An Approach towards Separable Lossy Data Hiding

Vinit Agham
PG Student
R C Patel Institute of Technology
Shirpur, Dist. Dhule (India)

Tareek Pattewar
Assistant Professor
R C Patel Institute of Technology
Shirpur, Dist. Dhule (India)

ABSTRACT
Communication over the internet is facing some problems such as data security, copyright control, authentication etc. Here we introduce a novel scheme for separable data hiding when lossy image used as a cover media. This paper illustrates the various objectives of implementing separable lossy data hiding technique. The system is consists of three steps in the first step encryption of the cover image using an encryption key. Then, a data-hider hides the message image (secure data) into encrypted cover image using a data-hiding key. The third step is to extract the message image and recover the original image. The actions i.e. extracting the message image and recover the original images are depends upon which key the receiver has. There is separation of these two actions according to availability of keys. The scheme's key feature is the way of getting lossy image after decryption and data extraction processes. Here we are concentrating on using RGB-LSB method for data embedding and finally verifies the performance of using RGB-LSB method in terms of data capacity as well as image quality.

General Terms
Cryptography, image processing, steganography, data hiding, security

Keywords
Image encryption, RGB-LSB, image recovery, reversible data hiding, Lossy image, encryption key, data-hiding key

1. INTRODUCTION
Images used in military, medical science are the media in which we found certain alteration which is un-acceptable. Hence we need such data hiding technique in which we can extract data correctly and after that original cover content can be perfectly recovered. This technique is also termed as reversible data hiding or it is also named as lossless, distortion free, or invertible data hiding technique [1].The author Xinpeng Zhang presented an exclusive reversible (lossless) data hiding technique which supports the exact recovery of the original cover medium with the extraction of the embedded information. The process of this recovery with lossless data is nothing but the reversible data hiding. Data hiding technique which does not support the exact recovery of the original cover medium with the extraction of the embedded information is known as irreversible data hiding or lossy data hiding technique. At the receiver side sometimes it is needed to have a hidden secure data only. Sometimes there is no use of cover medium in which the hidden secret data is hiding. Sometimes it is also needed to have the cover media which carries the secure and confidential data. In some applications channel administrator appends some additional extra information, image notation or authentication data, inside the encrypted image where administrator does not identify the original image content. As in case of image data hiding the original carrier medium may change i.e. we get lower PSNR of the carrier image in such cases. In some data hiding and data communication techniques there are the situations where the receiver wants only the cover media in the communication. In another case the receiver wants the hidden data plus cover medium. So in such situation we need a concept of Separable Data Hiding Technique. The concept ofseparable data hiding technique is based on the possibilities exists at the receiver side. There are three players in this scheme those are first the sender, second the data hider and third the receiver. As usual the concept starts from the sender side. At the sender side the cover media or original cover medium owner encrypts the cover image. Then a data-hider or channel administrator embeds the data (message image). Now at receiver side there are three possibilities say three cases as shown in Figure 1.

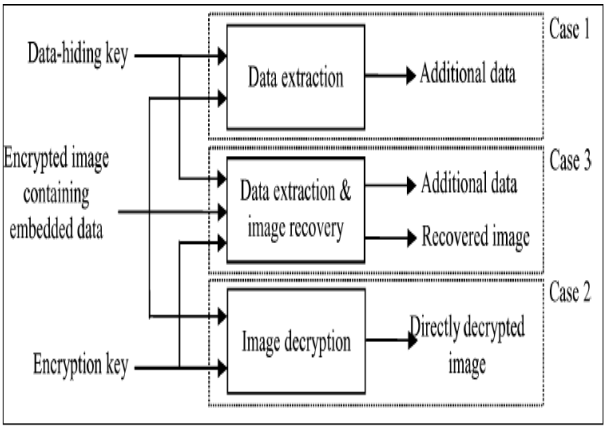

Fig.1: Three cases at receiver side of the proposed separable scheme [4].

Case one is if a receiver has the data-hiding key only, case two is if the receiver has the encryption key only and case three is If the receiver has both the keys. Now let's take case one if a receiver has the data-hiding key only then the receiver can take out the secure data even he does not know the cover media i.e. cover image content. In second case if the receiver has the encryption key only, he can decrypt the received data to obtain an image similar to the original cover image, but he cannot extract the additional data. If the receiver has both the keys i.e. data-hiding key as well as the encryption key he can extract the additional data and recover the original cover image. Thus we are separating the two actions i.e. recovery of the hidden data and recovery of the cover media. That's why it is termed as "Separable Data Hiding Technique" which is separable in nature.

The rest of this paper is organized as follows: in the next section we first give a literature survey of the topic which is followed by the motivation in section 3. In section four we propose the scheme theoretically followed by complete description of the methodology of the system. In section six we show the experimental results. In seventh section we conclude.

