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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Reversible Data Hiding with Lossless Data Embedding

K.G.S. Venkatesan[1], K.P.Kaliyamurthie[2]

Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, Tamil Nadu, India[1]

Professor & Head, Department of Computer Science Engineering, Bharath University, Chennai, Tamil Nadu, India[2]

venkatesan.cse@bharathuniv.ac.in

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. In this paper, we deal with 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 this algorithm, 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 knowledge activity is extremely helpful for a few extremely image such like medical pictures and military pictures. within the reversible knowledge activity schemes, some schemes area unit smart performance at activity capability however have a foul stego image quality, some schemes area unit smart stego image quality however have an occasional activity capability. it's tough to seek out the balance between the activity capability and stego image quality. during this paper, a unique reversible knowledge activity theme is planned. The planned theme uses the idea of reserving space before coding (RRBE) represented in [1], that keeps the stego image quality in an appropriate level, and uses the multi-layer embedding to extend the activity capability.

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 memory less 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

establishes the equivalence between data compression and RDH for binary covers.
In sensible side, several RDH techniques have emerged in recent years. Fridrich [9] made a general framework for RDH. By initial extracting compressible options of original cowl then pressure them losslessly, spare area will be saved for embedding auxiliary knowledge. A additional in style methodology relies on distinction enlargement (DE) [5], within which the distinction of every component cluster is enlarged, e.g., increased by a pair of, and therefore the smallest amount vital bits (LSBs) of the distinction area unit all-zero and may be used for embedding messages. Another promising strategy for RDH is bar graph shift (HS) [7], within which area is saved for knowledge embedding by shifting the bins of bar graph of grey values. The state-of-art methodology [10-13] sometimes combined Delaware or HS to residuals of the image, e.g., the anticipated errors, to realize higher performance

Some makes an attempt on RDH in encrypted pictures are created. Zhang in [5] divided the encrypted image intomany blocks. By flipping three LSBs of the 1/2 pixels in every block, area are often vacated for the embedded bit the info extraction and image recovery proceed by finding that half has been flipped in one block. This method are often complete with the assistance of special 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 planned in [3-5] all the higher than papers may be summarized because the framework, "vacating space when coding (VRAE)", as illustrated in Fig. 1(a).In this framework, a content owner encrypts the initial image employing a commonplace cipher with associate coding key. when manufacturing the encrypted image, the content owner hands over it to an information hider (e.g., a knowledge base manager)and also the information hider will plant some auxiliary information into the encrypted image by losslessly vacating some space in line with a data concealment key. Then a receiver, perhaps the content owner himself or a certified third party will extract the embedded information with the info concealment key and more recover the initial image.

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 non overlapping 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

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

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 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 space from the encrypted pictures is comparatively troublesome and typically inefficient. If we tend to reverse the order of encoding and vacating space, i.e., reserving space before image encoding at content owner aspect, the RDH tasks in encrypted pictures would be a lot of natural and far easier that leads to the novel framework, "reserving space before encoding (RRBE)" [1]..

As shown in Fig. 1(b), the content owner initial reserves enough house on original image. Now, |the information embedding method in pictures is inherently reversible for the information hider solely must accommodate data into the spare house antecedently reserved. Then the image with encrypted embedded knowledge is encrypted. Here we tend to use visual cryptography algorithmic rule to code the image. the information extraction and image recovery square measure the image of that of Framework VRAE [7]. Obviously, commonplace RDH algorithms square measure the best operator for reserving space before encoding and maybe simply applied to Framework RRBE to attain higher performance compared with techniques from Framework VRAE. this can be as a result of during this new framework, we tend to follow the customary concept that initial losslessly embedding the redundant secret knowledge within the elite areas in original image (e.g., exploitation wonderful RDH techniques) and so encrypts it with relation to protective privacy.
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 [6].

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 [9].

