ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 53-56 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

Data Extraction Using Steganography Techniques in DIP

[1]Kumara Guru Diderot [2] Reddy Girish, [3] Ruby Hazarika

[1] Asst Professor [2] UG Final Year [3] UG Final Year
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
HINDUSTAN UNIVERSITY
Rajiv Gandhi Salai(OMR),Padur,Chennai-603103

[1]pkguru@hindustanuniv.ac.in
[2]gaddamreddygirish@gmail.com
[3]rubyhazarika1220@gmail.com

***Abstract*— The paper discusses about securing of data in an encrypted image. The content owner in the first stage encrypts the original uncompressed image using the encryption key. The data hider then compresses the least significant bits of the encrypted image using data hiding key to create some space to accommodate some extra data. If the receiver has both the data hiding key and the encryption key only then receiver can extract the relevant data and the image.**

***Keywords*— Image encryption, image recovery, reversible data hiding, cryptography, steganography.**

I. INTRODUCTION

Recent day security needs have provoked the development of techniques to secure data. As a popular means for privacy protection, encryption converts the normal signal into a impossible to understandable data. In few cases we cannot trust the processing service provider. It is necessary to keep the data unrevealed . Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. It is differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret Steganography and cryptography are both ways to protect information from unwanted parties. Once the presence of hidden information is revealed or even suspected, the purpose steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

II. ABSTRACT

The transmission of images is a daily routineand it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time,the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem isto try to combine compression, encryption and data hiding in a single step. For example, some solutions was proposed in to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. In this group proper decryption of data requires a key. The second group bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data.

.

III. EXISTING SYSTEM

In the existing system reversible data hiding technique the image is compressed and encrypted by using the encryption key and the data to hide is embedded in to the image by using the same encryption key. The user who knows the secret encryption key used can access the image and decrypt it after extracting or removing the data hidden in the image. After extracting the data hidden in the image then only can be the original image is retrieved. The secret key used for encryption of compressed image and the data hiding is same. So, the user who knows the secret key used for encryption can access the data embedded and the original data.The original Image can be retrieved from the encrypted image after extracting or removing the data hidden in the image. The content owner and the data hider share the same encryption key for the encryption of the Image and data hiding.

IV.PROPOSED SYSTEM

In proposed method the image is encrypted bycontent owner by using the encryption key. The data hider can hide the data in the encrypted image compressing the least significant bits of the encrypted image to obtain the space to hide the data by using data hiding key. At the receiver side the data can be retrieved using the data hiding key by decrypting the image. But, the encrypted image unchanged still it is decrypted using the encryption key. The receiver who has the both the

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 53-56 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

encryption and data hiding keys can access the data embedded as well as the original image.

A. Encrption Of Image

Let the size of image be $N_1 \times N_2$ in uncompressed format and let the gray level value be in the range [0,255] is represented by 8 bits. Let the pixels be denoted as $b_{i,j,0}$, $b_{i,j,1}$ . . . . $b_{i,j,7}$ where $1 \le i \le N_1$ and $1 \le j \le N_2$, the grey value as $p_{i,j}$ and the total number of pixels as N ($N=N_1 \times N_2$). Therefore $b_{i,j,u} = [p_{i,i}/2^u] \bmod 2$, u = 0,1,2, . .7 (a)

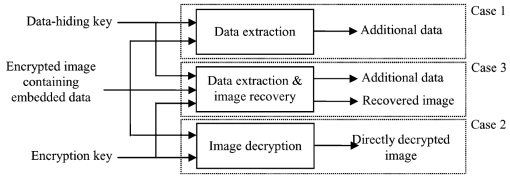


Fig. 2. Three cases at receiver side of the proposed separable scheme.

Then we also have

$P_{i,j}$ =

(b)

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

(c)

Here $r_{i,j,u}$ are determined by an encryptionkey using a standard stream chipper. Then $B_{i,j,u}$ are concatenated as the encrypted data.

