

Hiding Data into Encrypted Image and Recover Image Perfectly and Extract Data Correctly

Prof. Prashant. P. Rewagad

Mr. Satish R. Suryawanshi

Abstract — For conducting the secure communication data hiding, the new technique is evolved. Using data hiding technique one can send the information to the accurate user without noticing to third person. Data can be hiding using different cover Medias. Like video, audio or images, text. Here we take image as a cover media. As Internet based communications of images gone increase, Encryption of images has become an important way to protect images especially on the Internet. If we can use that both techniques at a time then it is use full to us. This novel system proposed that data hide into the encrypted image and then at receiver side receiver can get data or original image.

Key Words — data hiding, data extraction, image encryption, reversible data hiding.

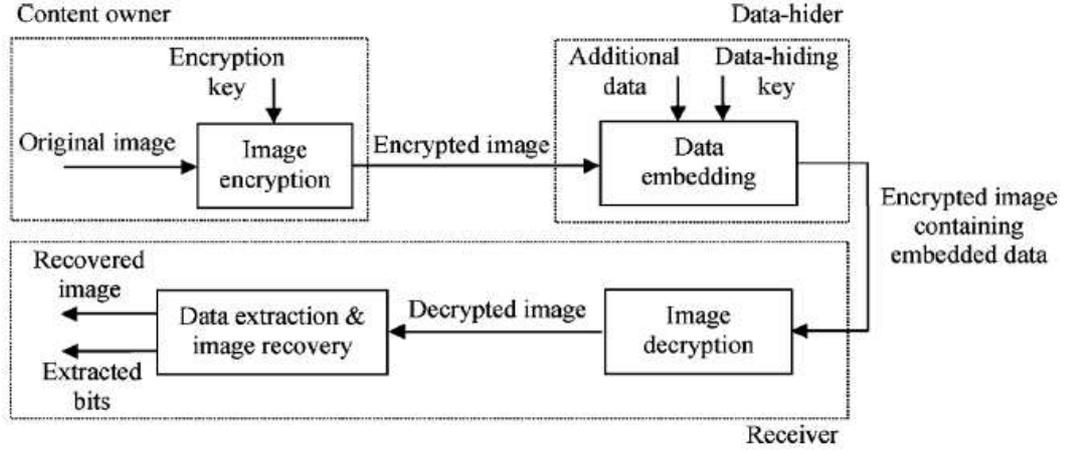
I. INTRODUCTION

Military and medical images are media having some distortion is un-acceptable. Hence for data hiding we have technique using which we can extract data correctly and after that original cover content can be perfectly recovered. This technique also known as reversible data hiding [4]. There are many reversible techniques such as expansion method and histogram shift method. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embedding [1].

Encryption is well known for privacy protection. For securely transmission of image content owner encrypt it before transmit it to other person. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into

the corresponding encrypted images. It may be also hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable [1]. But, in some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the data extraction is not separable from the content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is revealed before data extraction, and, if someone has the data-hiding key but not the encryption key, he cannot extract any information from the encrypted image containing additional data.

This paper proposed new scheme of data hiding it is also known as separable reversible data hiding. Content owner can encrypt his image before transmission by using encryption key. And additional data can be added using the data hiding key. At the receiver side if receiver has only data hide key, he can only extract the data from image. If receiver has encryption key then he can decrypt the image. But if receiver has both, data hiding and encryption key then he can extract hided data and as well as can recover image [2].


Fig 1: Proposed System [1]

II. PROPOSED SYSTEM

Proposed system has three main phases:

- A. Image Encryption
- B. Data embedding
- C. Data extraction and image recovery

Using encryption key content owner encrypt image. Then data hider create sparse space for hiding data by replacing least significant bits (LSB) in encrypt image using data hiding key. At the receiver side embedded data at sparsed space can retrieved from encrypted image using data hiding key. As data hiding affects only on LSB, hence after decryption original image can be correctly retrieved. When using both of the encryption and data-hiding keys, the embedded data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. Fig. 2 shows the three cases at the receiver side.

A. Image Encryption [4], [2]

Assume the original image is in uncompressed format and each pixel with gray value falling into $[0, 255]$ is represented by 8 bits. Denote the bits of a pixel as $b_{i,j,0}, b_{i,j,1}, \dots, b_{i,j,7}$ where (i,j) indicates the pixel position, and the gray value as $p_{i,j}$. Thus $b_{i,j,k} = \lfloor p_{i,j}/2^k \rfloor \bmod 2$, $k = 0, 1, \dots, 7$ (1)

$$p_{i,j} = \sum_{k=0}^7 b_{i,j,k} \cdot 2^k \quad (2)$$

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated.

