Unique LSB Compression Data Hiding Method

Ashwini Jarali, Jyoti Rao

Abstract—This paper presents a unique method of reversible data hiding separately in encrypted image..This work presents a new method that combines image cryptography, data hiding and LSB compressing technique for reversible data hiding separately. In this method we encrypt the original image with stream cipher algorithm. Then, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data-hiding key, she can extract the additional data though she does not know the image content. If the receiver has the encryption key, she can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key she can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image.

Keywords— LSB compressing, reversible data hiding, Image encryption, data embedding, Pixel Permutation.

I. INTRODUCTION

DATA HIDING [7] is referred to as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. The relationship between these two sets of data characterizes different applications. For instance, in covert communications, the hidden data may often be irrelevant to the cover media. In authentication, however, the embedded data are closely related to the cover media. In these two types of applications, invisibility of hidden data is an important requirement.

In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free, or invertible data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.

In most cases of data hiding, the cover media will experience some distortion due to data hiding and cannot be inverted back to the original media. That is, some permanent distortion has occurred to the cover media even after the hidden data have been extracted out. In some applications, such as medical diagnosis and law enforcement, it is critical to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations. In other applications, such as remote sensing and high-energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free, or invertible data hiding techniques. Reversible data hiding facilitates immense possibility of applications to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out, thus providing an additional avenue of handling two different sets of data.

A number of reversible data hiding methods have been proposed in recent years. In difference expansion method [1], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. A data hider can also perform reversible e data hiding using a histogram shift mechanism, which utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel gray values to embed data into the image [2]. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embed-ding [3]. Furthermore, various skills have been introduced into the typical reversible data hiding approaches to improve the performance [4]–[6]

As is well known, encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. 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.

The reversible data hiding in encrypted image is investigated in [8].Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain [1]–[21].

Manuscript received on January, 2013

Ms.Ashwini Jarali, Department of Computer Engineering/University of Pune, India.

Ms.Jyoti Rao Department of Computer Engineering/ University of Pune, India.

But, in some applications, an inferior assistant or a channel administrator 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. Reference [8] presents a practical scheme satisfying the above-mentioned requirements and Fig. 1 gives the sketch. This work proposes a reversible data hiding scheme for encrypted image, which is made up of image encryption, data embedding and data extraction/ image-recovery phases. The data of original cover are entirely encrypted, and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered. With an encrypted image containing additional data a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, she can further extract the embedded data and recover the original image from the decrypted version. But if someone has the data-hiding key but not the encryption key, she cannot extract any information from the encrypted image containing additional data. That is where the proposed method of unique LSB Compression data hiding method can be used

II. PROPOSED SCHEME

In the proposed scheme (Fig. 2), the original image is encrypted using an encryption key and the additional data are embedded into the encrypted image using a data-embedding key. With an encrypted image containing additional data, if the receiver has only a data-embedding key, she can extract the additional data though she does not know the image content. If she has only the encryption key, she can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If the receiver has both the data-embedding key and the encryption key, she can extract the additional data and recover the original image without any error.

In Fig.2, Em_k refers to data embedding and data extraction key .E_k refers to Image encryption and decryption key. Here symmetric keys are used for encryption and decryption

