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

An Efficient Image Steganography for Message Security

Dr.G.Karuna

Associate Professor, Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India

ABSTRACT - The major goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. For reducing transmission bandwidth and storing space, the JPEG image is very common on the Internet. There are many ways to send the data in JPEGs. One popular technique is, by hiding data into the digital images. In this method the data is hidden into images that can't be seen by others, in fact others couldn't find that if any data is present in images. Reversible or invertible image data hiding can imperceptibly hide data into digital images and can reconstruct the original image without any distortion after the hidden data have been extracted out. It is easy for the data hider to reversibly embed data in the encrypted image. The proposed embedding method gains promising performance in terms of secure embedding capacity against steganalysis, easy to hide the data and can attain real reversibility.

KEY WORDS: Steganography, distortion, embedding image, encryption, reversibility.

I. INTRODUCTION

Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography, as an important branch of information hiding techniques, is mainly applied to covert communication. Image Steganography allows you to embed text and files into images, with optional encryption. Therefore, a lot of researchers have paid attention to investigate the steganography in the JPEG format over the past decade, and a number of steganographic methods for hiding messages in JPEG images have been proposed.

There are two ways to send the data in JPEGs using watermarking and by hiding data into the images. In watermarking methods the data is seen by others. Whereas in second form the hidden into images can't be seen by others, in fact others couldn't find that if any data is present in images. Hence communication using the second way is safer and easy. In this method the data which is to be sent is encrypted using any algorithm with a secret key. The secret key should be known to the receiver so that he can decrypt the hidden data. After embedding the data is embedded in images and encrypted and these stored in a reserved room. At the receiver end the images are decrypted first and then decoded. This is a reversible process. Reversible, also referred to as invertible or lossless, image data hiding can imperceptibly hide data into digital images and can reconstruct the original image without any distortion after the hidden data have been extracted out. This method can achieve real reversibility, that is, data extraction and image recovery are free of any error. It is easy for the data hider to reversibly embed data in the encrypted image. The proposed scheme is more secure, simple way to hide data and can achieve real reversibility.

II. RELATED WORK

There has been a development of lot of methods for JPEG steganography over a last few years, nsF5 [1], F5 [2]. A novel reversible data embedding method for digital images is presented by T. Kalker and F.M.Willems [3]. In

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

this explore the redundancy in digital images to achieve very high embedding capacity, and keep the distortion low. W. Zhang, et al [4] presented the novelty of reversing the order of the steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security. The histogram-shifting technique to remedy the two major drawbacks of Tian's algorithm presented which is an Expansion Embedding Technique for Reversible Watermarking [5]. A reversible data hiding scheme based on histogram is proposed by J. Fridrich and M. Goljan [6]. J. Tian focused [7] on the design and analysis of a practical lossless image codec, where the image data undergoes stream-cipher based encryption before compression and proposed resolution progressive compression which has been shown better coding efficiency and less computational complexity. A novel scheme for separable reversible data hiding in encrypted images proposed by D.M. Thodi, et al [8].J. Kodovský and J. Fridrich [9] proposed Steganalysis of JPEG images using rich models and classifiers for steganalysis of digital media[13].In this paper, they derived a rich model of DCT coefficients in a JPEG file for the purpose of detecting steganographic embedding changes.T. Filler, J. Judas, and J. Fridrich [10] proposed trellis-coded quantization for minimizing embedding impact. Many mainstream universal feature sets for JPEG steganalysis, like MP-486D [11] and CC-PEV-548D [14]are employed to evaluate the security performances of the image steganographic schemes. N. Provos[12], discussed about the defending against statistical steganalysis.

In literature more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless Recovered after embedded data is extracted while protecting the image content's confidentiality. These methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefits from the extra space emptied out in previous stage to make data hiding process effortless.

There are many methods for steganography, to hide the secret message into the image. LSB is the well-known method for data hiding. The PVD Method i.e pixel-value differencing method divides the cover image into blocks and modifies the pixel difference in each block for data embedding. Gray-level modification Steganography is a technique to map data by modifying the gray level values of the image pixels. It uses the odd and even numbers to map data within an image.