2. RELATED WORK

The presenting theme i.e. Separable data hiding technique is primarily consists of three principal theories those are compression-decompression domain, data hiding/embedding and lossy data hiding. Mostly data hiding techniques are not separable in nature, not implemented in encryption-decryption domain, not based on RGB-LSB steganography.

While transmission of data over an insecure and bandwidth constrained channel, it is expected to first compress the data and then encrypt it. Mark Johnson et al. reversed the order of these steps that is first encrypting and then compressing. They showed that the performance of compressing encrypted data may be as good as that of compressing non-encrypted data in theory [2].Xinpeng Zhang proposed a scheme for lossy compression of an encrypted image with flexible compression ratio. This way, the higher the compression ratio, higher the PSNR values, smoother the original image, the better the quality of the reconstructed image [3].Mehmet UtkuCelik et al. presented a novel lossless data-embedding technique which enables the exact recovery of the original host signal upon extraction of the embedded information [4].

Most of the work on data hiding focuses on the data embedding/extracting on the plain spatial domain. But in some applications we have to work in encrypted domain; for example reference [5] uses the same concept for videos in which video used as a cover medium and fingerprint as a secure data. Jun Tian stated the new concept of reversible data embedding in which he calculates the differences of neighboring pixel values and selects some difference values for the Difference Expansion. This algorithm works on grayscale images only. He achieved the policy that quality degradation on the image after data embedding should be low [6]. An algorithm for reversible data hiding which is based on histogram modification is presented in [1]. This algorithm utilizes the zero or the minimum points of the histogram of an image and slightly modifies the pixel grayscale values to embed data into the image. Jobi.V.Das and Kripa Ganesh presented a special reversible data hiding scheme for encrypted image in which computation complexity of the algorithm is the low, execution time is very less and having high capacity of hiding the secure data in concern with time and complexity. They focused on computation time to be decreasing and data capacity is to be increased [7].Xinpeng Zhang proposed a novel reversible data hiding scheme for encrypted image which is separable and lossless[8].

3. MOTIVATION

Most of the work of implementing the data hiding has been done in plain spatial domain. So while hiding the secure or confidential data we are also interested to hide the cover media details from the channel administrator or any other network manager. So this notion motivates us to find out the robust and secure technique which will able to hide the details of cover media as well as secure or confidential data which is to be carry. Thus we attempt to implement data hiding technique in encryption-decryption domain rather than plain spatial domain i.e. trying to join steganography with cryptography.

The author in [8] suggests the method of separable reversible data hiding in encrypted domain he also notes that the amount of data to embed in the image(cover media) must be small in size here we are trying to vary this size. We are trying to use three planes of the pixel values; these three planes are nothing but R plane, G plane and B plane of MATLAB image thus RGB-LSB (The word "MATLAB image" used here means any image which is processed as a three dimensional array in MATLAB).Usage of LSB of red, green and blue parameters of the image allows hiding much enough data in the image.

Also the previous work was based on reversible data hiding technique here we are trying to develop the scheme of separable data hiding in lossy i.e. irreversible data hiding. The original carrier medium and hidden data may be affected by embedding process. The original carrier medium is the image itself and hidden data is also in the image format. After embedding the data we are focusing on PSNR values of the decrypted image it should be more for ideal case. So this is our one of the target to have more PSNR value.

4. PROPOSED SCHEME

The concept of Separable lossy data hiding technique is based on the possibilities exists at the receiver side. There are three players in this scheme those are first the sender, second the data hider and third the receiver. As usual the concept starts from the sender side. At the sender side the cover media or original cover medium owner encrypts the cover image. Then a data-hider embeds the data i.e. message image. Now at receiver side there are three possibilities saying three cases. Case one is if a receiver has the data-hiding key only, case two is if the receiver has the encryption key only and case three is if the receiver has both the keys. Now let's take case one; if a receiver has the data-hiding key only then the receiver can take out the message image even he does not know the cover media i.e. cover image content. In second case if the receiver has the encryption key only, he can decrypt the received data to obtain an image similar to the original cover image, but he cannot extract message image. If the receiver has both the keys i.e. data-hiding key as well as the encryption key he can extract message image and recover the original cover image. Now the complete flow of the concept is shown in Figure 2.

