ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Research Article***
www.ijptonline.com

A STEGANOGRAPHIC TECHNIQUE BASED REGION LEVEL SPARSE REPRESENTATION FOR HIGH DENSITY DATA HIDING

S. Hemalatha*[1] and L.Giridharan[2]
[1]School of Information Technology & Engineering, VIT University, Vellore-632 014, Tamil Nadu, India.
[2] School of Information Technology & Engineering, VIT University, Vellore-632 014, Tamil Nadu, India.
Email:shemalatha1079@gmail.com

Received on 10-05-2016 *Accepted on 09-06-2016*

Abstract

In this paper, a new steganographic method is proposed using region-level sparse representation for high density reversible data hiding. Reversible data hiding (RDH) is widely used in the field of secured communication. Using reversible data hiding, large amount of private messages can be embedded within one image and a stego image can be generated. In this work, the huge similarity of adjacent pixels of in sub image regions is efficiently utilized for reversible data hiding. In order to understand the relationship between pixels in a neighborhood, region-level sparse representation is used. The encryption and decryption processes used in the proposed steganographic technique apply auto keying and manual keying methods. Thus, the confidentiality of the data is increased. Sparse coding technique is used for the patch level linear representation of pixels considered over complete dictionary.

Keywords: Reversible Data Hiding, Difference Expansion, Sparse Representation, Minimum Embedding Rate, Singular Value Decomposition.

Introduction

Data hiding process in images covers a wide range of applications for embedding text message in images [1, 2]. Unavoidably, the data hiding process inserts distortion in the host image. Although, the distortion created by data hiding is invisible to the humans, there are some delicate images such as medical images and military images, for which, the distortion is unbearable. Particularly, for medical images, little bit distortions are insufferable. Therefore, reversible data hiding methods[3, 4, 5, 6, 7] are developed to address the issue of lossy insertion of text messages in images. Thus, once the inserted text is mined from the image, the original image is fully restored.

Basically, in reversible data hiding, the confidential text message is encrypted and inserted into a cover image to obtain a stego image, Since the stego image is very much similar to the cover image, the text message hidden in the stego image cannot be noticed by a third party. When the stego image is received by the authorized user, the encrypted text message is decrypted using an appropriate algorithm and the cover image is restored using the recovery algorithm.

Reversible data hiding techniques are classified into different classes such as compression based technique [8], histogram-based method[9, 4, 5], difference expansion method [10], dual-images method [6, 10]. Compression-based techniques usually extricate the features of the cover image that are least significant and compress them. Then, these features replaced with by compressed results and the text messages to be hidden.

Since, the least significant features are used for replacement; the image distortion is reduced considerably. But, the insertion rate is very less due to compression. The reversible contrast mapping technique [9, 11] concentrates on recovering both the cover image and the text message.

Many RDH algorithms have been already developed such as image compression based method[8], difference expansion based method[10], histogram shift based method[4, 5, 9], image pixel pair based method [7] and dual/multi image hiding[6, 10] methods. Digital watermarking method is used in [7, 8, 11, 12, 13], hiding the text message in an encrypted image.

Even though the above mentioned methods have provided satisfactory performance by the encryption method, they are insufficient to be used for delicate military and medical applications. Because, by using these methods, the cover image and the text message are kept confidential, but, lossless recovery of the cover image is not confirmed.

In this paper, the image is analyzed at the region level rather than at the individual pixel level. Since, regions contain contextual information; this method is advantageous in terms of computation and generalization. The huge similarity between adjacent pixels is represented by region level sparse representation and the text message is hidden in the cover image. The widely used sparse coding method has demonstrated that a region can be linearly represented by a complete dictionary. With the high density representation of a sparse coding, a large space can be achieved and thus the huge amount of data can be hiddenan hence in the encrypted image.

The remainder of this paper is organized as follows: Section 2 deals with the proposed method, planning, overview and detailed explanation of the project. Section 3 deals with the Implementation. Section 4 deals with Conclusion.

