ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Reversible Data Hiding with Lossless Data Embedding

Chinchu Lipson[1], Lipson Chirayath [2]

Technical Manager, Former M.Tech in CSE from Bharath University, Chennai, India [1]

Technical Manager, Former B.Tech in IT from Vinayaka Mission University, Salem, India [2]

ABSTRACT: Reversible data hiding (RDH) in images is an important technique, by which the original image can be losslessly recovered after the embedded data is extracted while protecting the image content's confidentiality. All the previous methods are trying to embed data after the encryption of original images, which may be subject to some errors on data extraction and/or image restoration. In this paper, we propose a novel method of data embedding before image encryption by providing more security with traditional RDH algorithm. The proposed method can achieve real reversibility and extra security.

KEYWORDS: Reversible data hiding, data embedding, image encryption, privacy protection, sharing process, image decryption, data extraction.

I. INTRODUCTION

Nowadays, more and more attention is paid to reversible data hiding (RDH) in encrypted images since it maintains the excellent property that the original image can be losslessly recovered after the embedded data is extracted. There are also a number of works on data hiding in the encrypted domain. This technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original image is allowed. Since first introduced, RDH has attracted considerable research interest.

Most of the work on reversible data hiding focuses on data embedding/extracting on the encrypted images. This proposed method is about embedding data before encryption by providing more security with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data on the images. Thus the data hider task becomes effortless. The proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy.

Reversible data hiding is very useful for some extremely image such like medical images and military images. In the reversible data hiding schemes, some schemes are good performance at hiding capacity but have a bad stego image quality, some schemes are good stego image quality but have a low hiding capacity. It is difficult to find the balance between the hiding capacity and stego image quality. In this paper, a novel reversible data hiding scheme is proposed. The proposed scheme uses the concept of reserving room before encryption (RRBE) described in [1], which keeps the stego image quality in an acceptable level, and uses the multi-layer embedding to increase the hiding capacity.

In theoretical aspect, Kalker and Willems [14] established a rate-distortion model for RDH, through which they proved the rate-distortion bounds of RDH for memoryless covers and proposed a recursive code construction which, however, does not approach the bound. Zhang [2], [6] improved the recursive code construction for binary covers and proved that this construction can achieve the rate-distortion bound as long as the compression algorithm reaches entropy, which establishes the equivalence between data compression and RDH for binary covers.

In practical aspect, many RDH techniques have emerged in recent years. Fridrich [9] constructed a general framework for RDH. By first extracting compressible features of original cover and then compressing them losslessly, spare

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

space can be saved for embedding auxiliary data. A more popular method is based on difference expansion (DE) [5], in which the difference of each pixel group is expanded, e.g., multiplied by 2, and thus the least significant bits (LSBs) of the difference are all-zero and can be used for embedding messages. Another promising strategy for RDH is histogram shift (HS) [7], in which space is saved for data embedding by shifting the bins of histogram of gray values. The state-of-art method [10]-[13] usually combined DE or HS to residuals of the image, e.g., the predicted errors, to achieve better performance. Some attempts on RDH in encrypted images have been made. Zhang in [5] divided the encrypted image into several blocks. By flipping 3 LSBs of the half of pixels in each block, room can be vacated for the embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one block. This process can be realized with the help of spatial correlation in decrypted image.

All the three methods try to vacate room from the encrypted images directly. However, since the entropy of encrypted images has been maximized, these techniques can only achieve small payloads [4],[5] or generate marked image with poor quality for large payload and all of them are subject to some error rates on data extraction and/or image restoration. In the present paper, we propose a novel method for RDH in encrypted images, for which we do not "vacate room after encryption" as done in previous methods, but "reserve room before encryption" [1] by providing extra security. In the proposed method, we first find the place/or space where the message is to be embedded by calculating the difference value for each two consecutive pixels with a traditional RDH method and then embedding the secret data using LSB replacement algorithm. This proposed method also achieves excellent performance in three different prospects.