III. PROPOSED METHOD

The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. This method reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image and great improvement on the quality of marked decrypted images. A receiver can successfully extract the embedded secret data and recover the original content in the subsets with an inverse order.

A Novel Steganographic Technique for hiding text behind image is proposed. There are two major steps. First one is embedding the secret message in cover media using stegokey the second one is extracting the secret message from the cover media using stegokey. For extraction the secret message from the stego-media the recipient must have the stego-key.

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

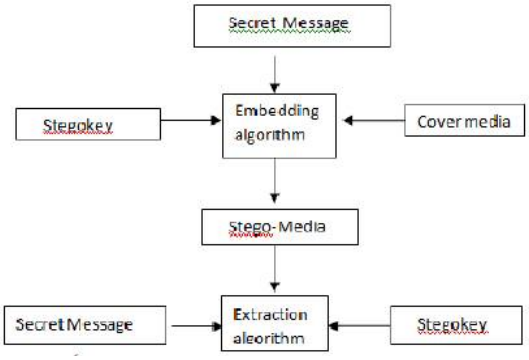


Fig.1

A. SYSTEM ARCHITECTURE

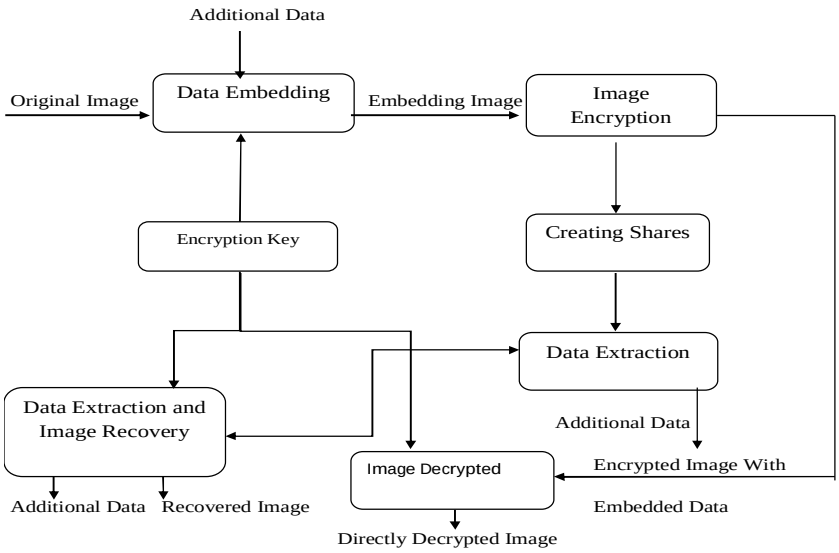


Fig. 2

B. PROPOSED ALGORITHM

The proposed Novel Embedding Image Encryption Method (NEIEM) has two major steps. In this algorithm, firstly, to get the place where the message is to be embedded and second, implement the embedding algorithm given below.

Step 1: Find Location to embed a message

1. Divide the cover image into blocks.
2. Calculate the median for each block M.
3. Calculate the square root of median for each block.
   S=fix(sqrt(M))
4. Calculate the difference value for each two consecutive pixels Pi and Pi+1.
   Di=Pi-Pi+1
5. If Di>=S then embed the message in Pi.

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

(Go to step 2)

Step 2: Embedding Algorithm

1. Split each pixel Pi into two equal parts.
2. Make the least significant four bits of the pixel to zeros.
3. Split the Message into two equal parts.
4. Make the most significant four bits to the zeros.
5. Apply bitxor operation on the two results.

The recipient uses the extraction algorithm i.e. reverse order of embedding algorithm to extract the secret message from the stego-image.

B.1REVERSIBLE DATA HIDING

Reversible Data hiding Image is a technique, by which the original cover can be loss lessly recovered after the embedded message has beenextracted.Reversible data hiding is very useful for some extremely image such like medical images and military images. In 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 a new embedding method, which is called Even-Odd embedding method, to keep the stego image quality in an acceptable level, and uses the multi-layer embedding to increase the hiding capacity.