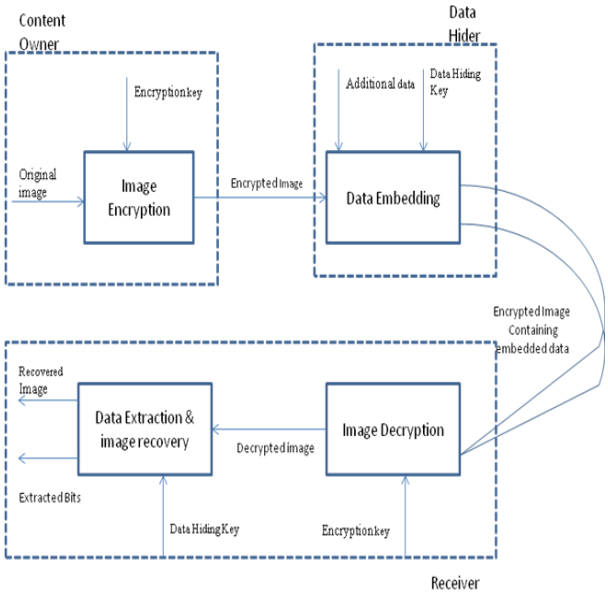


Fig.1 Sketch of Non Separable Reversible Data Hiding

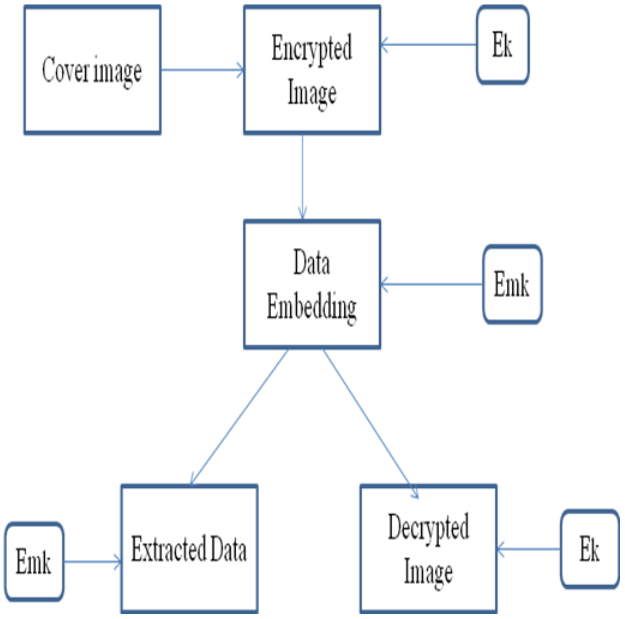


Fig.2. Sketch of Separable Reversible Data Hiding

A. Image Encryption

Suppose the gray scale original image of size N*M is taken then each pixel value falls between 0and 255.it is represented in 8 bits.Lets denote the bits of each pixel as b0,b1,b2,b3…..b7,the no of pixels as Q=N*M and the gray value as Gi.where

$$Gi = \sum_{u=0}^{7} bi * 2u \quad (1)$$

and bi=[Gi/2u]mod 2, i=0,1……..7 (2)

In Encryption phase we take a encryption key Ek, convert it into a standard stream cipher ci. Then compute

Bi=bi ex-or ci (3)

Bi‘s are concatenated in order to form the encrypted data.

B. Data Embedding.

In Data embedding, data hiding key is used by the data hider. Pseudo-random permutation of pixel is done in order to reduce the intelligible information .LSB of encrypted pixels are compressed to create a space for accommodating the additional data and the original data .the detailed steps are as follows.

Steps for Data Embedding

1. Data hider first selects the data hiding key Emk.
2. Some parameters for data hiding are embedded in small number of encrypted pixels Qp.
3. Remaining encrypted pixels(Q-Qp)are pseudo-randomly permuted and divided into number of groups of X pixels. Permutation is dependent on data hiding key.

   $\psi_w = \psi_w(Q)$ (4)

   where ψ_w is pseudo-random permutation operation
4. For each group, select M least significant bits of X pixels . let us denote them as P(j,1.•M) , P(j,2.•M), P(j,3.•M),…… P(j,X.•M) where j is the group index with in [1,(Q-Qp)/X] and M is a positive integer less than 4.
5. The data hider also generates a matrix T of size (M*X-Z)*(M*X), where

   T= $[I_{M \cdot X-Z} S]$ (5)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Where left part is an identity matrix of size (M.•X-Z)* (M.•X-Z), the right part S is (M.•X-Z)*Z is a pseudo-random binary matrix derived from the data hiding key . Z is a small positive integer

6. For each group of X pixel calculate

$$\begin{bmatrix} P(j,i) \\ ; \\ P(j,X*M-Z) \end{bmatrix} = T \bullet \begin{bmatrix} P(j,i) \\ ; \\ P(j,X*M-Z) \end{bmatrix} \quad (6)$$

Where ● is arithmetic modulo-2.

By (6) [P(j,1.•M) , P(j,2.•M), P(j,3.•M),…… P(j,X.•M)] are compressed as (M.•X-Z)bits, and a sparse space is therefore available for data accommodation.