B. Data Embedding

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accomadating the additional data and the original data at the positions occupied by by the parameters. The procedure is explained as followed.

In according to the data hiding key, the data hider pseudo-randomly selects N_P encrypted pixels that will be used for carrying data hiding. Where N_P is a small positive integer.for example when N_p=20, the other ($N-N_p$) encrypted pixels are pseudo-randomly permutted and divided into a number of groups, each of which contains L pixels. The data hiding would be determined by the permutation way. In each pixel group, collect L pixels among the M least significant bits and denote them as B(k,1), B(k,2), . . . B(k,M·L) where kis a group index within [1,($N-N_P$)/L] and M is appositive integer less than 5.

The data-hider also generates a Matrix G, which is compressed of two parts

$$G = [I_{M \cdot L} - sQ] \qquad (d)$$

While the left part is an (M·L-S)× (M·L-S) matrix. The right part Q is sized to(M·L-S) × S is a random binary matrix derived from data hiding key

A total of $(N-N_P) \cdot S/L$ bits made up of N_P original LSB are selected and $(N-N_P) \cdot S/L-N_P$ additional bits will be embedded into pixel group. The calculation for each group is done as followed

$$\begin{bmatrix} B'(k,1) \\ B'(k,2) \\ \vdots \\ B'(k,ML-S) \end{bmatrix} = \mathbf{G} \cdot \begin{bmatrix} B(k,1) \\ B(k,2) \\ \vdots \\ B(k,ML) \end{bmatrix} \qquad (e)$$

In encryption phase, the exclusive-or results of the original bits and where the arithmetic is modulo-2.By (e), pseudo-random bits are calculated are compresed as [B(k;1);B(k;2);..;B(k; M·L)] bits, and a sparse space is therefore available for data accommodation . let [B(k;1);B(k;2);..;B(k; M·L)] and put them in there original position by inverse permutation. Since S bits are embedded in the pixel group, the total $(N-N_P) \cdot S/L$ can be accommodated into groups. The embedding rate, a ratio between the data amount of net pay load and the total number of cover pixels is

$$R = \frac{((N-N_P) \cdot S/L - N_P)}{N} \approx \frac{S}{L}. \qquad (f)$$

C. Data extraction and image Recovery

Here we will consider the three cases that a receiver he sonly data hiding key , only the encryption key, and both data hiding key and encryption key respectively.

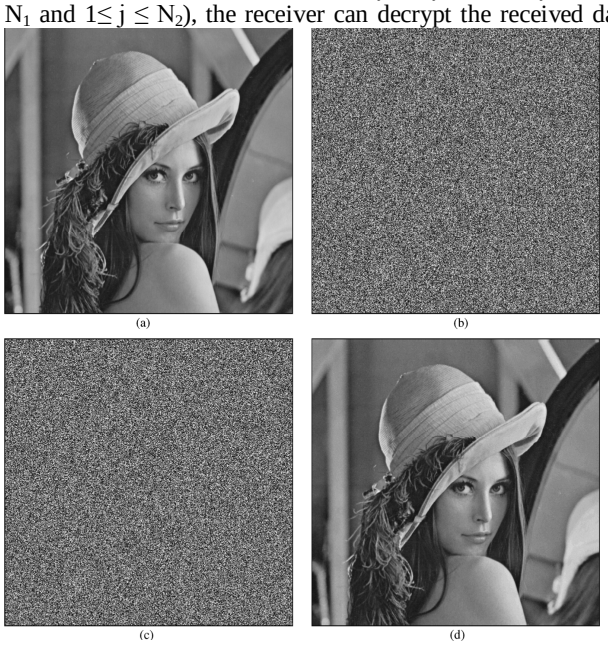
When an encrypted image containg the embedded data, if the receiver has data hiding key alone, he may first obtain the values of the parameters M,L and sS from the LSB of the N_P selected encrypted pixels. Then the receiver permutates and divides the other ,($N-N_P$) pixels into ,($N-N_P$)/L groups and extracts the S embedded bits from the M LSB plane of every group. When having the total ,($N-N_P$) · S/L extracted bits, the receiver can divide them into N_P original LSB of selected encrypted pixels and ($N-N_P$) · S/L-N_P additional bits. Note that because of the pseudo random pixel selection and permutation, any attacker without the data hiding key cannot obtain the parameter values and pixel groups, therefore cannot extract the embedded data . further although the receiver having th e data hiding key can success fully extract the embedded data, he cannot get any information about the original image content.

