IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 7, July 2016

Lossless and Reversible Data Hiding

Mayuri B. Lokhande[1], **Prof. N. G. Pardeshi**[2]

PG Student, Computer Engineering, SRES's College of Engineering, Kopargaon, India [1]

Assistant Professor, Computer Engineering, SRES's College of Engineering, Kopargaon, India [2]

Abstract: The paper proposes a lossless, a reversible, and a combined data hiding schemes for encrypted images. It uses the concept of Reversible data hiding and Lossless data hiding concept. Using these concepts the data can be embedded into cover image which is encrypted. For encryption of cover image, paillier algorithm is used. The paillier algorithm generates the pair of public private key. In contrast to using an existing cover image to hide messages, the algorithm conceals the source image and embeds secret messages using. This allows extracting the secret messages and source image from a embedded data in encrypted image. The approach offers some advantages. First, the scheme offers the embedding capacity that is proportional to the number of pixel in image. Second, the reversible capability inherited from this scheme provides functionality, which allows recovery of the cover image.

Keywords: Data embedding, reversible, lossless, histogram shrinks.

I. INTRODUCTION

There are various techniques available for data protection. Out of which encryption and data hiding are two effective means of data protection. The encryption techniques convert plaintext content into unreadable cipher text. The data hiding techniques embed additional data into cover media. The data can be embedded by introducing slight modifications. Data hiding may be performed with a lossless or reversible manner.

In the proposed system the terms "lossless" and "reversible" will be distinguished. In the previous references these two terms have the same meaning. If the display of cover signals containing embedded data is same as that of original cover even though the cover data have been modified for data embedding, in this case we can say that the data hiding method is lossless. If the original cover content can be perfectly recovered from the cover version containing embedded data even though a slight distortion has been introduced in data embedding procedure, in this case we can say that the data hiding scheme is reversible.

II. LITERATURE SURVEY

Xinpeng Zhang and Kuriyama [1] proposed a practical reversible data hiding scheme. The optimal rule of value modification under a payload distortion criterion is found by using an iterative procedure.

This work first finds the optimal value transfer matrix by maximizing a target function of pure payload with an iterative procedure, and then proposes a practical reversible data hiding scheme. The differences between the original pixel-values and the corresponding values estimated from the neighbors are used to carry the payload that is made up of the actual secret data to be embedded and the auxiliary information for original content recovery.

Advantage:

- The optimal transfer mechanism gives a new rule of value modification and can be used on various cover values.

Disadvantage:

- The computation complexity due to the prediction will be higher.

Subhanya R.J Anjani Dayanandh N. [2] uses the watermarking algorithm that embeds image/ text data invisibly into a video based on Integer Wavelet Transform and to minimize the mean square distortion between the original and watermarked image and also to increase PSNR.

Advantage:

- This approach can improve the quality of the watermarked image and give more robustness of the watermark and also increasing PSNR.

Disadvantage:

- Low hiding capacity.
- Complex computations.

X. Zhang. [3] proposed the a novel scheme for separable reversible data hiding, which consists of image encryption, data embedding and data extraction/ image-recovery phasespatch-based sampling and used the feathering approach for the overlapped areas of adjacent patches.

Advantage:

- The method is simple less computation is required.

Disadvantage:

- Data compression is not efficient.

DOI 10.17148/IJARCCE.2016.5764

W. Puech, M. Chaumont, and O. Strauss [4] showed that data embedding is performed in encrypted domain and authorized receiver can recover the original plaintext image and extract the embedded data.AES is used for data encryption.

Disadvantage:

- Quality of decrypted image degrades.

Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li [5] have developed the system by reserving room before encryption. To make the data hiding process effortless, extra space is made empty in the previous stage.

Advantages:

- The method can take advantage of all traditional RDH techniques achieves the excellent performance for the plain images and without loss of any secrecy.
- This novel method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images.

III.SYSTEM DESIGN

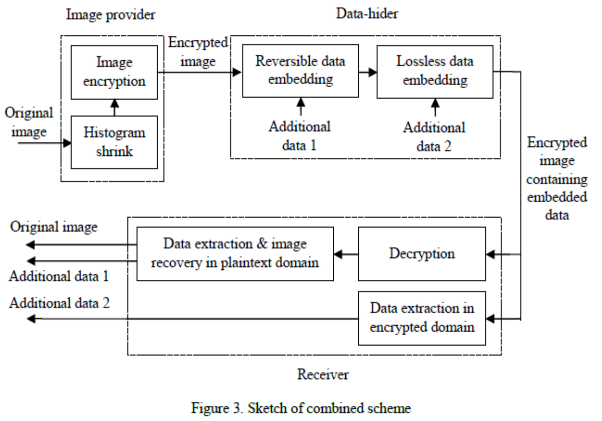


Fig. 1. System Architecture

Fig. 1 shows the system for A Lossless and Reversible Data Hiding in Encrypted Images.