1) Room Selection

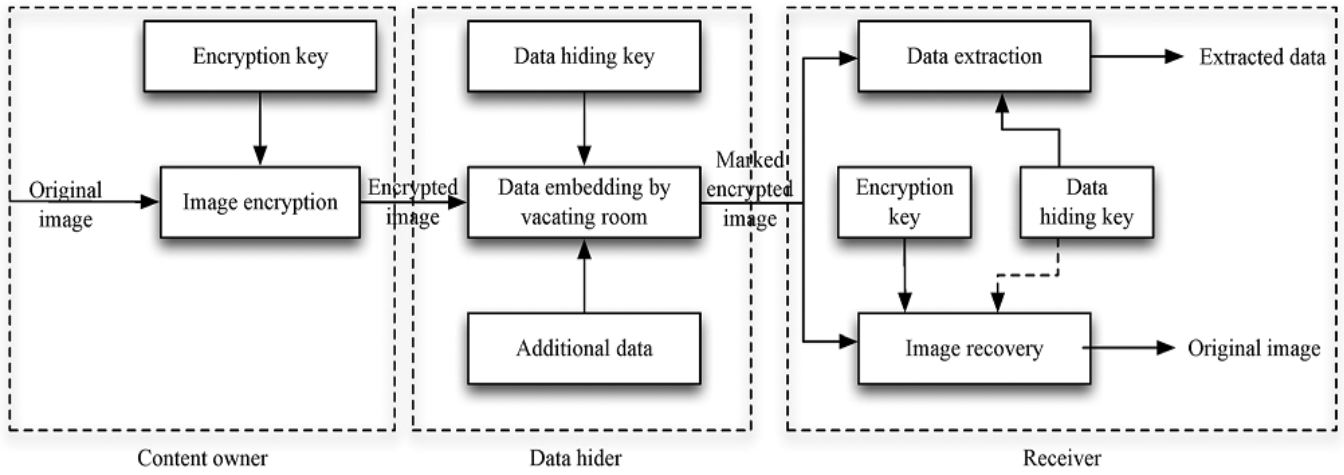
The operator here for reserving room or place before encryption is a standard RDH technique, so the goal of room selection is to select the place where the data is to be embedded, on which standard RDH algorithms can achieve better performance [10]. To do that, without loss of generality, assume the 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.

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

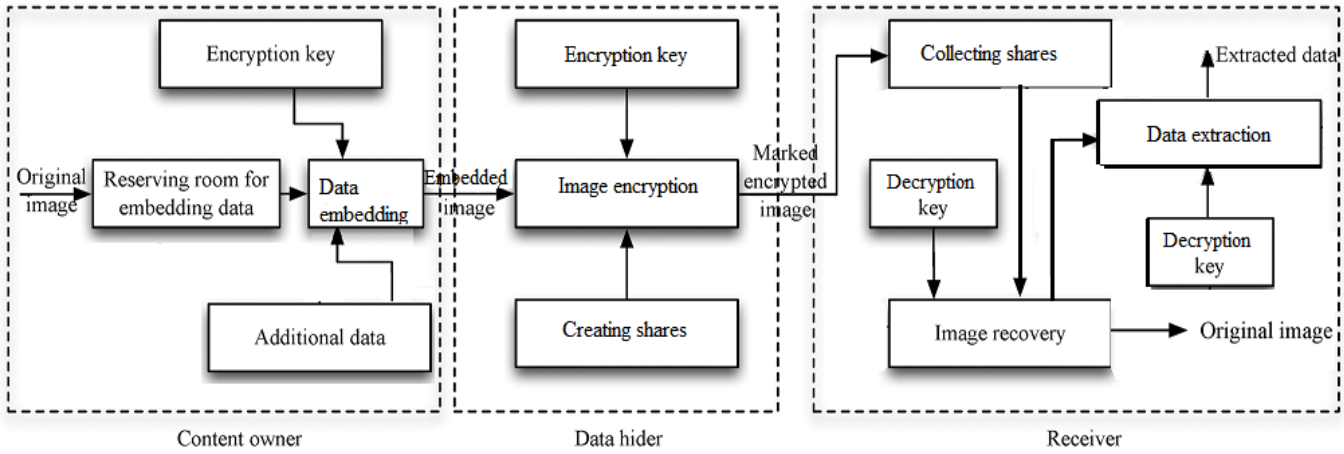
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015



(a)



(b)

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 [13].

