques are initially vacating room as of encrypted images. It generates many errors in data extraction. The Reserving room procedure is initially preserve room for embedded information and encrypts image. It accomplishes tremendous performance. The Real reversibility is attained and decrypted image quality also increased [9]. RDH method with encrypted information obtained within this paper. This exertion combines information encryption with an image encryption. Two major algorithms employed for images encryption and information encryption are AES (Advanced Encryption Standard) and Blowfish algorithm. Exertion instigates with information encoding stage which is executed by utilizing Huffman encoding technique to compress the information. The next stage is information encryption which is achieved by using AES and after this image will encrypt by using Blowfish technique which is extremely secure owing to its key length and fastest and strongest nature in the data processing when compare to further algorithms. Distant from information hiding in image, the future work also presents information hiding in the videos which obtain this exertion to new-fangled level in advanced RDH method. [10] The paper obtained that image protection quality and hidden information during communication based on reserve room method and also chaotic crypto scheme by LSB based information concealment. Here, exciting wavelet transform used to store space for covering data efficiently and the chaos encryption used to keep image contents. This scheme was produced stego-image by less error below most data hiding capability. Finally, system performance was estimated with excellence metrics like as SNR and error factor. It betters well-suited approach and better efficiency with flexibility rather than prior method. [11] Newly information hacking is extremely big issue arising in network field. Extra attention is agreed to reversible information hiding RDH method in the encrypted images. RDH preserves excellent possessions that original envelop can improved losslessly later than embedded information is extracted. RDH presents image content's, confidentiality and security. Space allotment for embedding data within an image can do before or after image encryption. Previous survey techniques regard all merits, demerits. [12] Kede Ma, et.al, describes reversible information hiding in encrypted images through means of spare space when reserving room earlier than encryption. Extra attention is agreed on RDH method which is dependable for reversibility i.e. original envelop can be lossless recovered. It presents security and confidentiality to user. Room reservation is achieved before encryption. An advantage of proposed scheme sustains additional room for embedding information in information hider module. System accomplishes excellent recitals with no data loss. Vinit Agham et. al. [13], explained Separable Reversible Data hiding method. The author first encrypt image then information is hidden using information hiding key. Information can be either image or text so in like state hiding data image into envelop image may be problem.

3. PROPOSED WORK

The conventional RDH techniques take advantage for simple images and accomplish excellent recital perfect secrecy with no loss. This technique can accomplish separate data extraction, real reversibility and significant quality improvement of decrypted images. The proposed method reserve the room first afterwards

encrypts the data by using traditional RDH approach. Through this approach hide the data easily. We can accomplish real reversibility, image recovery and data extractions are error free.

3.1. Reversible Data Hiding

Reversible information hiding is incredibly useful for few extremely image like military images and medical images. In reversible data hiding system, few schemes are excellent recital at hiding capability but have terrible stego image eminence, some methods are excellent stego image eminence but have stumpy hiding capacity. It's complex to get balance between hiding capability and quality of stego image. The traditional reversible data hiding system is proposed. Projected system utilize novel embedding technique, which is described Even-Odd embedding technique, to maintain quality of stego image in an suitable level, utilize multi-layer of embedding to enhance the capacity of hiding.

AES Algorithm

```
void Cipher(byte[] i, byte[] j, byte[] k) {
    byte[][] status = new byte[4][Nb];
    status = i;
AddRoundKey(status, k, 0, Nb - 1);
    for (int q = 1; round < Nq; q++) {
        SubBytes(status);
        ShiftRows(status);
        MixColumns(status);
        AddRoundKey(status, k, round*Nb, (q+1)*Nb - 1);
    }
        SubBytes(status);
        ShiftRows(status);
        AddRoundKey(status, w, Nq*Nb, (Nq+1)*Nb - 1); j = status;
    }
```