B.2 IMAGE ENCRYPTION

This describes the encryption of image to be transmitted. Here visual cryptography algorithm used for encrypt the image. So first the image is converting into streams of data array and each data will be encrypted. The shares will be created based on the number of users. For example if 5 users are there i.e creating 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.

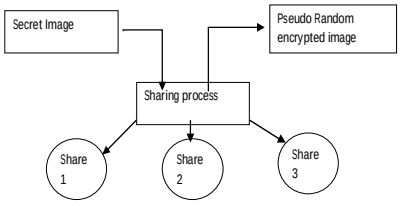


Fig.3

B.3 DATA EMBEDDING

Once encryption completed, the data is embedded with encrypted image for secret sharing. It takes one random encrypted image. Watermark gives the identification of the provider. Here we use LSB algorithm for data embedding. Before data hiding first encrypt the data using secret key. The embedding technique of watermark is given as follows.

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

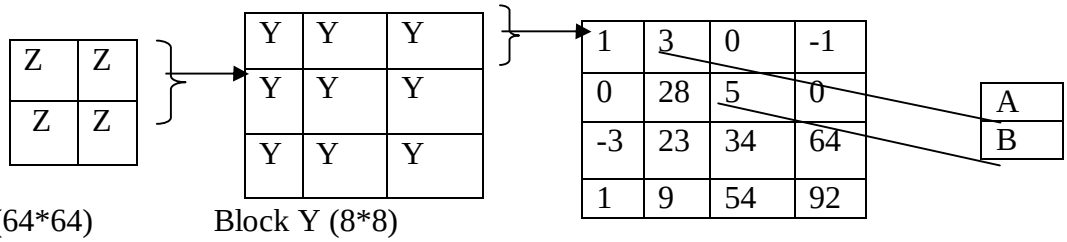
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 3, March 2017

Step 1: Assume that the size of the host image is 512×512. Host image is divided into small M×M blocks Z, block Z is divided into small M ×M blocks Y. If M=8 is used, the size of block Y is 8×8.



Block Z (64*64) Block Y (8*8)

Step 2: A number of pairs of coefficients (A, B) in block Y are chosen as A = a1, . . . , an, B = b1. . . bn based on a pseudo-random numbers, and mapping key that contains index of original chosen coefficients are kept.

Step 3: For embedding, two coefficient values (ai, bi) are modified by add parameterwhich is a parameter for watermark strength. i=1,…, n.

Step 4: Continue the above process according to n. Each block Y is embedded 1 bit watermark and watermark length decides how many blocks Y is embedded.

B.4 DATA PROTECTION

Image retrieval is computationally intensive and can benefit from offloading to save energy. To handle the protected data, the image retrieval program may be modified; the modified program must provide acceptable retrieval performance compared with the original program and unprotected data. Different retrieval algorithms may need different protection schemes. Consider two retrieval algorithms: Img Seek and Gabor filtering, and two protection schemes: Steganography and homomorphism encryption. Steganography uses a cover image to disguise the secret image so that it is difficult to detect. A simple and commonly used image Steganography technique is hiding images by replacing bits from the cover image with bits from the secret image. Encryption transforms plain data to make them unreadable. Steganography is different from encryption: the former hides the existence of data. In contrast, encryption makes the data meaningless without the key. ImgSeek can be performed on Steganography data as based on the linear property of feature extraction. However, ImgSeek assumes the images are with the same scales and orientations. Gabor filtering has better accuracy than ImgSeek for searching similar images with rotated objects. When using Gabor filtering, Steganography is not suitable to protect data anymore, because the feature extraction in Gabor does not show linear properties. Homomorphism encryption can be used in Gabor retrieval, because Gabor filtering mostly performs additions and multiplications on encrypted data.

B.5 EXTRACTING DATA FROM ENCRYPTED IMAGES

To manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. The order of data extraction before image decryption guarantees the feasibility of our work in this case. When the database manager gets the data hiding key, he can decrypt the LSB-planes of and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

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.6EXTRACTING DATA FROM DECRYPTED IMAGES

In Case, both embedding and extraction of the data are manipulated in encrypted domain. On the other hand, there is a different situation that 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 images' 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 decrypted images, i.e., decrypted images still including the notation, which can be used to trace the source and history of the data.