1. Proposed system

2.1. Working Model

The block diagram of the proposed system is shown in Figure 1. Inthis paper, the cover image and secret information are secured where, thecover holder needs to secure the original image. It is proposed to consider the patch-level sparse representation when hiding the secret data and by using K-SVD algorithm the selection of cover image for the original secret image by the relationship between the neighborhood pixels have stronger similarity between the patches. As the smoother patches have low error bits and if any changes made in the smoother patches of the cover image the difference of the image pixel has less difference than different patches in the image. And for the cryptography technique we are using Huffman encoding for the security and the requirement of privacy protection. It provides the separate keying for both data hiding and image hiding and auto keying and manual keying methods for additional protection for safer and secure transmission of image to other end.

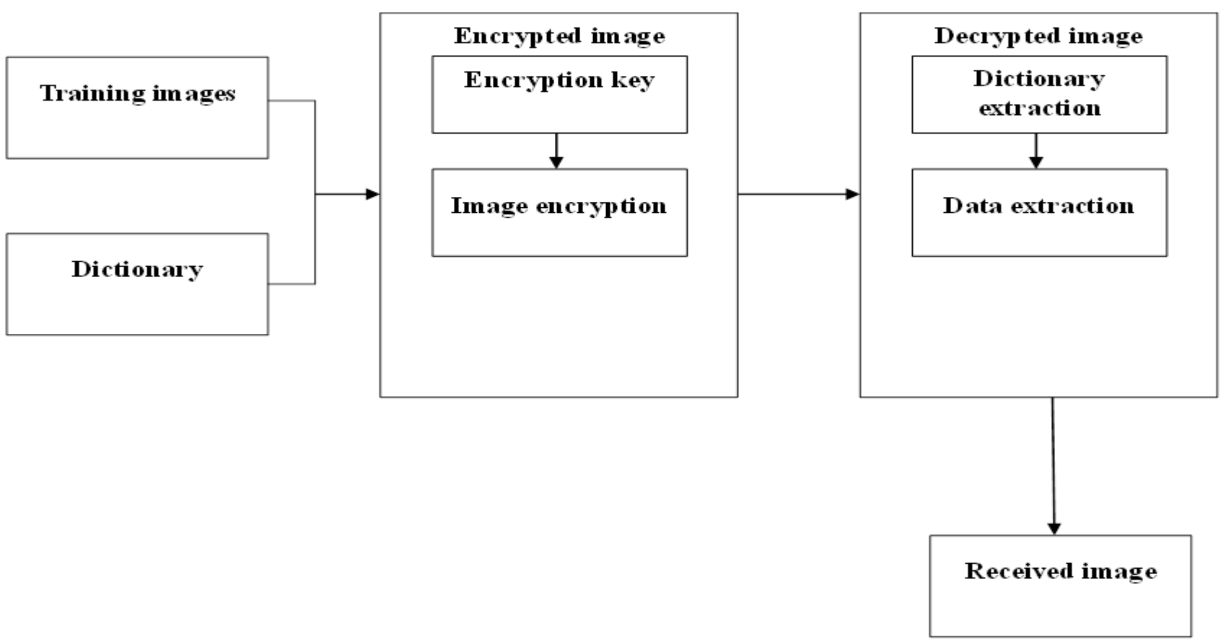


Figure 1. Block Diagram.

2.1.1. K-SVD algorithm

Singular value decomposition (K means single value) which is widely used for designing over complete dictionaries that lead to region level 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 that the cover image I with size $N_1 \times N_2$ we first divide it into a group of non-overlapped $N \times N$ patches Unless stated, the patch size N is set to 5 as default in our algorithm. Denote S as the number of patches of I, and$N_1 \times N_2/N \times N$. For each patch, the pixel value are vectorized as$y_i \in R^{n\times 1}$ (*i=1,2,…..,S*, and$n = N^2$),From equation (1)which contain S column vectors. Therefore the image $I \in R^{n\times S}$, which contains S column vectors. Using an overcomplete dictionary matrix$\boldsymbol{D} \in R^{n\times K}$ $(K > n)$that contain prototype signal atoms for columns, every image patch y_i can be represented as a sparse linear combination of these pixels.