- •Real reversibility is achieved, that is, data extraction and image recovery are free of any error.
- •Extra security is realized, that is, unauthorized access is mostly restricted
- •For given embedding rates, the PSNRs of decrypted image containing the embedded data are significantly improved; and for the acceptable PSNR, the range of embedding rates is greatly enlarged.

This paper is organized in the following manner. Section II briefly introduces previous methods proposed in [3]-[5]. The novel method is elaborated in Section III in. Experiments set up and comparisons are given in Section IV followed by results in Section V. The paper is concluded in Section VI.

II. RELATED WORKS

The methods proposed in [3]-[5] all the above papers can be summarized as the framework, "vacating room after encryption (VRAE)", as illustrated in Fig. 1(a).In this framework, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by losslessly vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key .

In all the above methods of [3]-[5], the encrypted 8-bit gray-scale images are generated by encrypting every bit-plane with a stream cipher. The method segments the encrypted image into a number of nonoverlapping blocks sized by n x n; each block is used to carry one additional bit. To do this, pixels in each block are pseudo randomly divided into two sets S_1 and S_2 according to a data hiding key. If the additional bit to be embedded is 0, flip the 3 LSBs of each encrypted pixel in S_1; otherwise flip the 3 encrypted LSBs of pixels in S_2. For data extraction and image recovery, the receiver flips all the three LSBs of pixels in S_1 to form a new decrypted block, and flips all the three LSBs of pixels in S_2 to form another new block; one of them will be decrypted to the original block. Due to spatial correlation in natural images, original block is presumed to be much smoother than interfered block and embedded bit can be extracted correspondingly. However, there is a risk of defeat of bit extraction and image recovery when divided block is relatively small or has much fine-detailed textures.

Hong [4] reduced the error rate of Zhang's [5] method by fully exploiting the pixels in calculating the smoothness of each block and using side match. The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks and recovered blocks can further be used to evaluate

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

the smoothness of unrecovered blocks, which is referred to as side match.Zhang's [3] method is pseudo randomly permuted and divided encrypted image into a number of groups with size of L. The P LSB-planes of each group are compressed with a parity-check matrix and the vacated room is used to embed data.

III. PROBLEM STATEMENT

Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, "reserving room before encryption (RRBE)" [1].As shown in Fig. 1(b), the content owner first reserves enough space on original image. Now, the data embedding process in images is inherently reversible for the data hider only needs to accommodate data into the spare space previously reserved. Then the image with encrypted embedded data is encrypted. Here we use visual cryptography algorithm to encrypt the image. The data extraction and image recovery are identical to that of Framework VRAE. Obviously, standard RDH algorithms are the ideal operator for reserving room before encryption and can be easily applied to Framework RRBE to achieve better performance compared with techniques from Framework VRAE. This is because in this new framework, we follow the customary idea that first losslessly embedding the redundant secret data in the selected spaces in original image (e.g., using excellent RDH techniques) and then encrypts it with respect to protecting privacy.