B.7 DATA HIDING IN ENCRYPTED IMAGE

Once the data hider acquires the encrypted image, he can embed some data into it, although he does not get access to the original image. The embedding process starts with locating the encrypted version of image. After knowing how many bit-planes and rows of pixels one 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 to point out the end position of embedding process and further encrypts according to the data hiding key to formulate marked encrypted image denoted by. Anyone who does not possess the data hiding key could not extract the additional data.

IV. EXPERIMENTAL RESULTS

A. ENCRYPTION PROCESS

In the proposed method the data which is to be sent is encrypted using Advanced Encryption Standard algorithm with a secret key. The secret key should be known to the receiver so that he can decrypt the hidden data.Then proposed method uses the reversible encrypted data concealment in digital images using visual cryptography algorithm and then least significant bit replacement technique.

Open the file to select an image of size 512 * 512 shown in Fig4(a) as an input image.Enter the data that to be hidden in image as shown in Fig 4(b). Before hiding the data first encrypt the data using Advanced Encryption Standard algorithm with a secret key of size 128 bits.

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

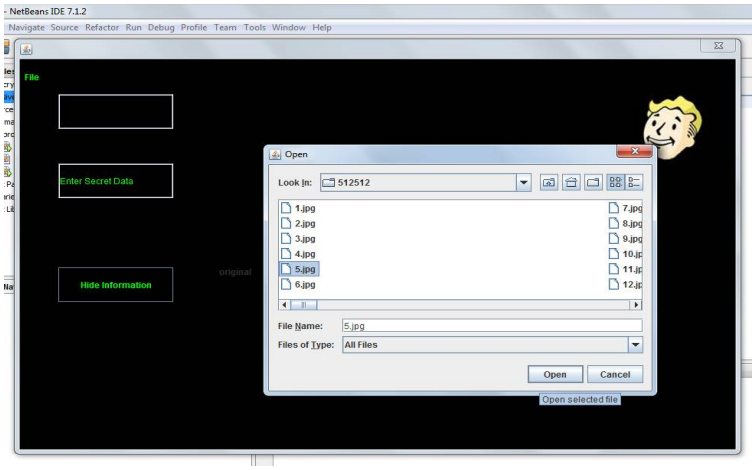


Fig. 4(a) Select an image of size 512*512

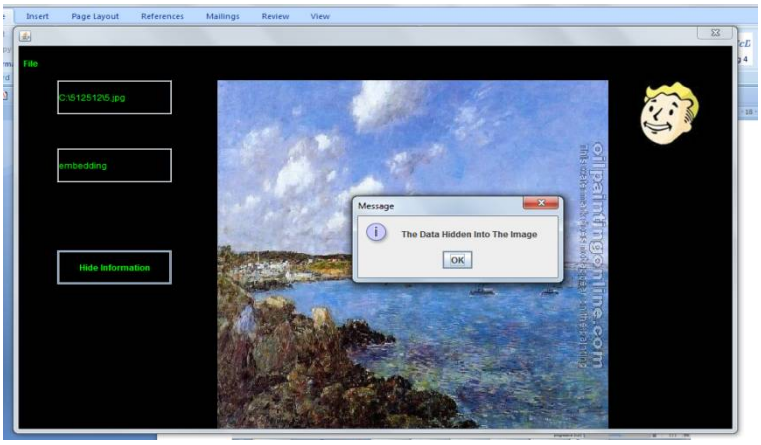


Fig. 4(b) Enter the data that is to be hidden

The visual cryptography algorithm used for encryption of the image. So first the image is converting into streams of data array and each data will be encrypted. The shares will be created based on the number of users which is explained in Fig.3. Here five users are taken i.e created five shares. Two shares are shown in Fig.4(c). For each share the user can reveal the image but only after five shares he can view the full image. Then data is embedded using Least Significant bits (LSB) algorithm. The proposed scheme also uses a new embedding method, which is called Even-Odd embedding method, to keep the stego image quality in an acceptable level, and uses the multi-layer embedding to increase the hiding capacity. After 5th share the encryption image is formed and embedded data in that image as shown in Fig.4(d)and these stored in a reserved room.