$$min_x \|y_i - Dx_i\|_2^2 \qquad subject\ to \quad \|x_i\|_0 \leq L \qquad (1)$$

Actually, the approximation of $\boldsymbol{y_i}$ using$\boldsymbol{Dx_i}$need not to be exact, and could absorb a moderate error. In other words the representation of y_i may be either exact $\boldsymbol{y_i = Dx_i}$ or approximate$\boldsymbol{y_i \approx Dx_i}$,From equation (2)**.** This suggests an approximation that trades off accuracy of representation with its simplicity. Therefore we can make an error correction step for loseless image recovery in Figure 2.

$$.Y_i = round(Dx_i) + e_i \qquad (2)$$

Here $\bar{e}_i$ considered as the residual error, which contains the reconstructed error caused by sparse coding.

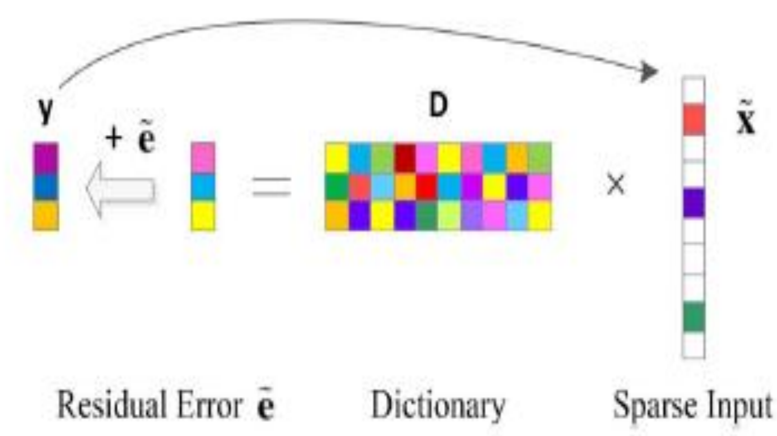


Figure 2. SVD algorithm.

2.1.2. Self-Reversible Embedding :

For room reserving, we select several patches to construct a smoother area A for room reserving, which contains C column vectors. Here C is the selected patch number, and the size of area A is nC. As smoother patches selection is done by analyze the length of error bits, and observing which patches are simple to represent. The patches with smaller error bits are likely ot be smoother than the patches with the larger ones. For example, the background, parts of face or parts of clothes will be simpler than the other complex ones such as eyes and hair. C is the selected patch number is the result of sorting it to ascending order. Note that Figure 3the smoother area selection is dependent on the cover image and is different from smooth and complex image.