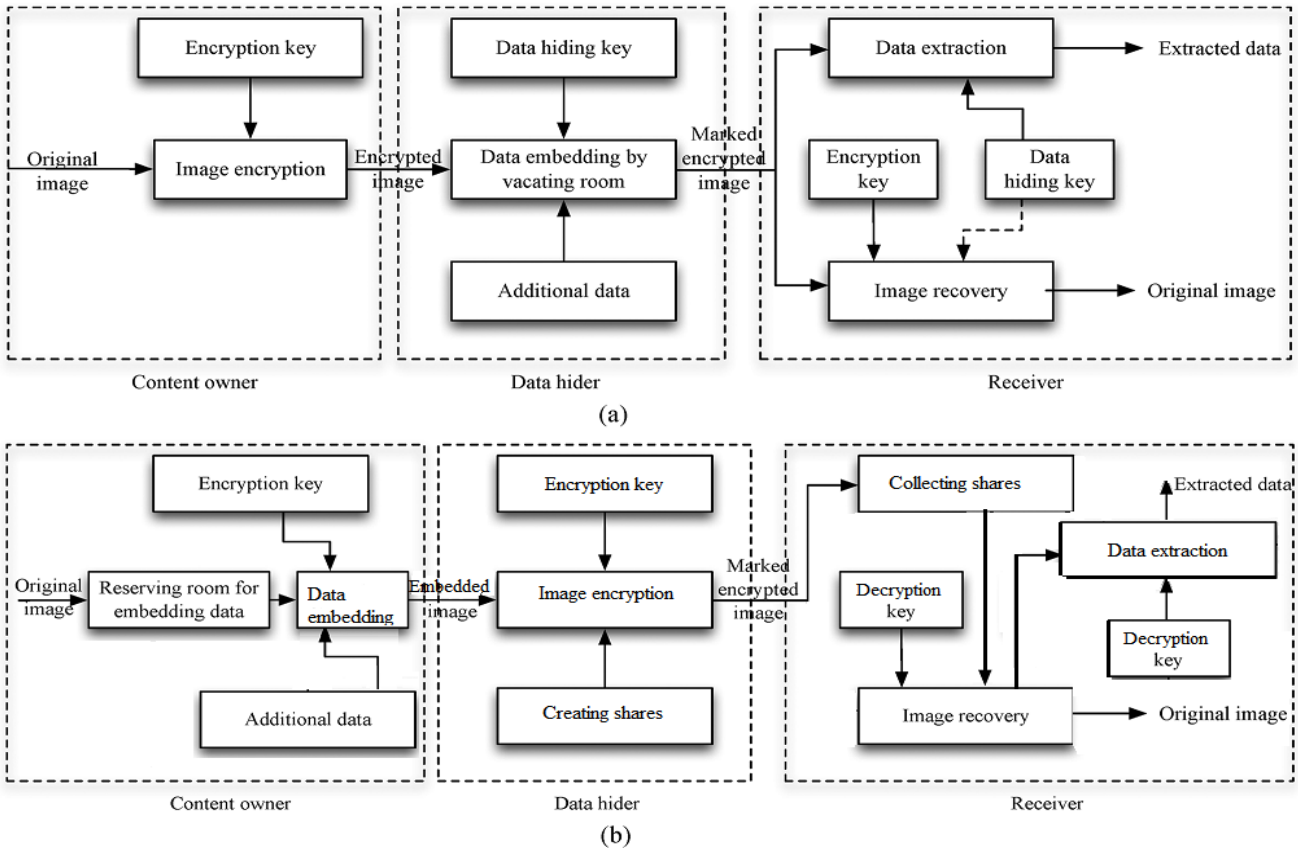

Fig. 1. a) Previous Method's Framework (b) Proposed Method's Framework

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Next we elaborate the practical method based on the framework "RRBE", which primarily consists of four stages: data embedding process, generation of encrypted image, image decryption and data extraction.

A. Data embedding Process

Actually, to embed data in the original image, the first stage can be divided into three steps: room selection, data encryption followed by data embedding. At the beginning, room selection finds the place where the message is to be embedded; then the secret data is encrypted to get more security using AES algorithm; at last the encrypted secret data is embedded into the image.

1) Room Selection

The operator here for reserving room or place before encryption is a standard RDH technique, so the goal of room selection is to select the place where the data is to be embedded, on which standard RDH algorithms can achieve better performance. To do that, without loss of generality, assume the original image C is an 8bits gray-scale image with its size M x N and pixels $C_{i,j} \in [0,255]$, $1 \le i \le M, 1 \le j \le N$. Then divide the original cover image into blocks. In detail, every block consists of m rows, where $m = [l / N]$, and the number of blocks can be computed through $n = M - m + 1$. An important point here is that each block is overlapped by previous and/or sub sequential blocks along the rows.Then calculate the median for each blocks i.e. represented as M. Find the square root of median for each block, i.e. S = fix (sqrt (M)). Then consider two consecutive pixels such as Pi and Pi+1. Then calculate the difference value for each two consecutive pixels Pi and Pi+1,i.e. Di = Pi – Pi+1. If the difference value of two consecutive pixels is greater than or equal to the square root value calculated by S, then embed the message in Pi.