The proposed system includes the following modules:

1. Histogram Shrink.
2. Image Encryption Module
3. Data Embedding module.
4. □Data extraction and image decryption module.

A. Image Encryption Module :

- Initially the histogram of original image is considered.
- From that original histogram new histogram is constructed.
- The value of this histogram is converted into binary stream bs1.
- The peak of new histogram is found by image provider.

$$V = \underset{\delta+1\leq v\leq 255-\delta}{\arg\max}\, h'_v$$

- The image provider also divides all pixels into two sets: the first set including (N−8) pixels and the second set including the rest 8 pixels, and maps each bit.
- Then, a histogram shift operation is made,

$$m_T(i,j)=\begin{cases} m_S(i,j) & , \text{ if } m_S(i,j)>V \\ V & , \text{ if } m_S(i,j)=V \text{ and the corresponding bit is 0} \\ V-1 & , \text{ if } m_S(i,j)=V \text{ and the corresponding bit is 1} \\ m_S(i,j)-1 & , \text{ if } m_S(i,j)<V \end{cases}$$

- At last, the image provider encrypts all pixels using a public key cryptosystem.

B. Image Encryption Module:

- Select the source image which is to be used as cover medium.
- Using Paillier algorithm the selected cover image is encrypted.

Algorithm:

- Select two large prime p and q.
- Calculate the product n=p x q.
- Choose semi random non zero integer g(Randomly chosen by mathematica),g has order multiple of n gcd (L(g^λ(n) mod n^2),n)=1
  Where L(t)=(t-1)/n and λ(n)=lcm(p-1,q-1)
- The public key is composed of (g,n), while the private key is composed of (p,q, λ)
- Encryption of message is given by C=g^mr^n mod n^2
- Decryption is given by
  m=(L(g^λ(n) mod n^2)/(L(g^λ(n) mod n^2))mod n

C. Data Embedding Module:

- The string are stored in sequence as data 1 and data 2.
- The message is also converted in byte array. C'(i,j)=C(i,j).(r'(i,j))^{n}modn^2
  Where c'(i,j) is the changed ciphertext.

D. Data Extraction and Image Decryption Module

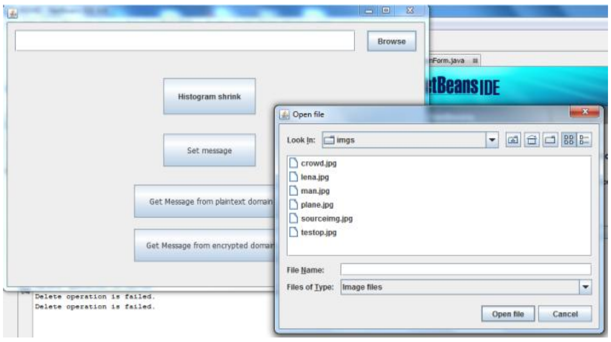
- Data can be extracted in two different domain.
- Data 1 i.e one added using reversible scheme is extracted in the decrypted domain, meaning the image is decrypted first and then the hidden data is extracted into it.
- Data 2 is extracted in the encrypted domain itself.
- Using reversible scheme we get the original cover image as well as the hidden data.

IV.EXPERIMENTAL RESULTS

We are going to evaluate this video inpainting approach on the ICDAR dataset. The performance of video inpainting scheme is evaluated by calculating peak signal to noise ratio. If PSNR of inpainted video sequence is high, then it can be said that a high performance is achieved with this approach.The output of the implemented modules of the system is as follows:

DOI 10.17148/IJARCCE.2016.5764

A. Select source image to hide data


Browse
Histogram shrink
Set message
Get Message from plaintext domain
Get Message from encrypted domain
Open file
Look In: imgs
File Name:
Files of Type: Image files
Open file
Cancel

crowd.jpg
lena.jpg
man.jpg
plane.jpg
sourceimg.jpg
testop.jpg

```
Delete operation is failed.
Delete operation is failed.
```