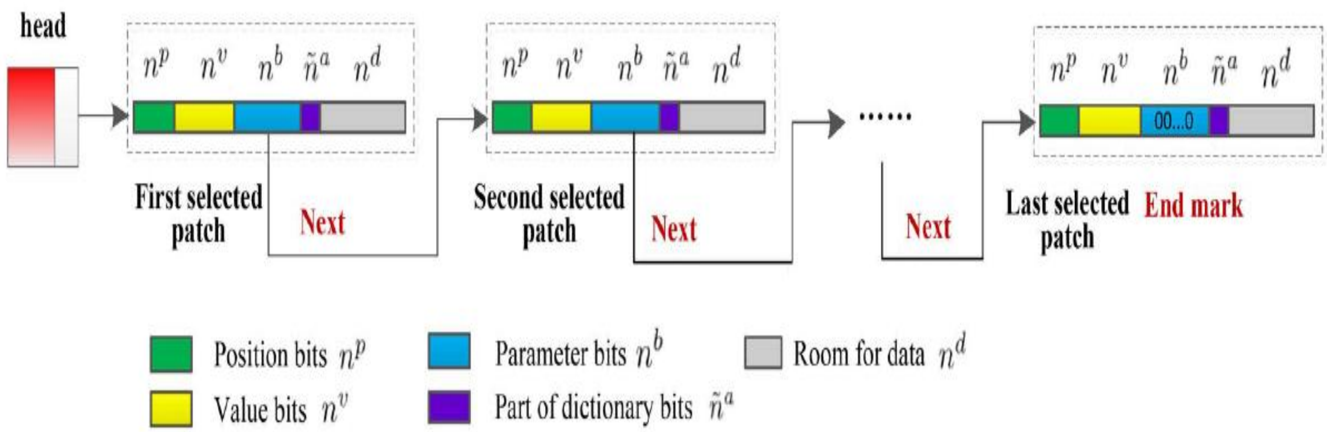


Figure 3 Self-reversible embedding.

2.1.3. Image Encryption:

For the room preserved self-embedded image I_c, we generate the encrypted imageI_e by z stream cipher. Denote the eight bits of the pixel $p_{i,j}$(i=1,2,….N_1,j=1,2,…N_2) as $b_{i,j,0}$,$b_{i,j,1}$,$b_{i,j,2}$, $b_{i,j,3}$, $b_{i,j,4}$,$b_{i,j,5}$, $b_{i,j,6}$ and $b_{i,j,7}$

$$b'_{i,j,m} = b_{i,j,m} \oplus r_{i,j,m} \qquad (3)$$

Where$_{i,j,m}$ is a pseudo random bit generated by the encryption key K_e using stream cipher. After encryption (3), we set the parameter bit in the selected patch to inform that data hider in the next patch that can be embedded. Here the encryption and decryption complete by encryption key $K_e$or data hiding key.

2.1.4. Data Hiding in Encrypted image

Once the encrypted image is received the data hider can insertion secret text for authentication. The insertion process starts in the smoother area of the cover image A. Image owner has insertion the position of the first patch the room size for each patch is encrypted, the data hider doesn't known about the where and how many bits they can modify. After that the data hider examines the encrypted image I_e, minimum embedding rate (MER) (4)and simply used for data hiding.

$$MER = \frac{C \times (8N^2 - L(n^p + n^v) - n^b) - n^a}{N_1 \times N_2} \qquad (4)$$

Where, n^a denoted as dictionary size, n^p position bits of the cover image, n^v value bits of the image, n^b parameter bit of the patches in the cover image, N_1 and N_2 are the original secret image. L denoted as nonzero elements in the secret image.

After data hiding, the first position of the cover image hiding patch and the large vacated room size of each patch are embedded into stego image with the additional embedded data by cryptography technique.

2.1.5. Data Extraction and Image Recovery

The encrypted image can have some additional data, the receiver face three different situation on whether the receiver has the data hiding key and/or Imaging key.

1) ***Data Extraction With only Data hiding key:*** For the receiver who only has data hiding key *K*, he first mines and calculates the starting position and the hiding room size for each patch and divides the received image into non over lapped $N \times N$ patches. Then, data mined is finished by checking the last *n* bits for the selected patches in the received image. After all that the original hidden data are mined and recovered with the data hiding key *K*.
2) ***Image Decryption Only With Encryption Key:*** In this case, the receiver has the encryption key K only. After extraction the position of the first selected patch by RDH algorithm
3) ***Data Extraction and Image Recovery:*** If the receiver has both data hiding and Encryption key the data extraction and original image recovery can be achieved easily.

3. Results and Discussion

Sample 1: Select the secret image for suitable cover image by using sparse representation

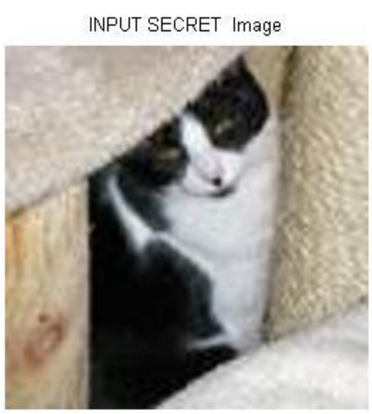
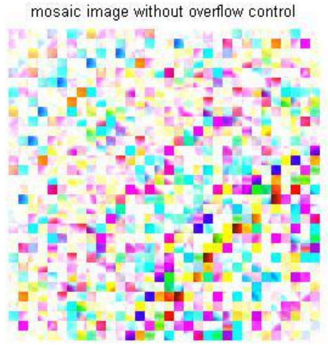