Following the above procedure, reserves all the possible places where we can embed the secret data or message according to its length. This is the first step of data embedding process. After completing room selection, then it goes to Secret data encryption.

2) Data Encryption

Once the data hider acquires the secret data to be embedded, he can encrypt those data to get more security. The secret data is protected from unauthorized access of any third party persons using some strong encryption algorithm. In this paper, we are suggesting Advanced Encrypt-ion Standard algorithm for encrypting the secret data.

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that encrypts and decrypts information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits toencrypt and decrypt data in blocks of 128 bit. AES is based on a design principle known as a Substitution permutation network.The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. This kind of decryption is needed during the data extraction process.

3) Data Embedding

Once the data hider acquires the image, he can embed the encrypted secret data into the places which we are selected out. The embedding process starts with locating the places to embed data. After knowing how many bit-planes and rows of pixels he can modify, the data hider simply adopts LSB replacement to substitute the available bit-planes with additional data. Finally, the data hider sets a label following the embedded data to point out the end position of embedding process. Anyone who does not possess the data encryption key could not extract the additional data.There are many methods for steganography, to hide the secret message into the image. LSB is the well- known method for data hiding. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

B. Image Encryption

After rearranged data embedded image is generated, we can encrypt this image by creating shares. Here we use visual cryptography algorithm for encrypting the image. So first the image is converting into streams of data array and each data will be encrypted using Advanced Encryption Standard. The shares will be created based on the number of users. For example if 5 users are there means we create five shares. For each share the user can reveal the image but only after five shares he can view the full image. This algorithm not uses the encryption key because if the key is obtained by some unauthorized person then he will reveal the image very easily.

Thus by processing the secret image into n shares which are then hidden in n user-selected camouflage images, protects from any unauthorized third party access. This kind of image encryption algorithm provides more security than traditional encryption algorithm. It is suggested to select these camouflage images to contain well-known contents, like famous character images, well-known scene pictures, etc., to increase the steganographic effect for the security protection purpose. Furthermore, an image watermarking technique is employed to embed fragile watermark signals into the camouflage images by the use of parity-bit checking, thus providing the capability of authenticating the fidelity of each processed camouflage image, called a stego-image [17].

C. Image Decryption and Data Extraction

Since data extraction is completely dependent upon image recovery, so first we have to decrypt the image to extract the secret data. Here the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. The following example is an application for such scenario. Assume Alice outsourced her images to a cloud server, and the images are encrypted to protect their contents. Into the encrypted images, the cloud server marks the images by embedding some notation, including the identity of the image's owner, the identity of the cloud server and time stamps, to manage the encrypted images. Note that the cloud server has no right to do any permanent damage to the images.

Now an authorized user, Bob who has been shared the encryption key and the data hiding key, downloaded and decrypted the images. Bob hoped to get marked decryptedimages, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data. The order of image decryption before/without data extraction is perfectly suitable for this case. Next, we describe how to generate a marked decrypted image.

1) Generating the Marked Decrypted Image

To form the marked decrypted image, the content owner should do the following two steps.In first step, the content owner collects all the n shares created during image encryption. By aggregating all these shares, then only the content owner can obtain the single original image. And in the second step, each share is decrypted by using the same encryption key used in image encryption. Thus the marked decrypted image is generated.

2) Data Extraction and Image Recovery

After generating the marked decrypted image, then only the content owner can further extract the data and recover original image. The process is essentially similar to that of traditional RDH methods used. The secret data is then extracted using the same encryption key used in data encryption. The same procedure done in data encryption is just reversed to extract the secret data from the original image. Thus we can extract the secret data and recover the original image.