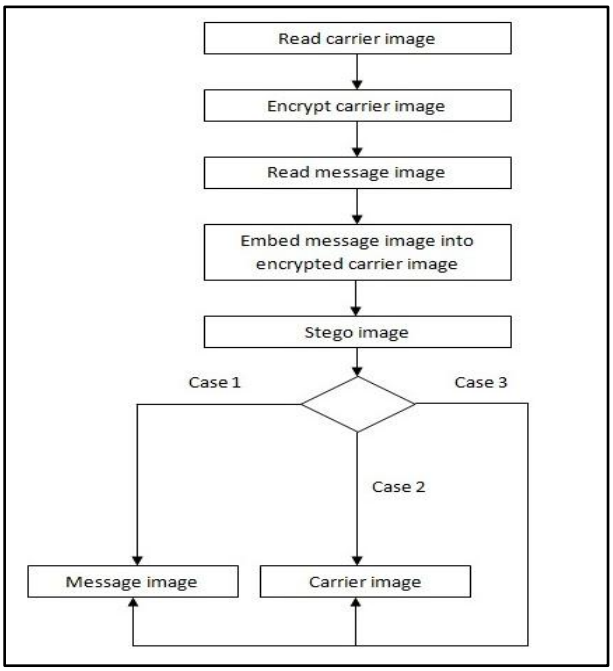

Fig.2: Proposed separable lossy data hiding technique block diagram.

5. METHODOLOGY

This paper is stating separable lossy data hiding method which is consists of following main procedures

5.1 ReadingCarrier Image

As shown in Figure 2.The first activity in the concept is to read the carrier image i.e. the content medium. It is nothing but input process. Just selecting any image may be of jpg, jpeg, png, bmp etc. We can use uigetfile( ),imread( )functions in MATLAB for this procedure. Select the appropriate cover image in which we want to add the bits of message image.

5.2 Encryption of Carrier Image

The second procedure is encryption of the input cover image. In this encryption phase, we calculate exclusive-or result of the original cover image bits and pseudo-random bits

$$A_{i,j,k,u} = B_{i,j,k,u} \oplus C_{i,j,k,u} \quad (1)$$

Where $C_{i,j,k,u}$ are determined by an encryption key. We can use bitxor( )function in MATLAB for this procedure.

5.3 Reading Message Image

In this procedure the secure data i.e. image in this case is chosen. Just selecting any image may be of jpg, jpeg, png etc. We can use uigetfile( ),imread( )functions in MATLAB for this procedure.

5.4 Data Embedding

In this step some parameters (i.e. bits of the pixels of the message image in this case) are embedded into a small number of encrypted pixels. The image obtained by making the room for embedding the message image is say temp image. Temp image is an imaginary image. A pixel of the temp image is represented by three values. Since temp image consisting of three separate arrays. In the RGB-LSB method message image can be embedded into encrypted version of the cover image using *or* operation between temp image and message image so that bits of the message image can easily be implanted into temp image. This implies

$$E_{i,j,k,u} = Di_{,j,k,u} + H_{i,j,k,u} \quad (2)$$

Where, $H_{i,j,k,u}$ are the bits obtained by shifting the bits of message image to the right, $Di_{,j,k,u}$ are the bits of temp image which generates Stego image. The embedding rate is a ratio between the data amount of net payload and the total number of cover pixels.

5.5 Message Image Extraction

Case one is with an encrypted image containing the embedded data if the receiver knows only a data-hiding key, he first get the values of the bits of the Stego image.

$$M_{i,j,k,u} = 8 + E'_{i,j,k,u} \quad (3)$$

Now here $E'_{i,j,k,u}$ are the bits obtained by shifting the bits of stego image to the left $M_{i,j,k,u}$ are the bits constitutes message image which is extracting from stego image. That is we get the embedded data in this case.

5.6 Carrier Image Recovery

Consider the case that the receiver has the encryption key but does not know the data-hiding key. Clearly, he cannot get the values of parameters of message image and cannot extract the embedded data. But, the original image content can be roughly recovered at the receiver. Denoting the bits of pixels in the stego image containing embedded data as $A'_{i,j,k,0}, A'_{i,j,k,1}, A'_{i,j,k,2}, \ldots\ldots\ldots A'_{i,j,k,7}$ the receiver can decrypt the received data

$$B'_{i,j,k,u} = A'_{i,j,k,u} \oplus C_{i,j,k,u} \quad (3)$$

Where $C_{i,j,k,u}$ are derived from the encryption key.

6. EXPERIMENTAL RESULTS

Our target is to implement the separable data hiding technique which is based on lossy image, having higher data capacity to hide and with better visual quality of the image.

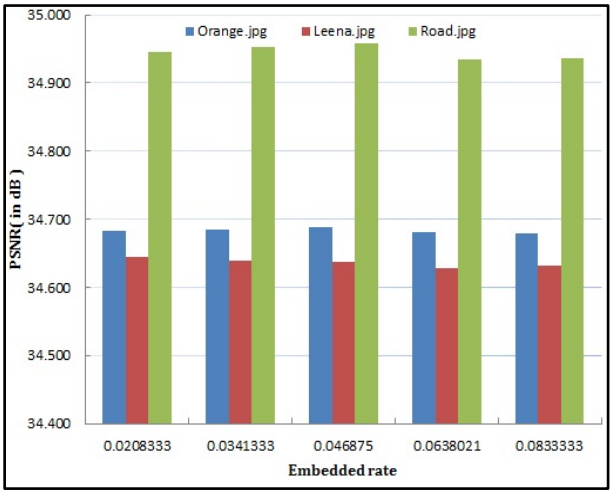

Fig.3: PSNR of decrypted version of the cover image.