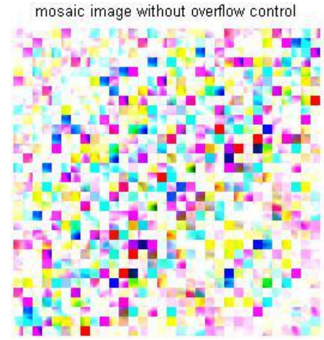
Figure 4. Sample 1

In Sample 1, the Original secret image is selected the suitable cover image for steganography using K-SVD algorithm.

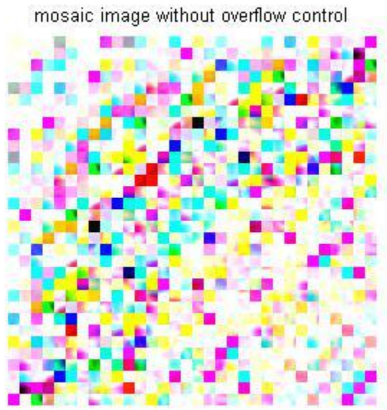
Sparse Representation 2: The mosaic image for the selected cover image from different direction like 0, 90, 180 and 360 degree and selecting the over flow control image for lossless data compression in the selected cover image.



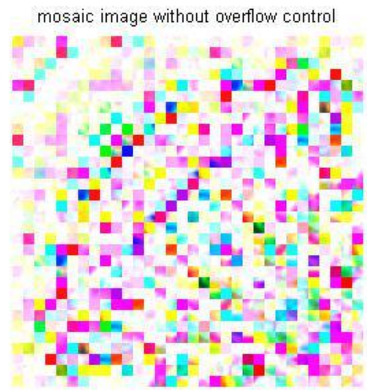
(a) 0 degree image



(b) 90 degree image



(c) 180 degree image



(d) 360 degree image

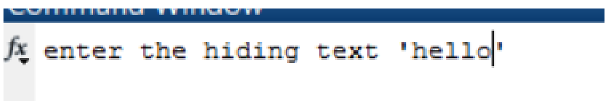
Figure 5. Sparse representations at various degrees.

From Figure 5, the control overflow image is select based on the cover image as selecting the neighbor pixels as the smoother patches have the strong correlation. For example we are hiding the sample text “hello” the hiding text are hidden through smoother patches, so that the cover image doesn’t give much difference after cryptographic technique.

In Figure 6, after the mosaic image has been selected, the secret image is embedded into the cover image as steganography image.

Figure 6. Secret image embedded into cover image.

In Figure 7, the secret text message is embedded into the cover image. The hidden text message is needed to be embedded to the cover image for transmission of secure data to the other end as stego image.



(a) Secret text

(b) Stego image

Figure 7. The stego image

Figure 8 shows the cryptographic technique by using huffman coding by using both manual and auto keying technique.

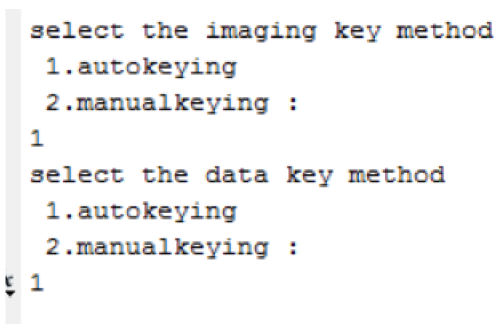
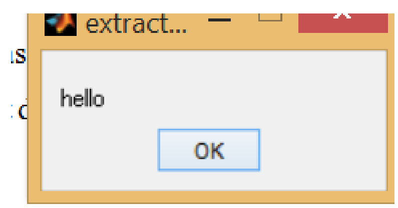


Figure 8. Encryption process.