IV. EXPERIMENT SETUP AND COMPARISONS

We have implemented the proposed framework using Java programming language. Java is developed by James Gosling at Sun Microsystems. We take standard image Lena, shown in Fig. 2(a), to demonstrate the feasibility of proposed method. Fig. 2(b) is the encrypted image containing embedded messages and the decrypted version with messages is illustrated in Fig. 2(c). Fig. 2(d) depicts the recovery version which is identical to original image.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

We have compared the proposed method with the state-of- the-art works [1], [3]-[5]. As mentioned in Section I, all methods maybe introduce some errors on data extraction and/or image restoration, while the proposed method is free of any error for all kinds of images. In addition, another advantage of our approach is the much wider range of embedding rate for acceptable PSNRs. In fact, the proposed method can embed more than 10 times as large payloads for the same acceptable PSNR (e.g., PSNR = 40 dB) as the previous methods, which implies a very good potential for practical applications.We have compared the security of the proposed methods with the previous methods. In this proposed method, the image encryption is done by creating shares. The previous methods encrypt the image using keys. By hacking these keys, an unauthorized third party can easily restore the image andextract the secret message. So the proposed method provides more security and protects privacy [18].

(a) (b) (c) (d)

Fig. 2. Original image Encrypted image Decrypted image containing Messages Recovery version

V. RESULTS

The user selects the image for embedding the secret data. The data hider then encrypts the secret data using AES algorithm as in Fig. 3. The encrypted data is hidden into the selected image by the data hider. After data embedding, the image is processed into 5 shares as shown in Fig. 4- Fig. 8. Each share hides some pixels group of the data embedded image. Here the image is processed into 5 different shares. And finally the image is completely encrypted

