ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Analysis and Implementation of High Efficient Steganography Using Patch Level sparse Representation

Sonali. M. Pawar

M. E Student, Dept. of E&TC, N.B.N. Sinhgad College of Engineering, Sholapur, India

ABSTRACT: This paper provides an overview of a proposed dissertation work-Analysis and implementation of high efficient steganography using patch level sparse representation. As we know in recent years, steganography has become very popular and a lot of research is being done in this field. Reversible data hiding is a method in which the image in which the encrypted data is hidden is losslessly recovered. In this paper I have proposed a method for reversible data hiding in encrypted images. This field has attracted considerable attention from the communities of privacy, security and protection, the proposed work will focus on the patch level sparse representation for hiding secret data. Because the pixels in the local structure (patch) have a strong similarity, as the sparse coding is an approximation solution, the leading residual errors will be encoded and self-embedded within the cover image. Furthermore, the learned dictionary is also embedded into the encrypted image. By this, a large space for hiding secret data can be achieved, and thus the data hider can embed more secret message bits in the encrypted image.

KEYWORDS: Steganography, RDH, sparse representation

I. INTRODUCTION

The basic concept of steganography is to hide the very presence of communication by embedding message into the cover objects. Reversible data hiding (RDH) is a method to hide (embed) additional message into some distortion free unacceptable cover media. Reversible data hiding in images aims to exactly recover both the embedded secret information and the original cover image. It has attracted intensive research interests. Military, medical and legal scenarios are its typical examples, in which even a slight distortion is not tolerable. Data hiding are a group of technique to hide secret data into images which is called a cover images. Most hiding technique embeds the message into the cover image to obtain the marked image by modifying only the least significant part of the cover image. This embedding can cause some distortion to cover image and hence, unable to reconstruct the original image from the marked image.

In most applications, small distortions due to data embedding are allowed whereas in applications like medical, law forensics and military imagery, no distortions are allowed. For these cases, we require a special kind of data hiding method, which is called as reversible data hiding (RDH). Reversible Data Hiding (RDH) is used to embed a piece of data into an image to generate a marked image and after extracting process the original image can be recovered from the marked image. It is also called as invertible or lossless data hiding. The hiding rate and quality of the marked image are important parameters for the measurement of the performance of the RDH algorithm as the increase in the hiding rate causes more distortion in the image content.

Here a patch-based RDHEI scheme. Although some other methods also divide the cover image into patches to perform RDHEI, their definition is mainly to consider the correlation of pixels within the patch. Therefore, they are kind of the pixel-level compressive methods essentially. In contrast, I regard the patch as a whole, and represent them using a small number of coefficients, which is beyond the traditional pixel-level case. And thus a high capacity room is available & in turn the efficiency is increased.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

II. RELATED WORK

Many RDH algorithms have already been developed, such as image compression-based [1], [2], difference expansion based [3]–[7], histogram shift (HS)-based [8]–[11], image pixel pair based [12], [13], and dual/multi-image [14], [15] hiding methods. Recently, due to the requirement of privacy protection, the cover owner usually encrypts the original content before transferring it to the data manager. Meanwhile, the data manager may want to embed additional messages into the encrypted image for authentication or steganography, even though the content of the original image is unknown to him. In this situation, hiding data in the encrypted image is an intuitive and effective way to meet such requirement. To hide data in encrypted domains, some digital watermarking based schemes are proposed. Besides, the commutative watermarking and ciphering schemes for digital images are introduced. Although the methods mentioned above have provided promising performance in encrypted domains, they are insufficient for more sensitive military and medical scenarios, where the image content should be not only kept secret strictly, but also be losslessly recovered after data extraction. Therefore, RDH in encrypted images (RDHEIs) is desirable. To this end, many RDHEI schemes have been proposed in past years.

One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the three LSBs of the cover-image with the message bits, which is kind of the pixel-level compressive methods essentially. In the encrypted image is segmented into a number of non overlapped blocks, while each block is divided into two sets. Each block carries one bit by flipping three LSBs of a set for predefined pixels. Hong et al gave an improved version. Specifically, they fully harness the pixels in calculating the smoothness of each block and consider the pixel correlations in the border of neighboring blocks. The resulting error rate of extracted-bits is thereby decreased. The proposed method creates a sparse space to accommodate some additional data by compressing the LSBs of the encrypted image.

III. DESIGN & IMPLEMENTATION

Methodology for the proposed work- Analysis and implementation of high efficient steganography using patch level sparse representation is presented in the following figure.