As the receiver side receives the cover image the receiver need to enter the data hiding key and image hiding if necessary for the manual keying.

In Figure 9, the Last part of the implementation part is shown, i.e. the receiver has extracted the both original secret image and secret data or text

(a) Extracted secret image



(b) Extracted secret message

Figure 9. Extracted secret image and secret message

The original secret image and additional secret image has been extracted to the receiver securely and this method increases the additional security by cryptography technique.

4. Conclusion

This paper provides an effective method for Reversible Data Hiding for encryption in images. By using sparse representation, a larger space is available data hiding than the existing methods. The data hiding text can simply endorse the available space from the cover image with the additional secret data. In this project, we use of relationship of adjacent pixel with similar patches by the region-level sparse representation when hiding the secret data. The decryption part of the proposed method has separate keys for the data hiding and image encryption, making the method free of errors. Thus, the security is increased significantly. Hence, the proposed method is found to be safe and secure for practical and sensitive applications.

Our proposed method has the satisfactory performances for hiding capacity, compression ratio, and decompression quality through color space. However, different parameters need to be improved in future.

References

1. M. Wu and B. Lin, "Data hiding in image and video: Part I-fundamental issues and solutions," *IEEE Trans. Image Process.*, vol. 12, no. 6, pp. 685–695, Jun. 2003.
2. M. Wu, H. Yu, and B. Liu, "Data hiding in image and video: Part IIdesigns and applications," *IEEE Trans. Image Process.*, vol. 12, no. 6, pp. 696–705, Jun. 2003.
3. C. F. Lee and Y. L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations," *J. Telecommun.Syst.*, vol. 52, no. 4, pp. 2237–2247, 2013.
4. Reversible Data Hiding Based on Histogram Modification of Pixel Differences Wei-Liang Tai, Chia-Ming Yeh, and Chin-Chen Chang, *Fellow, IEEE June 2009.*
5. Improving Histogram-based Reversible Information Hiding by an Optimal Weight-based Prediction SchemeShih-Lun Lin Jan 2013.
6. (*k*, *n*)-Image Reversible Data HidingGwoboa Horng1, Ying-Hsuan Huang1, Chin-Chen Chang2;3;∗ and Yanjun Liu3;41Department of Computer Science and Engineering,National Chung Hsing University, Taichung 40227, Taiwan April 2014.

7. S. Weng, Y. Zhao, J. S. Pan, and R. Ni, "Reversible watermarking based on invariability and adjustment on pixel pairs," *IEEE Signal Process.Lett.*, vol. 15, no. 20, pp. 721–724, Dec. 2008.
8. Z. Zhao, N. Yu, and X. Li, "A novel video watermarking scheme in compression domain based on fast motion estimation," in *Proc. IEEE Int. Conf. Commun. Technol.*, 2003, pp. 1878–1882.
9. T. C. Lu and Y. H. Huang, An effective lossless hiding technique based on reversible contrast mapping and histogram embedding methods, *Proc. of the 5th International Conference on InformationAssurance and Security*, pp. 299-602, 2009.
10. Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion Biswapati Jana1, Debasis Giri2 and Shyamal Kumar Mondal3International Journal of Network Security, Vol.18, No.4, PP.633-643, Aug 2015.
11. D. Coltuc, and J. M. Chassery, Very fast watermarking by reversible contrast mapping, *Journal of IEEE Signal Processing Letters*, vol. 14, no. 4, pp. 255-258, 2007.
12. A commutative digital image watermarking and encryption method in the tree structured Haar transform domain M. Cancellaro a, F.Battisti a, M.Carli a, _, G.Boato b, F.G.B.DeNatale b, A.Neri Nov 2010.
13. S. W. Weng, Y. Zhao, R. R. Ni, and J. S. Pan, "Parity-invariability based reversible watermarking," *Electron. Lett.*, vol. 45, no. 20, pp. 1022–1023, Sep. 2009.

Corresponding Author:

S. Hemalatha*,

Email:shemalatha1079@gmail.com