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k} \quad (3)$$

Where $r_{i,j,k}$ are determined by an encryption key using a standard stream cipher. Then, $B_{i,j,k}$ are concatenated orderly as the encrypted data. A number of secure stream cipher methods can be used here to ensure that anyone without the encryption key, such as a potential attacker or the data hider, cannot obtain any information about original content from the encrypted data.

B. Data Embedding [4], [2]

With the encrypted data, although a data-hider does not know the original image content, he can embed additional message into the image by modifying a small proportion of encrypted data. Firstly, the data-hider segments the encrypted image into a number of non overlapping blocks sized by $s \times s$. In other words, the encrypted bits $b_{i,j,k}$ satisfying $(m-1) + s + 1 \leq I \leq m + s$, $(n-1) + s + 1 \leq j \leq n + s$ and $0 \leq k \leq 7$ (m and n are positive integers) are within a same block. Then, each block will be used to carry one additional bit. For each block, pseudo-randomly divide the s^2 pixels into two sets S_0 and S_1 according to a data-hiding key. Here, the probability that a pixel belongs to S_0 or S_1 is $1/2$. If the additional bit to be embedded is 0, flip the 3 least significant bits (LSB) of each encrypted pixel in S_0 ,

$$B'_{i,j,k} = B_{i,j,k} \quad (i, j) \in S_0 \text{ and } k = 0, 1, 2 \quad (4)$$

If the additional bit is 1, flip the 3 encrypted LSB of pixels in S_1 ,

$$B'_{i,j,k} = B_{i,j,k} \quad (i, j) \in S_1 \text{ and } k = 0, 1, 2. \quad (5)$$

The other encrypted data are not changed.

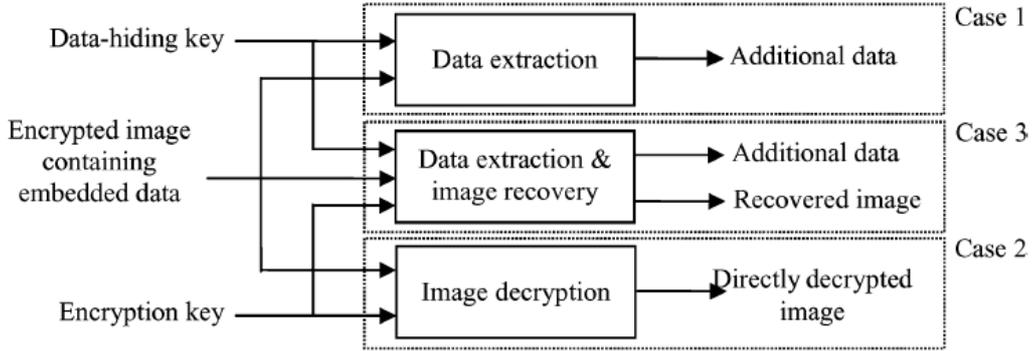


Fig 2: Three cases at the receiver side for the proposed separable scheme [2]

C. Data Extraction and Image Recovery [4], [2]

When having an encrypted image containing embedded data, a receiver firstly generates $r_{i,j,k}$ according to the encryption key, and calculates the exclusive-or of the received data $r_{i,j,k}$ and to decrypt the image. We denote the decrypted bits as. Clearly, the original five most significant bits (MSB) are retrieved correctly. For a certain pixel, if the embedded bit in the block including the pixel is zero and the pixel belongs to S_1 , or the embedded bit is 1 and the pixel belongs to S_0 , the data-hiding does not affect any encrypted bits of the pixel. So, the three decrypted LSB must be same as the original LSB, implying that the decrypted gray value of the pixel is correct. On the other hand, if the embedded bit in the pixel's block is 0 and the pixel belongs to S_0 , or the embedded bit is 1 and the pixel belongs to S_1 , the decrypted LSB That

$$= b'_{i,j,k} \quad k = 0, 1, 2 \quad (6)$$

That means the three decrypted LSB must be different from the original LSB. In this case:

$$b'_{i,j,k} + b_{i,j,k} = 1, \quad k = 0, 1, 2$$

So, the sum of decimal values of three decrypted LSB and three original LSB must be seven. The average energy of errors between the decrypted and original gray values is

$$E_A = \frac{1}{8} \sum_{u=0}^7 [u - (7-u)]^2 = 21.$$

As the probability of incorrect LSB-decryption is 1/2, when reconstructing an image using the decrypted data, the value of PSNR in the decrypted image is approximately