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

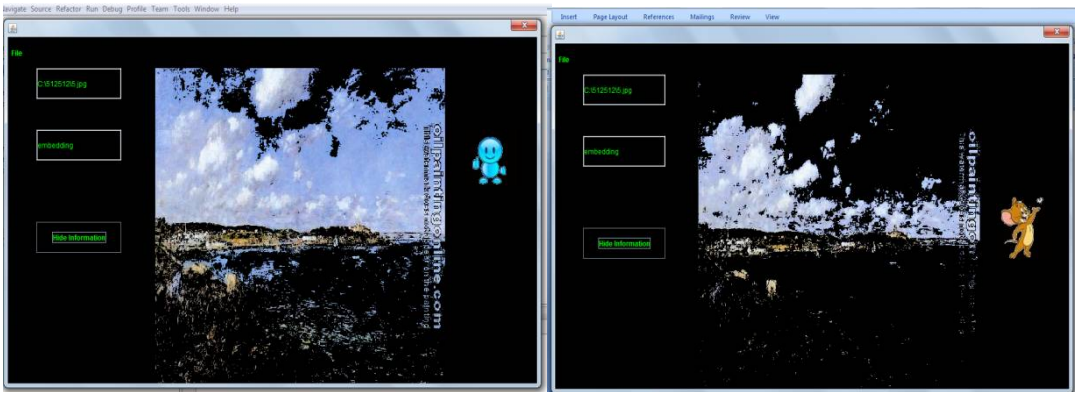


Fig.4(c) Shares are created (Two shares are shown)

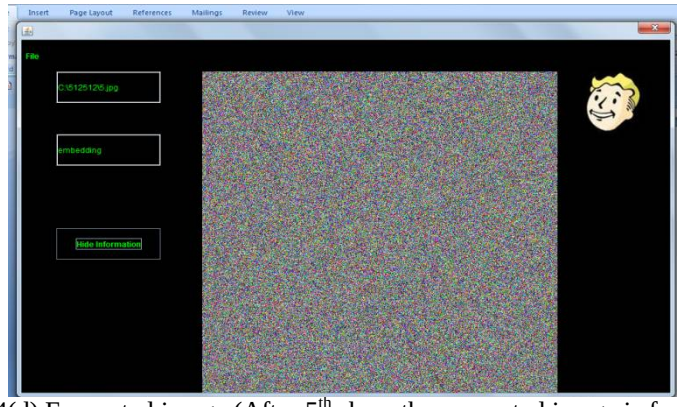


Fig. 4(d) Encrypted image (After 5th share the encrypted image is formed)

B. DECRYPTION PROCESS

At the receiver end the encrypted images are decrypted first and then decoded. So that an authorized user, who has been shared the encryption key and the data hiding key can choose the image downloadedat receiver site and enter the secret key shown in Fig. 5(a). The data is decrypted as shown in Fig.5(b) and the order of image decryption before orwithout data extraction is perfectly suitable for this case.