The cover image road.jpg, leena.jpg and orange.jpg were taken as a cover medium as shown in Figure 4. Figure 3 shows the cover image quality degradation since lossy image**.** Here we get the PSNR values in the range 30 to 35 dB. Thus we can state that it is separable lossy data hiding.

Table 1: PSNR of extracted message images when Orange.jpg used as a cover medium.

Message images	Message Image File Size	Embedded rate	PSNR of extracted message image (in dB)
Image1	88.1 KB	1	38.8373
Image2	13.8 KB	0.046875	40.1532
Image3	5.02 KB	0.0205833	37.8491
Image4	23.4 KB	0.5	39.4544
Image5	30.3 KB	0.0208333	39.2002
Image6	75.6 KB	0.0638021	35.6783
Image7	1.37 MB	1	38.7688
Image8	24.2 KB	0.0833333	38.6427
Image9	349 KB	0.64	38.1943
Image10	59.1 KB	0.146306	37.7424

Also the implemented system can handle enough data to hide as depicted in Table 1.Here the result shows that we could embed the possible amount of data or payload (i.e. themessage image) in the cover image and still there is sufficient amount of peak signal to noise ratio as displayed in Table 1.

(a) (b) (c)

Fig.4: Cover image used a) Road.jpg b) Orange.jpg c) Leena.jpg

7. CONCLUSION

In this paper we implemented the scheme of separable data hiding using lossy image as a carrier medium with the help of RGB-LSB method. So after studying this novel technique it has been concluded that it is possible to hide the image as a data in separable lossy data hiding. This new approach describes how we can maintain the performance after changing the form of the secure data. Also by using the novel RGB-LSB method for embedding the data, the size of the net payload can be increased sufficiently. We observed the PSNRs of extracted message image are enough higher to established the lossy compression. Still there can be more future aspects in this scheme.

8. ACKNOWLEDGMENTS

We express our sincere thanks to Dr. J B Patil, Principal R.C.P.I.T. Shirpur and Prof. N. N. Patil, Head, Computer & IT Dept. R.C.P.I.T. Shirpur for allowing us to present this paper.Also we express our heartiest thanks to all the staff of computer & IT department, R.C.P.I.T. Shirpur for their valuable guidance while preparing this paper and guiding time to time.

9. REFERENCES

[1] Ni Z., Shi Y-Q, Ansari N. and Su W., 2006 .Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354-362.

[2] Johnson M., Ishwar P., Prabhakaran V. M., Schonberg D., and Ramchandran K., 2004.On compressing encrypted data. IEEE Transactions on Signal Processing, vol. 52, no. 10, pp. 2992-3006.

[3] Zhang X., 2011.Lossy compression and iterative reconstruction for encrypted image. IEEE Transactions on Information and Forensics Security, vol. 6, no. 1, pp. 53-58.

[4] Celik M.U., Sharma G., Tekalp A.M. and Saber E., 2005. Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing, vol. 14, no.2, pp. 253-266.

[5] Kundur D. and Karthik K., 2004.Video fingerprinting and encryption principles for digital rights management. Proceedings IEEE, vol. 92, no. 6, pp. 918-932.

[6] Tian J., 2003.Reversible data embedding using a difference expansion. IEEE Transactions on Circuits and Systems for Video Technology,vol. 13, no. 8.pp.890-896.

[7] Das J.V. and Ganesh K., 2012.Data Hiding Using a Novel Reversible Method forEncrypted Image. International Journal of Advanced Research in Technology, vol. 2, Issue 5.

[8] Zhang X., 2012.Separable Reversible Data Hiding in Encrypted Image. IEEE transactions on information forensics and security, vol. 7, no. 2, pp. 826-832.

[9] Gangwar A.and Shrivastava V., 2013.Improved RGB - LSB Steganography Using Secret Key. International Journal of Computer Trends and Technology, vol. 4, Issue 2, pp. 85-89.

[10] Shi Y.Q., 2005.Reversible data hiding.Springer-Verlag Berlin Heidelberg, pp. 1-12.

[11] Yadav D., Singhal V.and Bandil D., 2012.Reversible data hiding techniques. International Journal of Electronics and Computer Science Engineering, vol. 1, no. 2, pp. 380-383.

[12] Zhaoa Z., Luoc H, Lu Z.-M. andPan J.-S., 2011.Reversible data hiding based on multilevel histogram modification and sequential recovery. International Journal of Electronics and Communications, pp.814-826.