7. Then replace the [P(j,1.•M) , P(j,2.•M), P(j,3.•M),…… P(j,X.•M)] with the new [P'(j,1.•M) , P'(j,2.•M), P'(j,3.•M),…… P'(j,X.•M)] and put them into their original positions by an inverse permutation .
8. After above step, the (8-M) most significant bits (MSB) of encrypted pixels are kept unchanged.

Z bits are embedded into each pixel group; the total $(Q-Qp)\bullet\frac{Z}{M}$ bits can be embedded in all groups. Clearly, the embedding rate R, a ratio between the data amount of net payload and the total number of cover pixels is

$$R=\frac{((Q-Qp)\bullet\frac{Z}{M}-Qp)}{Q}\approx\frac{X}{M} \quad (7)$$

C .Data Extraction and Image recovery

In this phase, we will consider the three cases.

1) The receiver has only the data hiding key : If the receiver has only the data hiding key, with the encrypted image containing embedded data, she may

a) First obtain the parameters M, X, Z from the LSB of the selected Qp pixels.
b) Perform the permutation operation on remaining encrypted pixels.
c) Divide them into (Q-Qp)/X groups and extract Z embedded bits from M LSB planes of each pixel of each group.

Because of the pseudo-random pixel selection and permutation method used the attacker cannot obtain the parameter values and the pixel groups without data-hiding key .Therefore she attacker cannot extract the embedded data .at the same time though the receiver has the data hiding key, she can extract only the embedded data, she cannot get any information about the original image content.

2) The receivers has only Encryption key : If the receiver has only the encryption key, but no data hiding key she may, the original image content can be recovered. but cannot extract the embedded data as required parameters and data hiding key is not known.

Bits of pixels in encrypted image are denoted as B1,B2……..BQ.

The receiver can decrypt the received data as bi′=Bi ex-or ci

Where ci is derived from encryption key

The gray values of decrypted pixel is given by

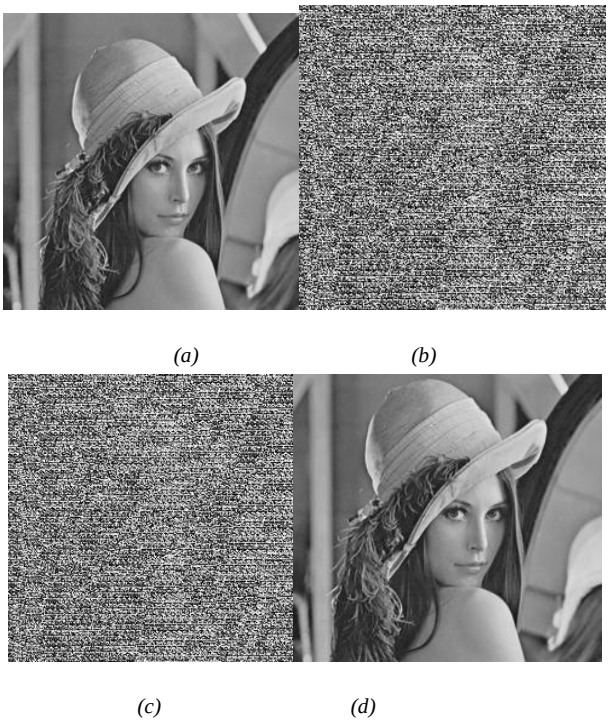
$$Gi=\sum_{u=0}^{7} b'i*2u$$

Since only LSB's are modified the remaining MSB's are almost similar to the original image. According to equation (6) only Z bits are modified in the original image which is significantly less than X*M.

3. The receiver has both the data-hiding key and encryption key.

If the receiver has both the data hiding key, and encryption key, then she may extract both the data embedded and image encrypted as in non separable reversible data hiding method.

Using the data-hiding key, the values of M, X, Z , the original LSB of the Qp selected encrypted pixels the embedded data can be extracted from the remaining (Q-Qp) pixels .



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

Fig. 3 (a) Original Lena,(256×256) (b) its encrypted version, (c) encrypted image containing embedded data with embedding rate 0.023 bpp, and (d) directly decrypted version with PSNR 39.0 dB.