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 [15].
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 cipher text; decrypting the cipher text 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 to encrypt and decrypt data in blocks of 128 bit. AES is based on a design principle known as a Substitution permutation network.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

The AES cipher is specified as variety of repetitions of transformation rounds that convert the input plaintext in to the ultimate output of cipher text. Every spherical consists of many process steps, together with one that depends on the coding key. A group of reverse rounds square measure applied to rework cipher text back to the initial plaintext mistreatment constant coding 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 [14]. 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.

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 [16]. 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 [18].

C. Image Decryption and Data Extraction

Since information extraction is totally dependent upon image recovery, therefore 1st we've to decode the image to extract the key information. Here the user needs to decode the image 1st and extracts the info from the decrypted image once it's required. the subsequent example is associate degree application for such state of affairs. Assume Alice outsourced her pictures to a cloud server, and also the pictures area unit encrypted to shield their contents [17]. Into the encrypted pictures, the cloud server marks the pictures by embedding some notation, as well as the identity of the image's owner, the identity of the cloud server and time stamps, to manage the encrypted pictures.
Now a licensed user, Bob UN agency has been shared the secret writing key and also the information activity key, downloaded and decrypted the pictures. Bob hoped to induce marked decrypted pictures, i.e., decrypted pictures still as well as the notation, which might be accustomed trace the supply and history of the info. The order of image cryptography before without information extraction is dead appropriate for this case. Next, we tend to describe the way to generate a marked decrypted image.[18]

1) Generating the Marked Decrypted Image

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

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 [19]. 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

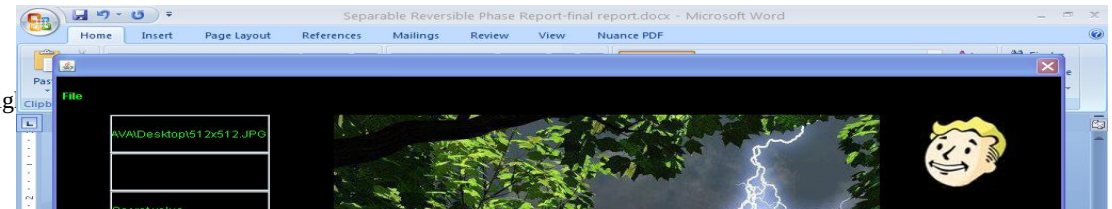
After generating the marked decrypted image, then only the content owner can further extract the data and recover original image. The process is essentially similar to that of traditional RDH methods used. The secret data is then extracted using the same encryption key used in data encryption. The same 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 [20].

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.[21]
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[22]. 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.[23] By hacking these keys, an unauthorized third party can easily restore the image and extract the secret message. So the proposed method provides more security and protects privacy.

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

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.[24] The encrypted data is hidden into the selected image by the data hider.



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

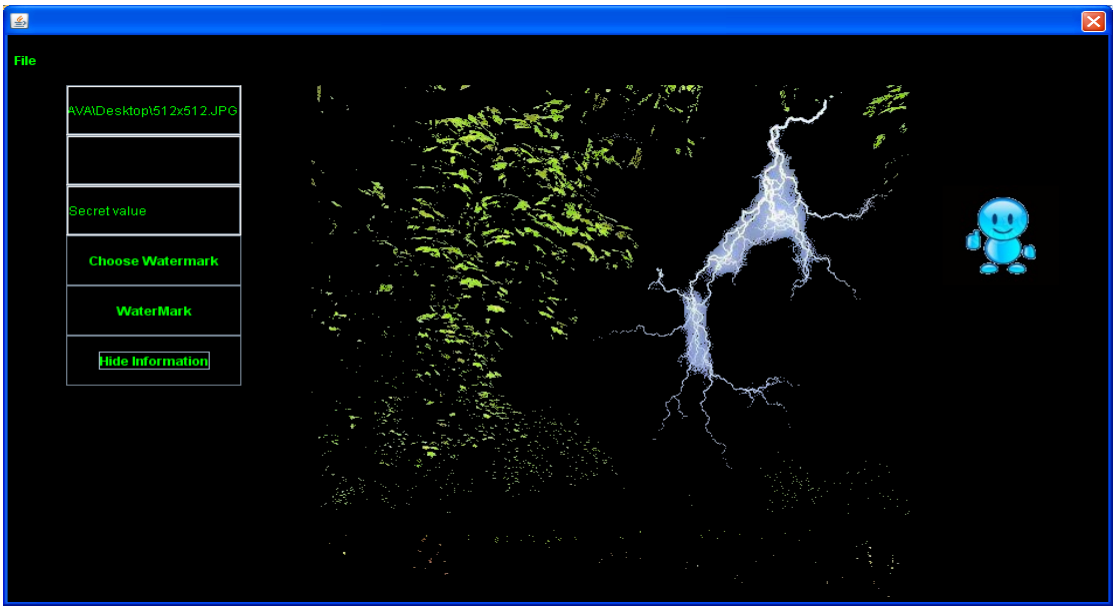
International Journal of Innovative Research in Computer and Communication Engineering