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

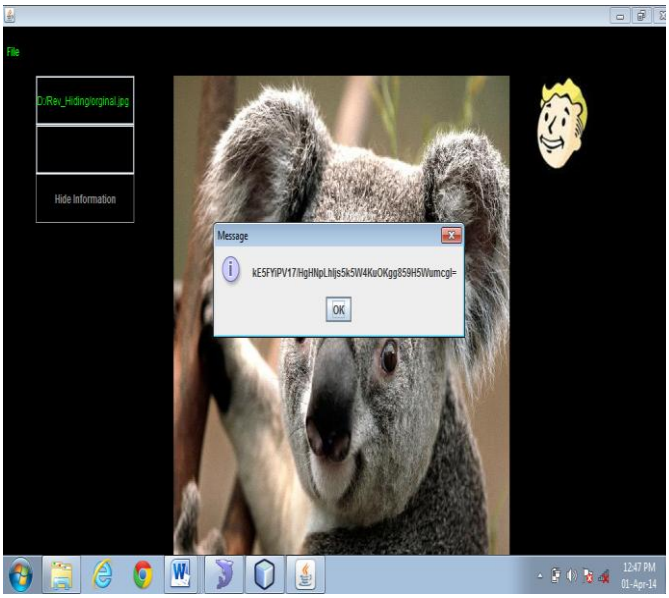

Fig. 3. Data hiding into the selected image

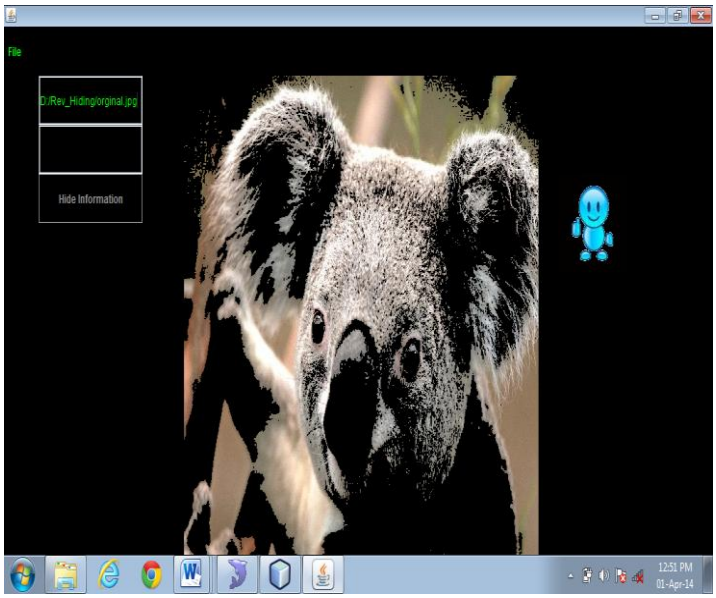

Fig. 4. Creation of Share1

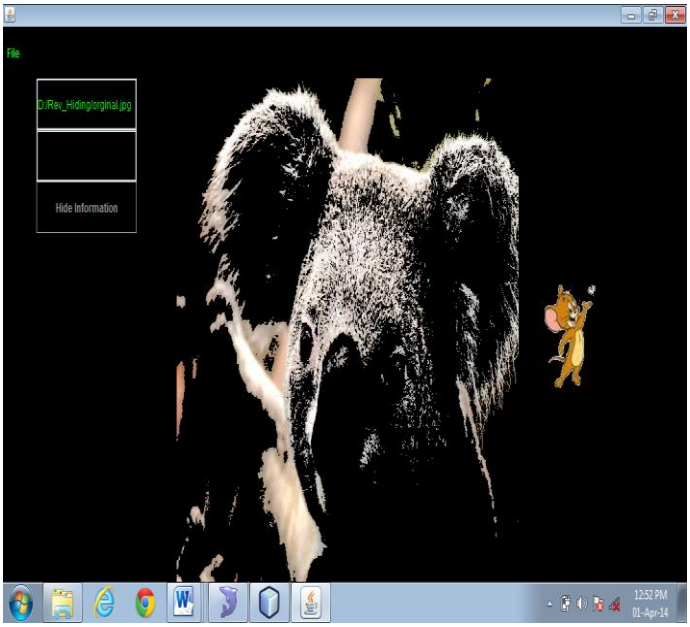

Fig. 5. Creation of Share2

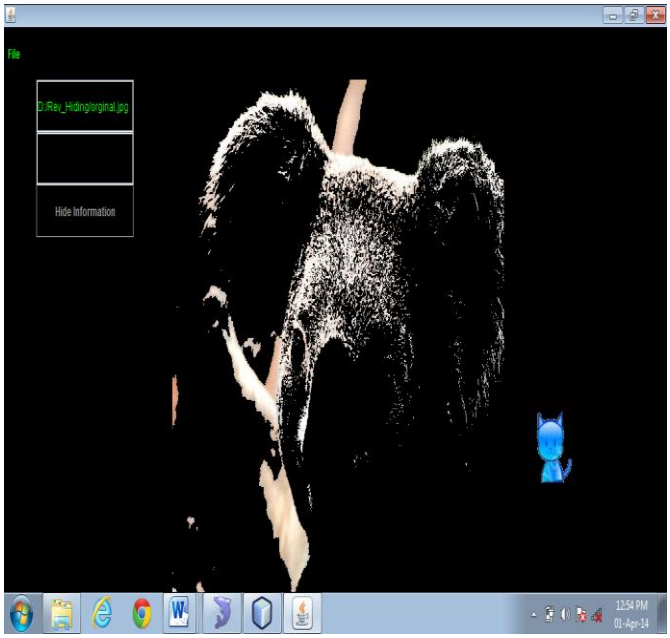

Fig. 6. Creation of share3

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

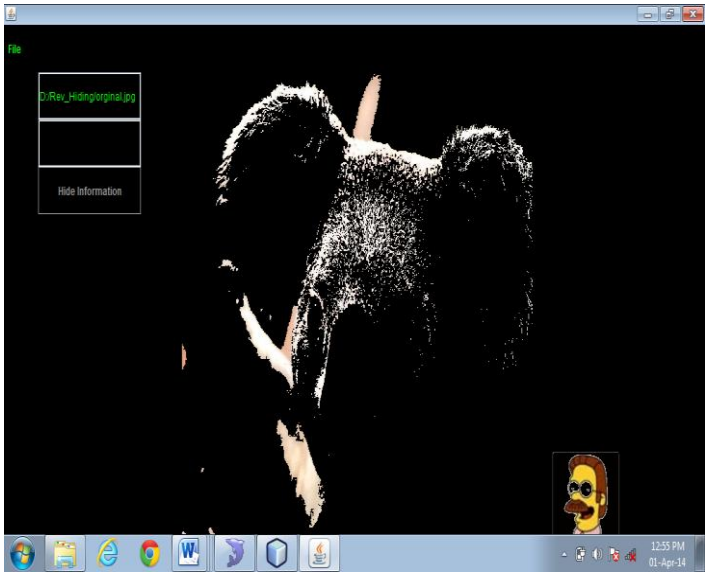

Fig. 7. Creation of Share4

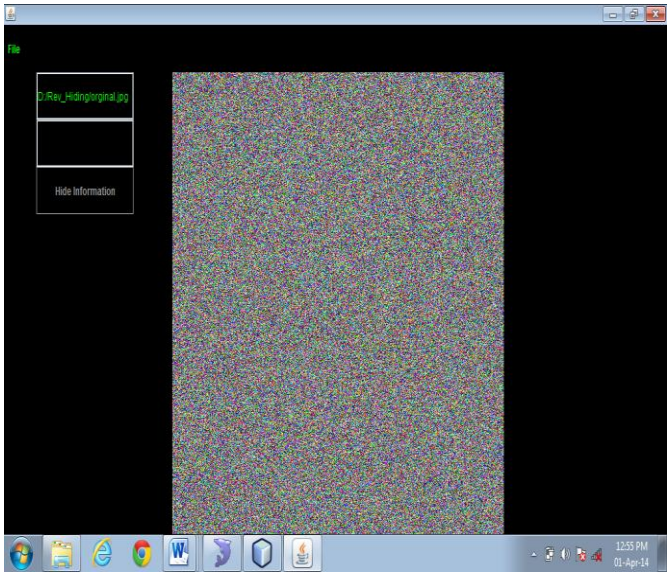

Fig. 8. Creation of share5