By putting the Qp LSB into their original positions, the encrypted data of the Qp selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys.

III. EXPERIMENTAL RESULTS

The test image Lena sized 256×256 shown in Fig. 3(a) was used as the original image in the experiment. After image encryption, the eight encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig. 3(b). Then, we let X=3,M=128,Z=3 to embed 1536 additional bits into the encrypted image . The encrypted image containing the embedded data is shown in Fig. 3(c), and the embedding rate R is 0.023 bit per pixel (bpp).With an encrypted image containing embedded data, we could extract the additional data using the data-hiding key. If we directly decrypted the encrypted image containing embedded data using the encryption key, the value of PSNR in the decrypted image was 39.0 dB, which verifies the theoretical value 39.1 dB. The directly decrypted image is given as Fig. 3(d).

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

By using both the data-hiding and the encryption keys, the embedded data could be successfully extracted and the original image could be perfectly recovered from the encrypted image containing embedded data.

Tables I and II list the embedding rates, PSNR in directly decrypted images when different M, X and Z were used for images Lena(Fig.4) and Vegetable(Fig.5). The embedding rate is dependent on Z and M and the larger Z and the smaller M correspond to a higher embedding rate. On the other hand, the smaller the values of X and Z, the quality of directly decrypted image is better since more data in encrypted image are not changed by data embedding.

Input Images used for experiments

Fig.4(a)Lena 512*512 pixels

Fig 5.(b)Vegetable 320*240 pixels

TABLE I
Embedding rate, PSNR in directly decrypted images (db) containing embedded data for test image Lena.

		Z=1	Z=2	Z=3	Z=4	Z=5
X=1	M=2000	0.0005 , 55.10	0.0010, 52.83	0.0015, 52.56	0.0020, 51.95	0.0025, 51.54
	M=1500	0.0006 , 54.86	0.0013, 52.42	0.0020, 51.85	0.0027, 51.57	0.0033, 51.25
	M=1000	0.0010 , 54.96	0.0020, 52.51	0.0030, 52.17	0.0040, 51.71	0.0050, 51.27
X=2	M=400	0.0025 , 47.84	0.0050, 45.60	0.0075, 45.04	0.0100, 44.61	0.0125, 44.16
	M=300	0.0033 , 47.74	0.0067, 45.53	0.0100, 45.05	0.0133, 44.56	0.0167, 44.13
	M=200	0.0050 , 47.81	0.0100, 45.56	0.0150, 44.97	0.0200, 44.57	0.0250, 44.16
X=3	M=150	0.0067	0.0133,	0.0200,	0.0267,	0.0333,
		, 41.56	39.23	38.36	38.36	38.00
	M=125	0.0080 , 41.65	0.0160, 39.29	0.0240, 38.79	0.0320, 38.35	0.0399, 37.96
	M=100	0.0100 , 41.54	0.0200, 39.29	0.0300, 38.76	0.0400, 38.32	0.0500, 37.94

TABLE II
Embedding rate, PSNR in directly decrypted images (db) containing embedded data for test image Vegetable

		Z=1	Z=2	Z=3	Z=4	Z=5
X=1	M=2000	0.0004,54.4	0.00094 , 52.5	0.00147 , 52.1	0.00198 , 51.7	0.0025 , 51.22
	M=1500	0.0006, 55.24	0.0014, 52.74	0.0020, 52.2	0.0027, 52.00	0.0033 , 51.53
	M=1000	0.0009, 54.72	0.0020, 52.65	0.0029, 52.1	0.0040, 51.6	0.0050 , 51.27
X=2	M=400	0.0025, 54.36	0.0050, 52.41	0.0075, 52.04	0.0100, 51.59	0.0125 , 51.17
	M=300	0.0033, 47.37	0.0067, 45.36	0.0100, 44.98	0.0133, 44.48	0.0167 , 44.25
	M=200	0.0050, 47.59	0.0100, 45.53	0.0150, 45.14	0.0200, 44.60	0.0250 , 44.23
X=3	M=150	0.0067, 41.27	0.0133, 39.20	0.0200, 38.82	0.0266, 38.28	0.0333 , 37.92
	M=125	0.0079, 41.50	0.0159, 39.14	0.0240, 38.77	0.0320, 38.33	0.0400 , 37.90
	M=100	0.0100, 41.26	0.0200, 39.21	0.0300, 38.76	0.0400, 38.28	0.0500 , 37.93