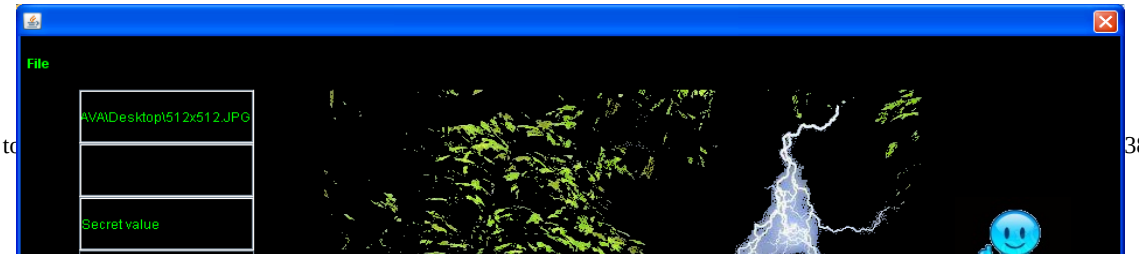
(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Fig. 3 :Data hiding into the selected image

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.[25] And finally the image is completely encrypted





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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Fig. 5 : Creation of Share 2

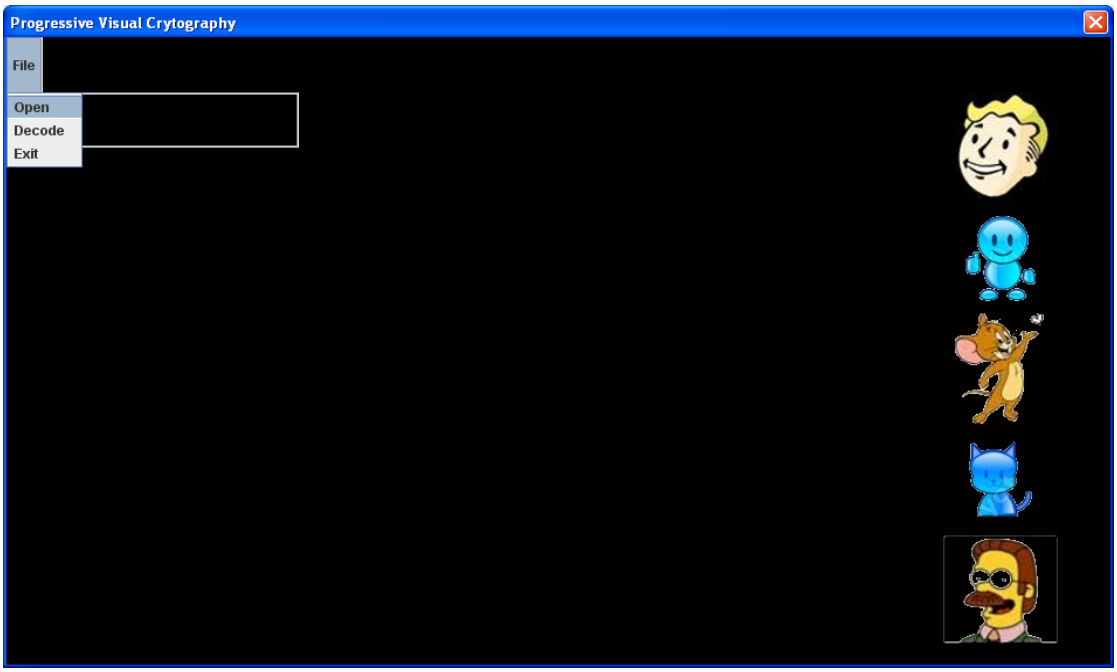
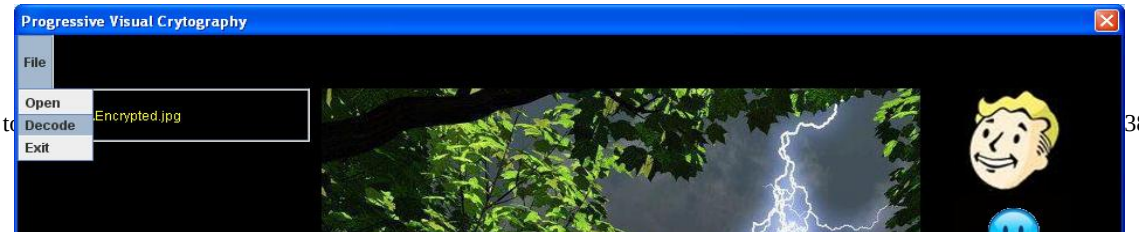