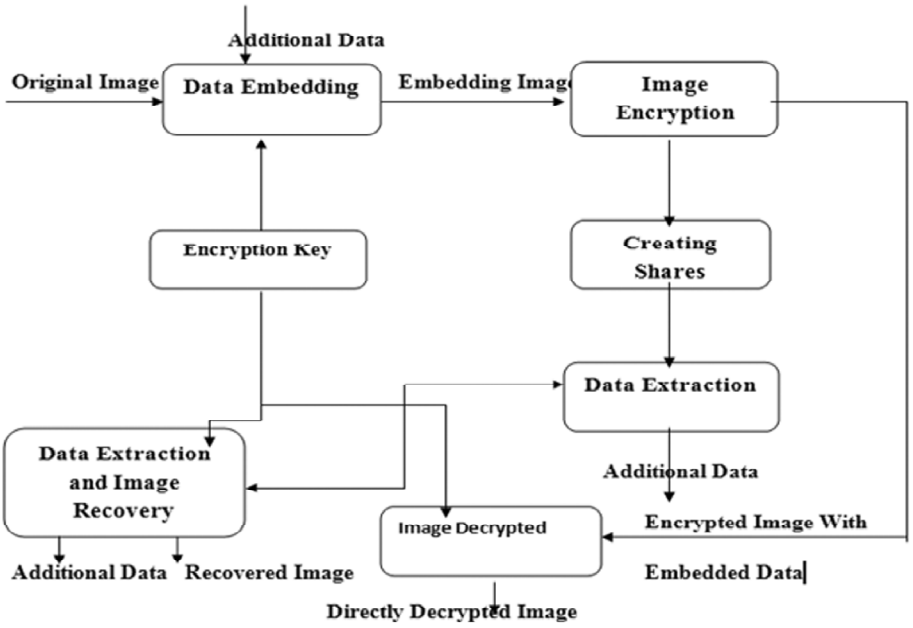

Figure 1: Overall Architecture

3.2. Data Embedding and LSB (Least Significant Bit)

This sector describes about embedding information for surreptitious sharing. It obtain single random encrypted image. The Watermark provides the provider identification. Here we utilize LSB technique for the data embedding. We encrypt data before data hiding using secret key.

3.3. The Embedding Technique Of Watermark Is Given As Follows:

1) Assume host image size 512 × 512. The Host image separated into diminutive M × M in blocks Z, that divided into diminutive M × M in Y blocks. If the M = 8 is utilize, Y block size is the 8 × 8.
2) Number of coefficients pairs (I, J) in Y block choose I = i1, . . . , in, J = j1. . . jn derived from mapping key and pseudo random number that contains original index selected coefficients reserved.
3) For embedding, the two coefficient value (ak, bk) are adapted by insert watermark strength parameter. k = 1, …, n.
4) Continue exceeding procedure according to the n. Each Y block is implanted 1 bit watermark as well as its length choosing how many Y blocks embedded.

3.4. Data Protection

- Image recovery is an intensive computationally and save energy from offloading. To handle confined data, image retrieval can be customized; modified program should provide suitable retrieval recital compared with unprotected original program data. Dissimilar retrieval technique may require dissimilar protection methods. We regard two retrieval methods: Gabor filtering and ImgSeek, two security methods homomorphism and Steganography encryption. Steganography utilize wrap image to mask secret image consequently that is hard to detect.
- A common and simply worn image Steganography method is hiding image through replacing bits as cover image among bits from secret image. Encryption converts plain information to build them unreadable. The Steganography is dissimilar starting encryption: earlier hides existence information. In contrast, the encryption formulates the data pointless without key. ImgSeek may perform on the Steganography information based on feature extraction linear property.
- Nevertheless, ImgSeek presume images with same orientations and scales. Gabor filter have more accuracy than the ImgSeek for incisiving similar images through rotated objects. While using Gabor filter, Steganography not appropriate to defend data anymore, as Gabor feature extraction not explaining linear properties. The homomorphism encryption may be utilized in the Gabor retrieval, as it mostly achieves multiplications and additions on encrypted information.

3.5. Extracting Data from Encrypted Images

To control and modernize personal information images which encrypt for defensive clients' privacy, inferior database administrator may only obtain access to information hiding key also have to control information in encrypted domain. Data extractions order ahead of the image decryption feasibility guarantee of work.When database administrator obtains information hiding key, user able to decrypt LSB-planes then extract additional information with directly read decrypted edition. When appealing for modernizing encrypted images information, database administrator renews information by LSB alternative and encrypts efficient in sequence according to information hiding key over. As entire process is operated on the encrypted field, it avoids original content leakage.

3.6. Extracting Data from Decrypted Images

Both extraction and embedding data are controlling in encrypted field. There is dissimilar condition that user needs to decrypt image and extracts information from decrypted image while it is required. The following

model is an appliance for scenario. Imagine Alice subcontract her image to cloud server, images that encrypted to keep their contents. Cloud server embeds the image with identity of time stamps to maintain encrypted image. The cloud server can't able to damage the image. Now an official user, Bob shared information hiding key also encryption key, downloaded then decrypt. Bob expected to obtain decrypted images that have notation; it can used to map out history and source data. The image order decryption without extraction is completely suitable. Next, we explain how to create noticeable decrypted image.