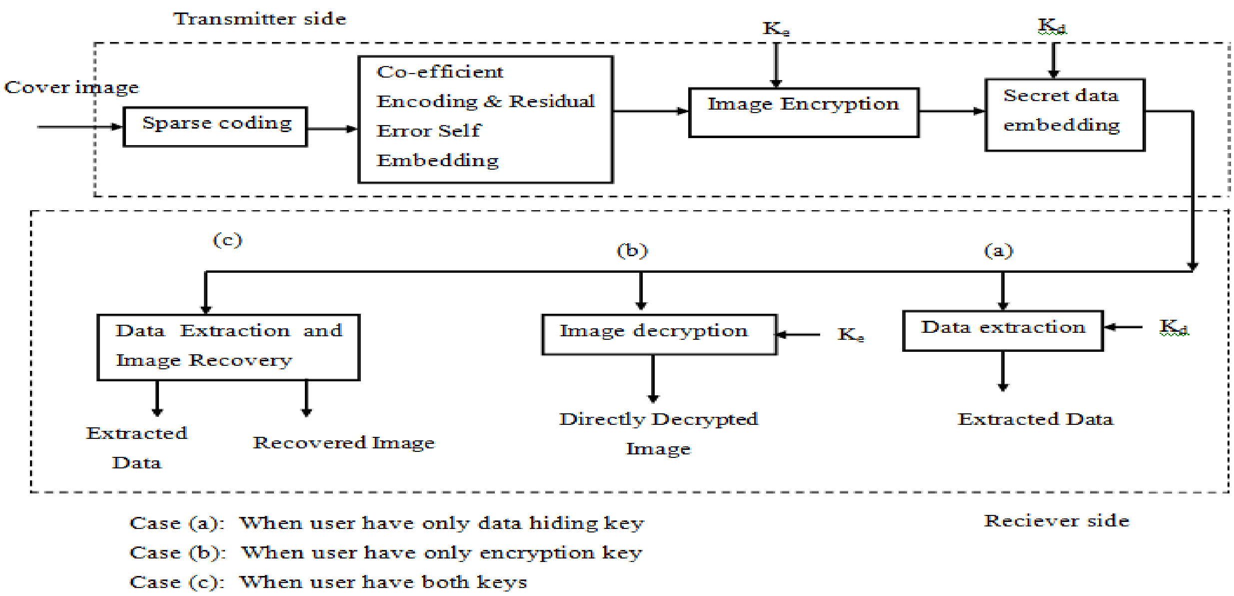

Fig.1: Overview of proposed system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A. ***DESCRIPTION OF THE PROPOSED ALGORITHM:***

The proposed framework aims to perform 3 main operations.
1. Encrypted image generation
2. Data embedding in encrypted image
3. Data extraction and image recovery
First two operations will be performed at transmitter side and third will be at receiver side.

Transmitter: Transmitter consists of 4 blocks as-
1. Sparse coding
2. Coefficient encoding and residual error self embedding
3. Image encryption
4. Secret data embedding

1. Sparse coding:
Given a cover image of size 512*512, first divide it into patches of size 4*4 that are then represented according to an over complete dictionary via sparse coding. Then, the smoother patches with lower residual errors are selected for room reserving. These selected patches are represented by the sparse coefficients.

2. Coefficient encoding and residual error self embedding:
After the cover image is represented by sparse coefficients, for the given selected patches, the corresponding coefficients and reconstructed residual errors will be encoded directly without quantization. Here, for losslessly recovering the cover image, corresponding residual errors are reversibly embedded into the other nonelected patches with a standard RDH algorithm. The learned dictionary will be also embedded into the encrypted image for further use. The output of this block will be selected patches with a space reserved for further data hiding.

3. Image encryption:

Finally, the room preserved and self-embedded image is encrypted using stream cipher to generate the final version.

4. Secret data embedding:
Once the encrypted image is received, the data hider will embed secret data for management or authentication requirement. The standard RDH algorithm will be used for this data hiding. After data hiding, the position of the first data hiding patch and the hiding room size for each patch are also embedded into the encrypted image containing additional embedded data with RDH algorithm.
Finally this encrypted image with hidden data will be transmitted to the receiver.

Receiver: With the encrypted image containing additional embedded data, the receiver faces three situations depending on whether the receiver has data hiding and/or encryption keys. The data extraction and image decryption can be processed separately.

1. Data Extraction With Only Data Hiding Key:
For the receiver who only has data hiding key K_d. It will first extract and compute the starting position and the hiding room size for each patch and divides the received image into non-overlapped N × N patches. Then, data extraction will be finished by checking the last n^d (parameter bits) bits for the selected patches in the received image. After that, all original hidden data are extracted and recovered with the data hiding key K_d.

2. Image Decryption With Only Encryption Key:
In this the receiver will have the encryption key K_e only. After extraction the position of the first selected patch by RDH algorithm, all the selected patches will be identified one by one. Moreover, the dictionary D is will be also obtained by extraction. After patch segmentation of the received image, the decryption procedure will be performed and it will include two cases as unselected patch decryption and selected patch decryption.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

3. **Data Extraction and Image Recovery With Both Data Hiding and Encryption Keys:**

If the receiver has both the data hiding key K_d and encryption key Ke, the data extraction and image recovery will achieve full reversibility. On the one hand, with the data hiding key K_d, one can extract the hidden secret data without any error. On the other hand, with the encryption key Ke, will first perform directly image decryption, then the corresponding coefficient for selected patches will be obtained. After that, the residual errors will be extracted from the non-selected patches & the recovery patch is computed.