Fig. 6 : Decryption Stage



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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Fig. 7 :Decrypted Image

Once we obtain the image, then we can decode the data by entering the secret key for decoding as in Fig. 8.

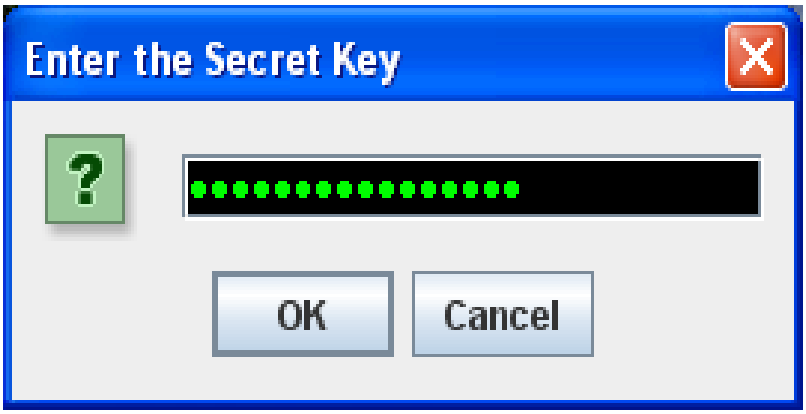
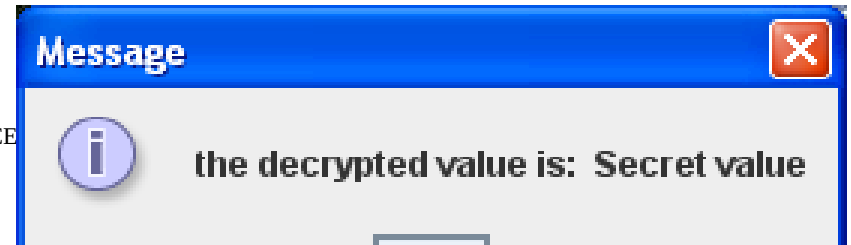


Fig. 8 : Decoding

Now the hidden data is extracted and it is as in Fig. 9.



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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Fig. 9 : 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. This novel method can achieve real reversibility, extra security and greatly improvement on the quality of marked decrypted images.

VII.ACKNOWLEDGEMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, HOD of Computer Science & Engineering, **Dr. K.P. Kaliyamurthie**, Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank **Dr. A. Kumaravel** for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science &Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

[1] 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, March 2013.
[2] K.G.S. Venkatesan and M. Elamurgaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, pp. 75 – 80, April 2013.
[3] B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary covers," IEEE Trans. Image Process., vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[4] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.
[5] K.G.S.Venkatesan, "Automatic detection & control of Malware spread in decentralized peer to peer network", International journal of Innovative Research in Computer & Communication Engg.,", Vol. 1, Issue 1, September – 2013.
[6] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Processs. Lett, Vol. 18, No. 4. Pp. 255-258.
[7] 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.
[8] L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.
[9] Kamatchi P., Selvaraj S., Kandaswamy M., "Synthesis, magnetic and electrochemical studies of binuclear copper(II) complexes derived from unsymmetrical polydentate ligands", Polyhedron, ISSN : 0277-5387, 24(8) (2005) PP.900-908.
[10] K.G.S. Venkatesan and M. Elamurugaselvam, "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, pp. 778 – 785, 2013.
[11] 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