4. RESULT AND DISCUSSION

The figure 2 shows accuracy. When compare to existing technique vacate room the proposed system reserving room has high accuracy.

The figure 3 shows Parameters. When compare to existing system parameters like reliability, quality and efficiency the proposed system parameters has high performance.

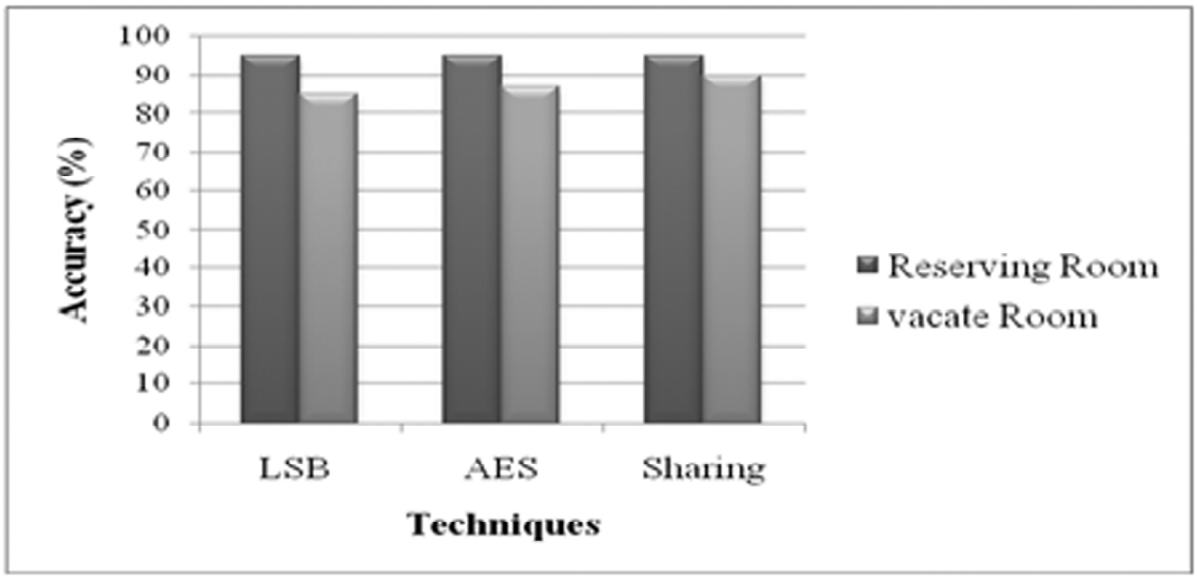

Figure 2: Accuracy

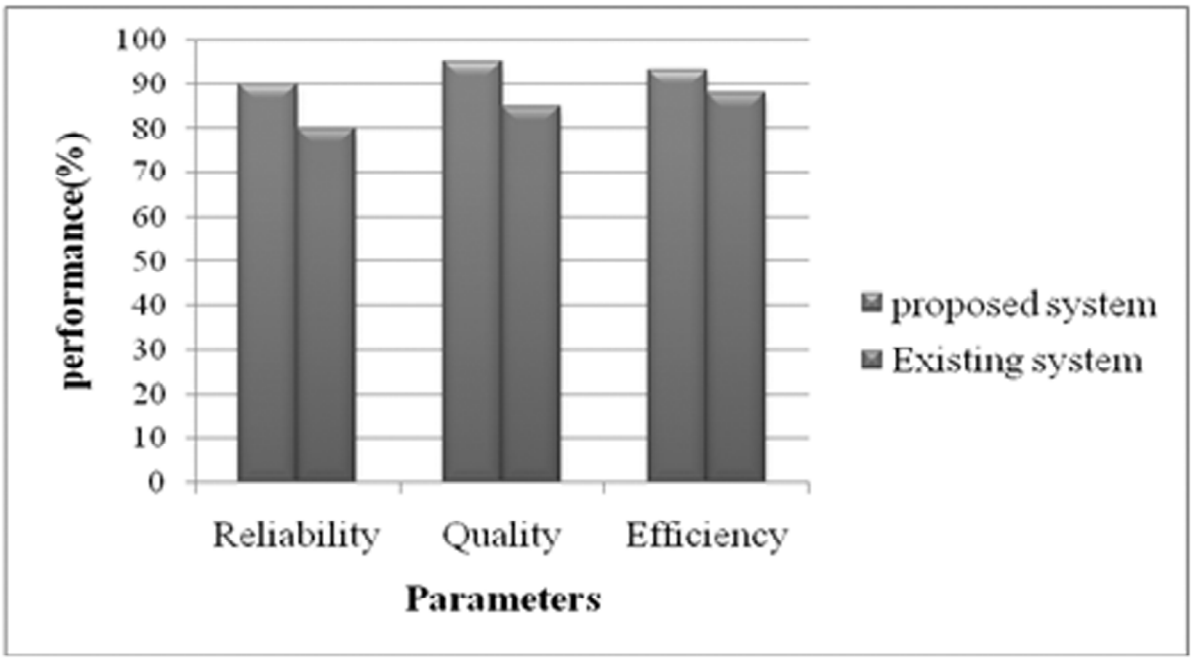

Figure 3: Parameters

5. CONCLUSION

RDH in Advanced Encryption Standard Encrypted image through reserving room earlier than encryption may attain high confidentiality reversibility for secret data due to multiple keys use during information hiding key with encryption key. By AES encryption, secret key is recognized to both receiver and sender. The AES technique remainder secure, key can't be firmed by any known.AES is enormously fast comparing to any block ciphers.Using arrangement of cryptography and steganography to self-reversible implanting is enhanced technique to obtain lossless information and inventive cover image. This paper significance is agreed to embedding technique adopt for RDH technique and relative revise is finished to hide extra data by extra protected embedding process.

REFERENCES

[1] Xianfeng Zhao, Weiming Zhang, Kede Ma, "REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYPTION" IEEE transactions on information security and forensics, volume. 8, number. 3, March 2013.

[2] Kshetrimayum Jenita Devi "A SESURE IMAGE STEGANOGRAPHY USING LSB TECHNIQUE AND PSEUDO RANDOM ENCODING TECHNIQUE" project thesis submitted on may 2013.

[3] G. Sharma, A. M. Tekalp, E. Saber, and M. U. Celik, "LOSSLESS GENERALIZED- LSB DATA EMBEDDING",IEEE transaction. image process., volume-14(2), page-253–266, 2013.