The encrypted image is decrypted by reversing the order of processes done during encryption. The 5 different shares are then collected and aggregated to form the original image. Fig. 9 shows the decryption of the share2.

By aggregating these 5 shares, we can get the original image as shown in Fig. 10.

Fig. 9. Decryption Stage

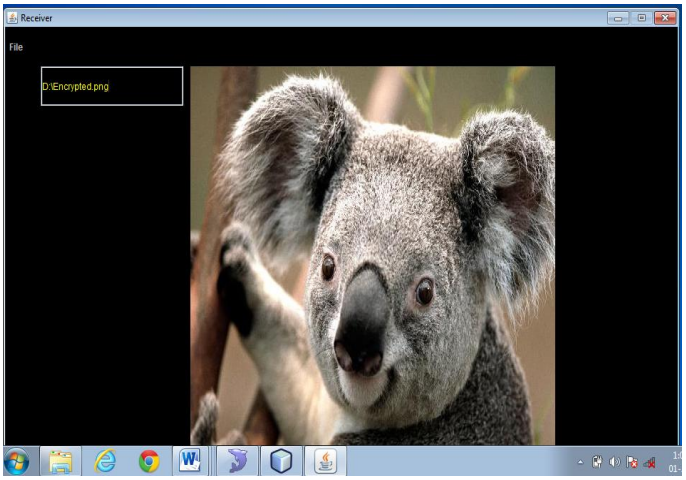

Fig. 10. Decrypted Image

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Once we obtain the image, then we can decode the data by entering the secret key for decoding as in Fig. 11.

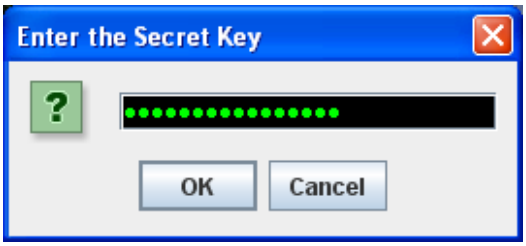

Fig. 11. Decoding

Now the hidden data is extracted and it is as in Fig. 12.