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\frac{E_A}{2}} = 37.9 \text{ dB}.$$

$$\begin{aligned} b'_{i,j,k} &= r_{i,j,k} \oplus B'_{i,j,k} \\ &= r_{i,j,k} \oplus B_{i,j,k} \\ &= r_{i,j,k} \oplus b'_{i,j,k} \oplus r_{i,j,k} \end{aligned}$$

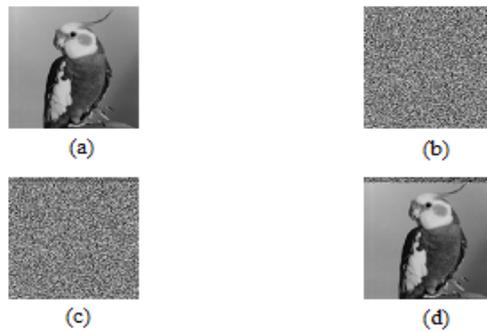


Fig 3: (a) Original image (b) Encrypted version (c) Encrypted image with message (d) Decrypted image. [3]

Then, the receiver will extract the embedded bits and recover the original content from the encrypted image. According to the data-hiding key, he may segment the decrypted image into blocks and divide the pixels in each block into two sets in a same way. For each decrypted block, the receiver flips all the three LSB of pixels in S_0 to form a new block, and flips all the three LSB of pixels in S_1 to form another new block. We denote the two new blocks as H_0 and H_1 . There must be that either H_0 or H_1 is the original block, and another one is more seriously interfered due to the LSB flip operation. For the two blocks sized by $S \times S$, define a function to measure the fluctuation in them and denote the values of fluctuation function of H_0 and H_1 as f_0 and f_1 respectively. Because of spatial correlation in natural image, the fluctuation function of original block is generally lower than that of a seriously interfered version. So, the receiver can perform data extraction and image recovery by comparing f_0 and f_1 . If $f_0 < f_1$, regard H_0 as the original content of the block and let the extracted bit be 0. Otherwise, regard H_1 as the original content of this block and extract a bit 1.

$$f = \sum_{u=2}^{s-1} \sum_{v=2}^{s-1} \left| p_{u,v} - \frac{p_{u-1,v} + p_{u,v-1} + p_{u+1,v} + p_{u,v+1}}{4} \right|$$

Finally, concatenate the extracted bits to retrieve the additional message and collect the recovered blocks to form the original image [4], [2].

CONCLUSION

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 in [6] or [7] 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 [2]. However, the lossy compression method in [5] compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation [2]. So, in future a complete mixture of image encryption and data hiding compatible with lossy compression demands further research.

ACKNOWLEDGMENT

I express my sincere thanks to **Dr. Prabhakar Bhat, Principal G.H.R.I.E.M., Jalgaon.** And **Prof. Mr. P. P. Rewagad, H.O.D. of CSE dept of G.H.R.I.E.M., Jalgaon** for allowing me to present this paper. also I express my heartiest thanks to **Prof. C. D. Badgujar, Assist. Prof. of G.H.R.I.E.M., Jalgaon,** for his valuable guidance while preparing this paper and guiding time to time.

REFERENCES

- [1] Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image" IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 4, APRIL 2011.
- [2] Xinpeng Zhang, "Separable Reversible Data Hiding in Encrypted Image" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.
- [3] R. Suchitra and C. Vinothkumar, "Data Hiding in Encrypted Images".
- [4] Manikandan R and Uma M, MahalakshmiPreethi S M, "Reversible Data Hiding for Encrypted Image", Journal of Computer Applications ISSN: 0974 - 1925, Volume-5, Issue EICA2012-1, February 10, 2012.
- [5] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 1, pp. 53–58, Feb. 2011.
- [6] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K.Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
- [7] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

AUTHOR'S PROFILE



Prof. Prashant. P. Rewagad

Head of the department Computer Engineering
 G.H.Raisoni Institute of engineering and management,
 Jalgaon.
 Email id: prashant_rewagad@rediffmail.com



Mr. Satish R. Suryawanshi

Pursuing Masters Degree in Computer Science &
 Engineering from G.H.Raisoni Institute of
 Engineering and Management, Jalgaon and doing
 research work under guidance of Mr. Prashant P.
 Rewagad sir. Email id: 19satish8@gmail.com