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

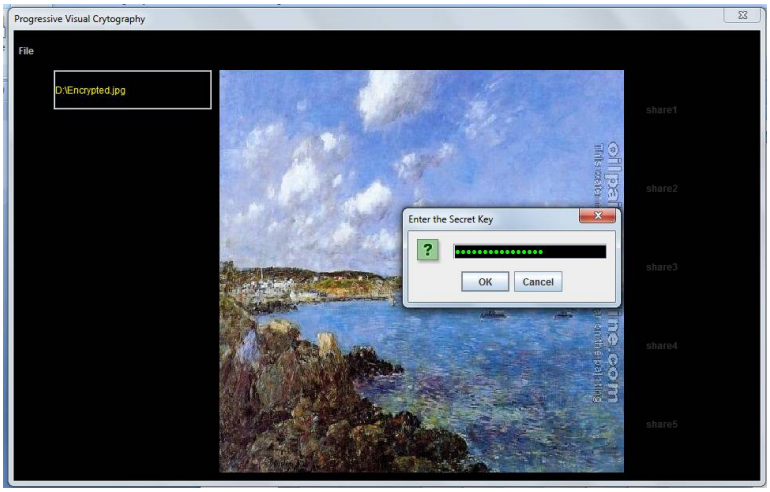


Fig. 5 (a) Choose image and enter secret key

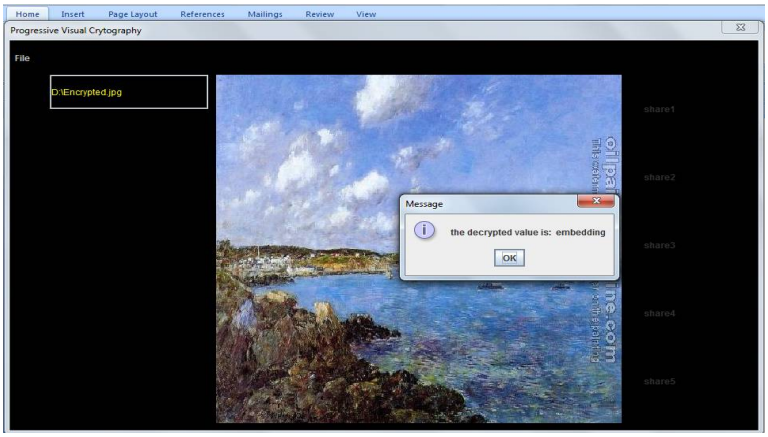


Fig. 5 (b) Decrypted Image

V. CONCLUSION

A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. Initially the sender encrypts the original uncompressed image using an encryption key. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data.

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

However, the lossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

REFERENCES

[1]J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends challenges, andopportunities", in Proc. 9th ACM Workshop Multimedia Security, Dallas, TX, USA, pp. 3–14, Sep. 2007.
[2] A. Westfeld, "F5-A Stenographic algorithm", in Proc. 4th Inf. Hiding Conf., vol. 2137, pp. 289–302, 2001.
[3] T. Kalker and F.M.Willems, "Capacity bounds and code constructions for reversible data-hiding", in Proc. 14thInt. Conf. Digital Signal Processing
(DSP2002), pp. 71–76, 2002.
[4] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding", in Proc 13th InformationHiding (IH'2011),LNCS 6958, pp. 255–269, Springer-Verlag, 2011.
[5]W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binarycovers", IEEE Trans.Image Process, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[6] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats", in Proc. SPIE Proc. Photonics West, Electronic Imaging, Securityand Watermarking of Multimedia Contents, San Jose, CA, USA, vol. 4675, pp. 572–583, Jan. 2002.
[7] J. Tian, "Reversible data embedding using a difference expansion",IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug.2003.
[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, Mar. 2007.
[9] J. Kodovský and J. Fridrich, "Steganalysis of JPEG images using rich models", Proc. SPIE, vol. 8303, p. 83030A,Jan. 2012.
[10]T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography usingtrellis-coded quantization", in Proc. SPIE, Electron.Imag., Security, Forensics Multimedia XII, N. D. Memon, E. J. Delp, P. W. Wong, and J. Dittmann, Eds., San Jose, CA, Jan. 17–21, vol. 7541, pp. 05-01–05-14, 2010.
[11]C. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in *Proc. IEEE Int. Symp. Circuits Syst.* pp. 3029–3032, Mar. 2008.
[12]N. Provos, "Defending against statistical steganalysis", in *Proc. 10th USENIX Security Symp.*, Washington, DC, USA, pp. 323–335, 2001.
[13]J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media", IEEE Trans. Inf. Forensics Security, vol.7,no.2, pp. 432–444, Apr. 2012.
[14]J. Kodovský and J. Fridrich, "Calibration revisited", in *Proc. 11th ACM Workshop Multimedia Security*, New York, NY, USA, pp. 63–74. Sep. 2009.

BIOGRAPHY

Dr.G. Karuna is currently working as an Associate Professor in Computer Science and Engineering Department at Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India. She hascompletedM.Tech andPh.D.(CSE)from Jawaharlal Nehru Technological University, Hyderabad, Telangana, India. She has eleven years of experience in teaching for both undergraduate and post graduate students. She has published 15 research papers in National and International journals and conferences. Her research interests are in the Areas of Image Processing, Image Watermarking, Cryptography and Network Security.