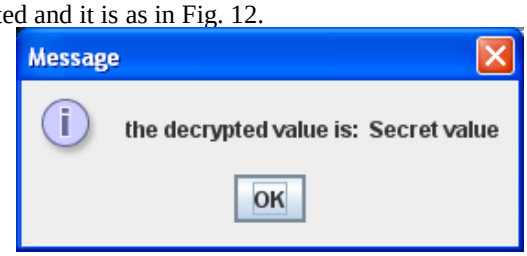

Fig. 12. Data Extraction

VI. CONCLUSION

Reversible data hiding in encrypted images is a new topic drawing attention because of the privacy preserving requirements from cloud data management. Previous methods implement RDH in encrypted images by embedding data after encryption, as opposed to which we proposed by reserving room for lossless data embedding before encryption with more security. Thus the data hider can embed data in the space already selected to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. Furthermore, this novel method can achieve real reversibility, extra security and greatly improvement on the quality of marked decrypted images.

VII. ACKNOWLEDGMENT

The authors would like to thank the colleagues from Feasible investments who provided insight and expertise that greatly assisted the research. The authors are thankful to Dr. A. Kumaravel for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the workand fruitful discussions in completing the work and the Faculty Members of Department of CSE. Also, they take privilege in extending gratitude to their parents and family members who rendered their support throughout this Research work.

REFERENCES

[1] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012

[2] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEET, Nenghai Yu, and Fenghua Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE Trans. On Information Security, Vol 8, Vo.3, March 2013.

[3] W. Zhang, B. Chen, and N. Yu, "Improving various reversible datahiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

[4] W. Hong, T. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.
[5] X. Zhang, "Reversible data hiding in encrypted images," IEEE SignalProcess. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
[6] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes forreversible data hiding," in Proc 13th Information Hiding (IH'2011), LNCS 6958, 2011, pp. 255–269, Springer-Verlag.
[7] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of en- crypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[8] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.
[9] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Secu- rity and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[10] D.M.ThodiandJ.J.Rodriguez,"Expansionembeddingtechniquesfor reversiblewatermarking,"IEEETrans.ImageProcess.,vol.16,no.3, pp.721–730,Mar.2007.
[11] L.Luoetal.,"Reversibleimagewatermarkingusinginterpolationtech- nique,"IEEETrans.Inf.ForensicsSecurity,vol.5,no.1,pp.187–193, Mar.2010.
[12] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.
[13] P.Tsai,Y.C.Hu,andH.L.Yeh,"Reversible imagehiding scheme usingpredictivecodingand histogramshifting,"*SignalProcess*
[14] Kalker and F. M. Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71-76.
[15] 89,pp.1129–1143,2009A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook ofApplied Cryptography. Boca Raton, FL, USA: CRC, 1996.
[16] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data," IEEE Trans. SignalProcess., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[17] Z.Ni,Y.Shi,N.Ansari,andS.Wei,"Reversible datahiding," *IEEE Trans.CircuitsSyst.VideoTechnol.*,vol. 16, no. 3, pp.354–362,Mar.2006.
[18] J.Tian,"Reversible dataembedding usingadifferenceexpansion," *IEEETrans.CircuitsSyst.VideoTechnol.*,vol.13,no.8,pp.890–896, Aug.2003.
.

BIOGRAPHY

Chinchu Lipsonis currently working as a Technical Manager.She pursued her M.Tech in Computer Science & Engineering from Bharath University, Chennai. She received her B.Tech degree in CSE from IES College of Engineering, Calicut University, Kerala. She has 2 years of teaching and 3 years of industrial experience in the field of Information Technology.

Lipson Chirayath received his B.Tech degree in Information Technology from Vinayaka Mission University, Salem. He is having 14 years of experience in the field of Information Technology, Telecom, Networking, and Project Management. He is leading two IT related organizations with 100 employees. He has attended a variety of technological exhibitions, conferences in India and overseas. He has introduced latest trends in IT in his organizations to build up into core digital company.