[4] X. Li, X. Wang, Z. Guo, and B. Yang, "EFFICIENT GENERALIZED INTEGER TRANSFORM FOR REVERSIBLE WATERMARKING", IEEE signal process. lett., volume-17(6), page- 567–570, 2012.

[5] Xianfeng Zhao, Weiming Zhang, , Kede Ma, *Member, IEEE*, Fenghua Li and Nenghai Yu, "REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYPTION" IEEE transaction. on information security and forensics, volume. 8, number. 3, page- 553, march 2013.

[6] Anagha Markandey, "A REVIEW ON DATA HIDING TECHNIQUES IN ENCRYPTED IMAGES", International journal of computer trends and technology (ijctt) – vol- 4 issue10 – oct 2013.

[7] P. Kalpana, P. Radhadevi, Assistant Professors, DEPT Of CA, "SECURE IMAGE ENCRYPTION USING AES" IJRET , Vol-1 Issue 2,Oct 2012.

[8] Ms.M.Usha2, Nithya.R1 "A SURVEY ON ANALYSIS OF REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE", international journal for trends in engineering & technology volume 3 issue 3 – march 2015 – issue number: 2349 – 9303 ijtet©2015 103

[9] Vincy Salam**,** Shilpa Sreekumar, "ADVANCED REVERSIBLE DATA HIDING WITH ENCRYPTED DATA" IJETT, Page 310**,** Vol-13, No-7, July 2014 ISSN: 2231-5381

[10] G.Sankar Babu, S.Natarajan & Dr.M.Anto Bennet, "RESERVE ROOM TECHNIQUE FOR REVERSIBLE DATA HIDING", JCPS, July- 2015

[11] *Prof. Vaibhav Deshpande, Janhavi Dongare, "REVIEW ON DATA HIDING SCHEME FOR ENCRYPTED IMAGE USING SPACE PRE-ALLOCATION"* international journal for engineering applications and technology**.**

[12] Xianming Liu, Jiantao Zhou, Yuan Yan Tang and Oscar C. Au, "DESIGNING AN EFFICIENT IMAGE ENCRYPTION-THEN-COMPRESSION SYSTEM VIA PREDICTION ERROR CLUSTERING AND RANDOM PERMUTATION", IEEE transactions on Information Security and Forensics, Volume- 9, number- 1, January 2014.

[13] Neeraj Sharma, Aasif Hasan, "A NEW METHOD TOWARDS ENCRYPTION SCHEME", 2014 international conference on reliability", ICROIT, page- 6-8, Feb 2014.