Fig. 2 Select source data

B. Histogram Shrink:

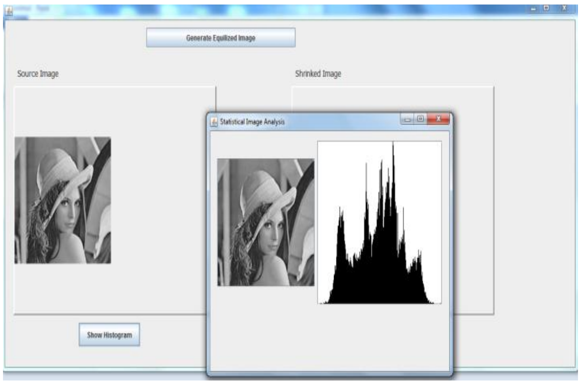
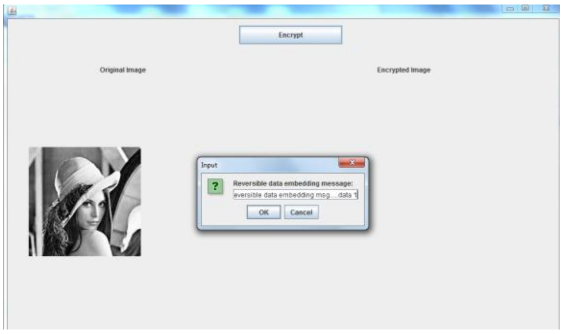


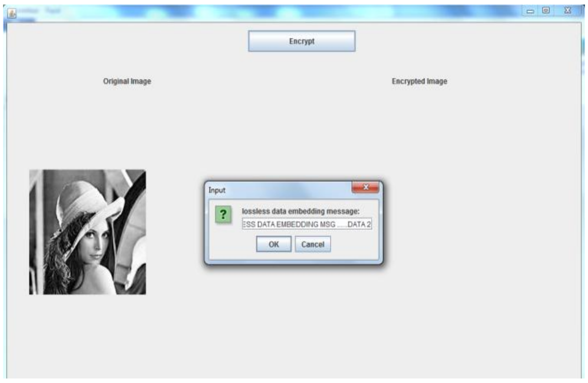
Fig. 3.Generated equalised image and histogram.

C. Message Embedding:



Reversible data embedding message:
eversible data embedding msg....data 1

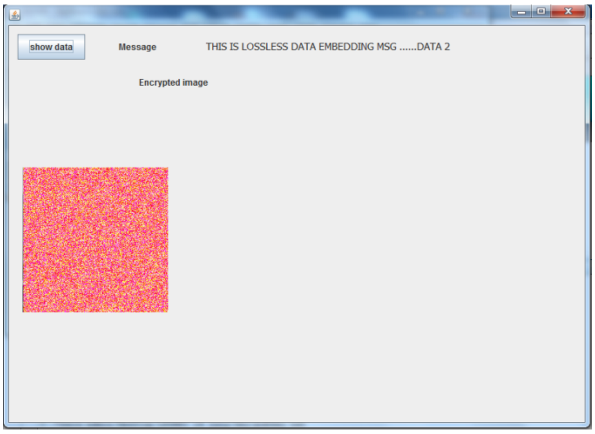
Fig. 4.Embedding Data Using RDH



lossless data embedding message:
ESS DATA EMBEDDING MSG ......DATA 2

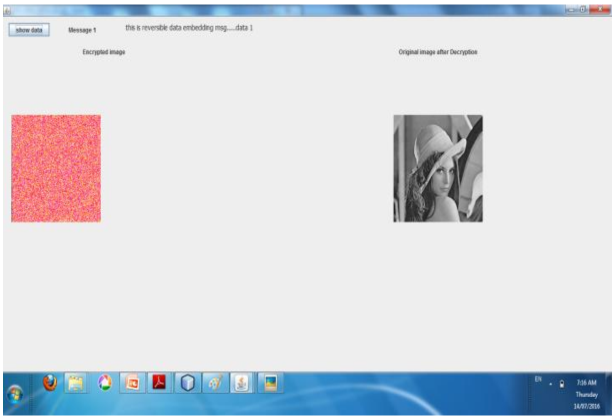
Fig. 5.Embedding Data Using LDH

D. Data Extraction And Image Decryption:



Message THIS IS LOSSLESS DATA EMBEDDING MSG ......DATA 2

Fig 6 Data Extraction of data in encrypted domain (LDH)