Consider the case that the receiver has the encryption key but doesnot know the data hiding key. Clearly he cannot

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 53-56 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

obtain the values of the parameter s and cannot extract the embedded data. However the original image content can be roughly covered., Indicating the bits of pixels in the encrypted image containg embedded data as $B_{i,j,0}$, $B_{i,j,1}$, ... $B_{i,j,7}$ ($1 \le i \le N_1$ and $1 \le j \le N_2$), the receiver can decrypt the received data



$$b'_{i,j,u} = B'_{i,j,u} \oplus r_{i,j,u} \qquad \text{(g)}$$

Where $r_{i,j,u}$ are derived from the encryption key. The gray values of the decrypted pixels are

$$p'_{i,j} = \sum_{u=0}^{7} b'_{i,j,u} \cdot 2^u. \qquad \text{(h)}$$

Sice the data embedding operation does not alter any MSB of encrypted image, the decrypted MSB must be same as the original MSB. So the content of the decrypted image is similar to that of the original image .according to (e), there is

$$B'(k,v) = B(k,v), \quad v = 1, 2, \ldots, ML - S. \qquad \text{(i)}$$

The probability of this case is $1/2^S$, and, in this case the original (M·L-S) bits in the M LSB planes can be correctly decrypted. Since S is significantly less than M·L, we ignore the distortion at other S decrypted bits. If there are non zero bits among B(k, M·L-S+1), B(k, M·L-S+2), ... B(k, M·L),the encrypted data in the M LSB planes have been changed by the data embedding operation, so that the decrypted data is in the M LSB planes differ from the original data. Assumping that the original distribution of the data is the M LSB- data. Assuming the original distribution of the data in the M LSB planes is uniform, the distortion energy per each decrypted pixel is

$$D_{\mathrm{E}} = 2^{-2M} \cdot \sum_{\alpha=0}^{2^M-1} \sum_{\beta=0}^{2^M-1} (\alpha - \beta)^2. \qquad \text{(j)}$$

Because the probability of this case is $(2^S\text{-}1)/2^S$, the average energy of distortion is

$$A_{\mathrm{E}} = \frac{(2^S - 1)}{2^S} \cdot 2^{-2M} \cdot \sum_{\alpha=0}^{2^M-1} \sum_{\beta=0}^{2^M-1} (\alpha - \beta)^2. \qquad \text{(k)}$$

Here, the distortion in the N_P selected pixels is also ignored since their number is significantly less than the image size N. So, the value of PSNR in directly decrypted image is

$$\mathrm{PSNR} = 10 \cdot \log_{10}(A_{\mathrm{E}}). \qquad \text{(l)}$$

TABLE I
THEORETICAL VALUES OF PSNR (DB) WITH RESPECT TO S AND M

	$S=1$	$S=2$	$S=3$	$S=4$	$S=5$
$M=1$	54.2	52.4	51.7	51.4	51.3
$M=2$	47.2	45.4	44.7	44.4	44.3
$M=3$	40.9	39.1	38.5	38.2	38.1