Dictionary training:

For reserving room to hide data, we train the dictionary based on K-means singular value decomposition (K-SVD) algorithm which is widely used for designing over-complete dictionaries that lead to sparse signal representation. The K-SVD training is an offline procedure, and the corresponding dictionary produced by training is then considered fixed for the whole RDH procedure. Given a cover image **I** with size $N1 \times N2$, we first divide it into a bunch of non overlapped $N \times N$ patches. Denote S as the number of patches of **I**, and $S = N1 \times N2/N \times N$. Using an over complete dictionary matrix **D** that contains K prototype signal atoms for columns, every image patch **y***i* can be represented as a sparse linear combination of these atoms.

The dictionary is trained for 50 images. For training the dictionary, the sample image from database is taken. If the selected image is the color image then this color image is converted to gray scale image. For processing in MATLAB, the window length of 8 is decided and the number of rows and columns of the selected image are calculated. The dictionary is trained using k-svd algorithm using the command.

IV. EXPERIMENTAL RESULTS FOR DICTIONARY TRAINING

The implementation of this project is done in MATLAB R2014a. Here in this project, publicly available standard images for training of the sparse dictionary are taken and these images will be processed.

1. Image acquisition: Publically available standard images are used for training the sparse dictionary. Here, for understanding perpose the demo images available in MATLAB are taken.

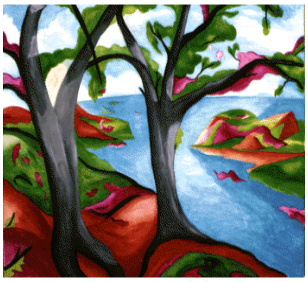

Fig 3.1: original image

Fig 3.1 shows original image which is the MATLAB demo image 'trees'. This is input for dictionary training. This image is then converted into gray scale image using the MATLAB commands.

Fig 3.2: grayscale image

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Fig 3.2 shows the gray scale image generated by MATLAB. The obtained grayscale image is processed horizontally and vertically and is converted into a dictionary patch of pixel size 8*8. The patch after processing will look llike as follows:

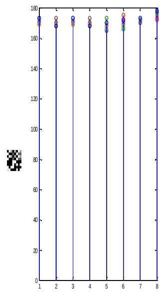

Fig 3.3: selected patch & pixel intensity values of selected patch

Fig 3.3 shows the plot of selected patch in the image with its pixel intensity values. Pixel values are the floating point values.

V.CONCLUSION

In this paper, the work is completely done by using MATLAB 14a. This paper has proposed a novel method called the HC_SRDHEI, which inherits the merits of RRBE, and the separability property of RDH methods in encrypted images. Compared to state-of-the-art alternatives, the room vacated for data hiding by our method is much larger used. The performance analysis implies that our proposed method has a very good potential for practical applications.

REFERENCES

[1] Xiaochun Cao, Ling Du, Xingxing Wei, Dan Meng and Xiaojie Guo, "High Capacity Reversible Data Hihing In Encrypted Images By Patch Level Sparse Representation" IEEE Transactions on cybernetics, VOL. 46, NO. 5, MAY 2016
[2] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images," in *Proc. Inf. Technol. Coding Comput.*, Las Vegas, NV, USA, Apr. 2001, pp. 223–227.
[3] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013
[4] Hao-Tian Wu, Jean-Luc Dugelay and Yun-Qing Shi, *Reversible Image Data Hiding with Contrast Enhancement"* IEEE Transaction on SIGNAL PROCESSING, VOL. 22, NO. 1, JANUARY 2015
[5] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, *Dept. of Computer Science Narain College of Technology, Bhopal(India) "A Survey On Different Image Encryption and Decryption Techniques." International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 – 116*
[6] M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2,pp. 253–266, Feb. 2005.
[7] J.Fridrich, M. Goljan, and R. Du, "Invertible authentication watermark for JPEG images," in Proc. Inf. Technol. Coding Comput., Las Vegas, NV, USA, Apr. 2001, pp. 223–227.
[8] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, and H. G. Choo, "A novel difference expansion transform for reversible data embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 456–465, Sep. 2008.
[9] D. Coltuc, "Improved embedding for prediction based reversible watermarking," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3,pp. 873–882, Sep. 2011.
[10]M. U. Celik, G. Sharma, and A. M. Tekalp, "Lossless generalized- LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.
[11] X. Li, B. Ying, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[12] Y. Hu, H. K. Lee, K. Chen, and J. Li, "Difference expansion based reversible data hiding using two embedding directions," *IEEE Trans. Multimedia*, vol. 10, no. 8, pp. 1500–1511, Dec. 2008.
[13] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise predictionerror expansion for efficient reversible data hiding," *IEEE Trans. Image Process.*, vol. 22, no. 12, pp. 5010–5021, Dec. 2013.
[14] W. L. Tai, C. M. Yeh, and C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 6, pp. 906–910, Jun. 2009.
[15] C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognit.*, vol. 41, no. 12, pp. 3582–3591, Dec. 2008.