[12] S.Sathish Raja and K.G.S. Venkatesan, "Email spam zombies scrutinizer in email sending network infrastructures", International journal of Scientific & Engineering Research, Vol. 4, Issue 4, PP. 366 – 373, April 2013.
[13] Kumaravel. A, 2013. "Cryptography Automata", Indian Journal of Science & Technology, 6 (5s) : 4561 – 4566.
[14] K.P.Kaliyamurthie, D.Parameswari and R.Udayakumar "QOS Aware Privacy Preserving Location Monitoring in Wireless Sensor Network", Indian Journal of Science and Technology, Vol.6(5S) , P: 4648-4652, May 2013, ISSN : 0974-6846
[15] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[16] Babu T.A., Joseph N.M., Sharmila V., "Academic dishonesty among undergraduates from private medical schools in India. Are we on the right track?", Medical Teacher, ISSN : 0142-159X, 33(9) (2011) PP.759-761.
[17] S.Sathish Raja and K.G.S.Venkatesan, " Electronic mail spam zombies purify in Email connection", International Journal of Advanced Research in Computer Science Engineering & Information Technology, Vol. 1, Issue 3, June 2013.
[18] Suresh V., Jaikumar S., Arunachalam G., "Anti diabetic activity of ethanol extract of stem bark of Nyctanthes arbor-tristis linn", Research Journal of Pharmaceutical, Biological and Chemical Sciences, ISSN : 0975-8585, 1(4) (2010) PP.311-317.
[19] K.P.Kaliyamurthie, D.Parameswari and R.Udayakumar , "K-anonymity Based Privacy Preserving for Data Collection in Wireless Sensor Networks", Indian Journal of Science and Technology ,Vol.6(5S), P:4604-4614, May 2013. ISSN : 0974-6846.
[20] Singamsetty P., Panchumarthy S., "Automatic fuzzy parameter selection in dynamic fuzzy voter for safety critical systems", International Journal of Fuzzy System Applications, ISSN : 1562-2479 , 2(2) (2012) PP. 68-90..
[21] P.Tsai,Y.C.Hu,andH.L.Yeh,"Reversible image hiding scheme using predictive coding and histogram shifting,"SignalProcess.,
[22] 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.
[23] Kiran B., Kareem S.A., Illamani V., Chitralekha S., "Case of Phthiriasis palpebrarum with blepheroconjunctivitis", Indian Journal of Medical Microbiology, ISSN : 0255-0857, 30(3) (2012) PP. 354-356..
[24] K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
[25] K.P.Kaliyamurthie, R. Udayakumar, D. Parameswari, "Highly Secured Online Voting System over Network". Indian Journal of Science and Technology ,Volume 6(6S), P:4831-4836,June 2013. ISSN : 0974-6846
[26]Dr.A.Muthu Kumaravel, KNOWLEDGE BASED WEB SERVICE, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 5881-5888, Vol. 2, Issue 9, September 2014
[27]Dr.A.Muthu Kumaravel, Data Representation in web portals, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 5693-5699, Vol. 2, Issue 9, September 2014
[28]Dr.Kathir.Viswalingam, Mr.G.Ayyappan,A Victimization Optical Back Propagation Technique in Content Based Mostly Spam Filtering ,International Journal of Innovative Research in Computerand Communication Engineering ,ISSN(Online): 2320-9801 , pp 7279-7283, Vol. 2, Issue 12, December 2014
[29]KannanSubramanian,FACE ECOGNITION USINGEIGENFACE AND SUPPORT ECTORMACHINE,International Journal of Innovative Research in Computerand Communication Engineering,ISSN(Online): 2320-9801,pp 4974-4980, Vol. 2, Issue 7, July 2014.
[30]Vinothlakshmi.S,To Provide Security & Integrity for StorageServices in Cloud Computing ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 2381-2385 ,Volume 1, Issue 10, December 2013