Table I gives the theoretical values of PSNR with respect to and If the receiver has both the data-hiding and the encryption keys,he may aim to extract the embedded data and recover the original image. According to the data hiding key, the values of M, L and S, the original LSB of the N_P selected encrypted pixels, and the $(N\text{-}N_P) \cdot S/L\text{-}N_P$ additional bits can be extracted from the encrypted image containing embedded data. By putting the N_P LSB into their original positions, the encrypted data of the N_P selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys. In the following, we will recover the original gray values of the other $(N\text{-}N_P)$ pixels. Considering a pixel-group, because B(k, M·L-S+1), B(k, M·L-S+2), ... B(k, M·L) in (e) must be one of the vectors meeting
are given,

$$\mathbf{v} = \left[B'(k,1)B'(k,2)\cdots B'(k,ML-S)00\cdots 0\right]^T + \mathbf{a} \cdot \mathbf{H} \qquad \text{(m)}$$

where **a** is an arbitrary binary vector sized 1×S, and **H** is an S× M L matrix made up of the transpose of **Q** and an S×S ident ity matrix

$$\mathbf{H} = [\mathbf{Q}^T \ \mathbf{I}_S]. \qquad \text{(n)}$$

In other words, with the constraint of (e), there are 2^S possible solutions $[B(k,1),B(k,2), \ldots ,B(k,M\cdot L)]^T$. for each vector **V,** we attempt to put the elements in it to the original positions to get an encrypted pixel-group and then decrypt the pixel-group using the encryptionkey. Denoting the decrypted pixel-group as G_k and the gray values in it as $t_{i,j}$, calculate the total difference between the decrypted
and estimated gray values in the group

$$D = \sum_{(i,j)\in G_k} |t_{i,j} - \tilde{p}_{i,j}| \qquad \text{(o)}$$

where the estimated gray values is generated from the neighbors in the directly decrypted image, by (p), as shown at the bottom of the page. Clearly, the estimated gray values in

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.2, Pages : 53-56 (2013)
Special Issue of NCRTECE 2013 - Held during 8-9 February, 2013 in SMK Fomra Institute of Technology, OMR, Thaiyur, Kelambakkam, Chennai

(p) are only dependent on the MSB of neighbor pixels. Thus, we have 2^S different ***D*** corresponding to the 2^S decrypted pixel-group $\boldsymbol{G}_k$. Among the 2^S decrypted pixel-group, there must be one that is just the original gray values and possesses a low ***D*** because of the spatial correlation in natural image. So, we find the smallest ***D*** and regard the corresponding vector ***V*** as the actual $[B(k,1),B(k,2), \ldots ,B(k,M\cdot L)]^T$. and the decrypted $t_{i,j}$ as the recovered content. As long as the number of pixels in a group is sufficiently large and there are not too many bits embedded into each group, the original content can be perfectly recovered by the spatial correlation criterion. Since the 2^S different ***D*** must be calculated in each group, the computation complexity of the content recovery is $\boldsymbol{O(N\cdot 2^S)}$. On the other hand, if more neighboring pixels and a smarter prediction method are used to estimate the gray values, the performance of content recovery will be better, but the computation complexity is higher. To keep a low computation complexity, we let be less than ten and use only the four neighboring pixels to calculate the estimated values as in (p).

$$\tilde{p}_{i,j} = \frac{\lfloor p'_{i-1,j}/2^M \rfloor + \lfloor p'_{i+1,j}/2^M \rfloor + \lfloor p'_{i,j-1}/2^M \rfloor + \lfloor p'_{i,j+1}/2^M \rfloor}{4} \cdot 2^M + 2^{M-1}$$

(p)

REFERENCES

[1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “Oncompresing encrypteddata,”IEEETrans.Signal Proces.,vol.52,no.10,p.292–306,Oct.204.
[2] W.Liu,W.Zeng,L. Dong, and Q.Yao, “Ef?cientcompresionofen-cryptedgrayscaleimages,”IEEETrans.ImageProces.,vol.19, no.4, p.1097–102,Apr.2010.
[3] X. Zhang, “Losy compresion and iterative reconstruction for en- cryptedimage,”IEEETrans.Inform.Forensics Security,vol.6,no.1, p.53–58, Feb. 201.
[4] T.Bianchi, A.Piva, and M.Barni, “On the implementation of the discreteFouriertransform in the encrypteddomain,”IEEETrans.Inform. ForensicsSecurity,vol.4,no.1,p.86–97,Feb.209.