Message 1 this is reversible data embedding msg.....data 1

Fig.7Data Extraction of data in decrypted domain (RDH)

Result Analysis:

Table 1: Computing time (seconds)

	PSNR(dB)			
Embedding rate (bpp)	Lena	Plane	Man	Crowd
0.005	67.16	65.94	57.49	67.22
0.01	63.44	63.18	55.71	64.13
0.05	55.46	57,02	50.19	56.75
0.1	52.33	54.2	46.17	52.62
0.2	49.07	50.98	40.68	49.1
0.3	45	48.26	35.87	45.21
0.4	40.65	44.67	31.16	41.24
0.5	35.84	40.78	25.92	35.99

Table 2: Embedding Capacity & PSNR

Sr.no	Size of image	Computing time in (ms)
	160 x 120	16ms
2	314 x 235	30ms
3	512 x 512	32ms
4	1920 x 2560	93ms

DOI 10.17148/IJARCCE.2016.5764

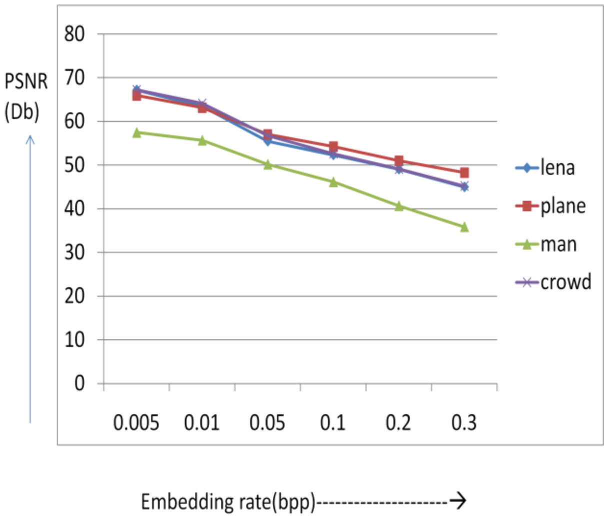


Fig. 8.Graph of Embedding Rate Vs PSNR

V. CONCLUSION

The system proposes a combined approach using a lossless and reversible data hiding approach. The secrete data is hidden in the encrypted cover image. Using reversibility concept it is possible to recover the original source image. The approach provides reversibility to retrieve the original cover image. The presented algorithm is secure and robust. The proposed scheme offers substantial benefits and provides an opportunity to extend data hiding applications.

ACKNOWLEDGMENT

I would like to take this opportunity to express our profound gratitude and deep regard to my Project Guide **Prof. N. G. Pardeshi** sir, for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the work. His valuable suggestions were of immense help throughout my project work. His perceptive criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience for me.

REFERENCES

[1] Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng, “Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography”, IEEE Transactions on Circuits and Systems for Video Technology.

[2] X. Zhang, “Reversible Data Hiding with Optimal Value Transfer,” IEEE Trans. on Multimedia, 15(2), 316−325, 2013

[3] X. Zhang, “Separable Reversible Data Hiding in Encrypted Image,” IEEE Trans. Information Forensics & Security, 7(2), pp. 526−532, 2012.

[4] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, “High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis,” Digital Signal Processing, 20, pp. 1629−1636, 2010.

[5] J. Tian, “Reversible Data Embedding Using a Difference Expansion,” IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.

[6] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible Data Hiding,” IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.

[7] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless Generalized-LSB Data Embedding,” IEEE Trans. on Image Processing, 14(2), pp. 253–266, 2005.

[8] X. Hu, W. Zhang, X. Li, and N. Yu, “Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding,” IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.

[9] W. Zhang, X. Hu, X. Li, and N. Yu, “Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications,” IEEE Trans. on Image Processing, 24(1), pp. 294-304, 2015.

[10] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative Encryption and Watermarking in Video Compression,” IEEE Trans. on Circuits and Systems for Video Technology, 17(6), pp. 774−778, 2007.

BIOGRAPHY

Mayuri B. Lokhande received the B.E. Degree in Information technology from University of Pune, Pune, Maharashtra, India in 2013. She is currently pursuing the M.E. Degree in Computer Engineering with SRES Sanjivani College of Engineering, Kopargaon, Savitribai Phule Pune University, Pune, Maharashtra, India. Her current research interests include Image Processing.