IV. CONCLUSION

In this work, a novel separable reversible data hiding scheme for encrypted image with a low computation complexity is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases. The original images are entirely encrypted by a stream cipher. Although a data-hider does not know the original content, he can embed additional data into the encrypted image by modifying a part of encrypted image. With an encrypted image containing embedded data, a receiver may decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be correctly extracted while the original image can be perfectly recovered. Although someone with the knowledge of encryption key can obtain a decrypted image, but if he does not know the data-hiding key, it is still impossible to extract the additional data. 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 Furthermore, this algorithm is quite simple, and the execution time is rather short. Therefore, its overall performance is better than many existing reversible data hiding algorithms. It is expected that this reversible data hiding technique will be deployed for a wide range of applications in the areas such as secure medical image data systems, and image authentication in the medical field and law enforcement, and the other fields where the rendering of the original images is required or desired.

REFERENCES

1. J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol. , vol. 13, no. 8, pp. 890–896, Aug. 2003
2. Z.Ni,Y.-Q.Shi,N.Ansari,andW.Su,"Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, 2006.

3. M.U.Celik,G.Sharma,A.M.Tekalp,andE.Saber,"Losslessgeneralized-LSB data embedding," IEEE Trans. Image Process. ,vol.14, no. 2, pp. 253–266, Feb. 2005.
4. L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique,"IEEE Trans. Inf. Forensics Secur., vol. 5, no. 1, pp. 187–193, 2010.
5. W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification, "Signal Process.,vol.90,pp.2911–2922,2010
6. C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data embedding scheme using differences between original and predicted pixel values, "Inform. Secure. , vol. 2, no. 2, pp. 35–46, 2008
7. W. Zeng, "Digital watermarking and data hiding: technologies and applications," in Proc. Int. Conf. Inf. Syst., Anal. Synth., vol. 3, 1998, pp.223–229.
8. X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
9. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in IEEE Trans. on Image Processing , vol. 6. No. 12, pp. 1673-1687, Dec. 1997.
10. J. Huang and Y. Q. Shi, "An adaptive image watermarking scheme based on visual masking," Electronics Letters , 34 (8), pp. 748-750, 1998.
11. B. Chen, G. W. Wornell, "Quantization index modulation: a class of provably good meth-ods for digital watermarking and information embedding," IEEE Transaction on Information Theory, vol. 47, no. 4, pp. 1423-1443, May 2001.
12. An Improved Reversible Data Hiding in Encrypted Images Using Side Match ,Wien Hong, Tung-Shou Chen, and Han-Yan Wu , IEEE SIGNAL PROCESSING LETTERS, VOL. 19, NO. 4, APRIL 2012
13. 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
14. 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.
15. X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inform. Forensics Security, vol. 6, no. 1,pp. 53–58, Feb. 2011.
16. A Survey on Various Data Hiding Techniques and their Comparative Analysis Harshavardhan Kayarkar* Corresponding Author M.G.M"s College of Engineering and Technology, Navi Mumbai, India
17. Stream Encryption Standard for Digital Images, Akhil Kaushik, Satvika Khanna, Manoj Barnela and Anant Kumar, International Journal of Computer and Electrical Engineering, Vol. 3, No. 2, April, 2011
18. Efficient Data Hiding With Plus-Minus One or Two, Xinpeng Zhang, IEEE SIGNAL PROCESSING LETTERS, VOL. 17, NO. 7, JULY 2010
19. An Overview of Reversible Data Hiding, Mohammad Aurangzeb, National University of Singapore, published at ICCIT 2 003, 19- 21 Dec, Jahangirnagar University , Bangladesh, pp 75-79
20. Reversible Data Hiding ,Yun Q. Shi, Department of Electrical and Computer Engineering, New Jersey Institute of Technology.