An Efficient RDH Algorithm for Data Separation and Image Retrieval in Fused Image

V.Archana[#1], N.Kalaivani[*2], V.Srividhya[*3], S.Panimalar[*4], Dr.S.Hemalatha[*5], Dr.T.Kalaichelvi[*6]

[1,2,3]*Final Year, Department of Computer Science and Engineering, Panimalar Institute of Technology,Chennai*

[4]*Assistant Professor, Department of Computer Science and Engineering, Panimalar Institute of Technology, Chennai*

[5,6]*Professor, ,Department of Computer Science & Engineering, Panimalar Institute of Technology, Chennai*

Abstract— This efficient novel proposes the implementations of [RDH] Reversible data hiding techniquewith an adaptive high embedding capacity by using the [LSB] Least significant method to embed the data into the fused image. RDH can be used in important and sensitive areas like military applications where image secrecy is maintained. This method helps to hide or encrypt a data into an image with full embedding efficiency and the original content can be losslessly recovered and also includes the watermarking algorithm. The existing algorithm used generalized integer transformation [GIT] which was used for embedding process and generalized and adaptively embeds additional bits into different kinds of blocks. Thus, to enhance the security while encryption and decryption and to minimize the distortion and achieve security to the embedded data the RDH algorithm is used.

Keywords— Reversible data hiding, least significant bit, Discrete wavelet transform, data embedding.

1. Introduction

Stegnography is the process to hide the communication and embedding a data into an image to ensure security and secure transmission of the data or information from sender to the authorized receiver. Reversible data hiding has attracted much interest over the past decades and intensively studied in the community of signal processing.

Using RDH, a message can be embedded into the original or host image, and the original message can be losslessly recovered from the original image. The technique of RDH is applied in some sensitive areas where there is no permanent change is allowed on the original or host signal. The existing RDH methods has different categories like compression based RDH ([1][3]), quantisation based RDH ,expansion based ([2][5][6]), Histogram based RDH ([4]) and integer transformation([7]-[10]) which explains the various implementations of RDH techniques. Also referred as invertible or lossless data hiding, RDH is to embed a piece of data which is to be hidden from a third party or from eaves dropping into a host signal to produce the marked one, and from which the original signal can be recovered after extracting the embedded information. The Discrete wavelet transform method is applied for the watermarking process and the data is embedded into the fused image. Both the image and data are encrypted using Least significant bit where the MSB bit of the data is embedded to the LSB of the image of the first pixel, this whole process is called as reversible data hiding. It then uses the AES for encryption of the data and the image and for the decryption process the data is recovered from the fused image using the key which is given to encrypt. Thus, the data and the image are recovered without any loss and full efficiency is obtained in the proposed paper.

2. Literature Review

Table 1: Articles with its advantages and disadvantages

S.No	Base Paper Title	Techniques Used	Advantages	Disadvantages
1	A Recent Survey of Reversible Watermarking Techniques by A. Khan, A. Siddiqa, S. Munib, and S. A. Malik.,Sep. 2014	Viterbi algorithm Data embedding Syndrome coding scheme	It gives up any ambitions for perfect secrecy. It is more flexible. It is not only limited to binary embedding operations but also embed changes dynamically. The embedding operation need not be shared with recipient.	This allows reliable detection of embedding changes. An adversary can usually rather easily identify statistical quantities that beyond the chosen model. It is costly.
2.	Expansion Embedding Techniques For Reversible Watermarking by Diljith M. Thodi and Jeffrey J. RodríguezMar. 2007	Digital watermarking Expansion embedding. Difference	This method enables data embedding without loss of any information. This method improves the quality of watermarked images.	This method suffers from undesirable distortion at low embedding capacity.

		expansion.		
3	Recursive Histogram Modification Establishing Equivalency Between Reversible Data Hiding and Lossless Data Compression by W. Zhang, X. Hu, X. Li, and N. Yu,"Jul 2013.	DCT algorithm. Redundant bit.	Redundant bits can be modified without detectable degrading the cover medium. The bits should be selected in which the hidden information should be placed. It securely shares the information.	To prevent detection of steganographic content we need to reduce the size of the hidden message. It decreases the hidden message capacity.
4.	Reversible Data Hiding, byZ. Ni, Y. Q. Shi, N. Ansari, and W. Su, Mar 2006	Universal distortion function.	This method covers smooth regions and clean edges. Higher frequency rate.	Relating distortion to statistical detectability is hard and open problem. It is very complex to implement. Its performance is poor.
5.	Efficient Generalized Integer Transform for Reversible Watermarking byX. Wang, X. Li, B. Yang, and Z. Guo, Mar 2008	Reversible watermarking Integer transform.	It can be applied to blocks of arbitrary size. The other is establishing a payload-dependent location map which occupies small payload. We can select the blocks with better expandability based on a distortion estimation function.	That allows reliable detection of embedding changes. It is costly.
6.	Reversible image watermarking using interpolation techniqueby L .Luo, Z.Chen, M. Chen, X. Zeng, and Z. Xiong, Apr. 2007	Watermarking Interpolation robustness	Very low distortion Relatively large capacity We utilize an interpolation technique to generate residual values named interpolation-errors and expand them by addition to embed bits.	This model is easy to attack the secure message. Huge capacity.
7	Reversible image watermarking using interpolation techniqueby L .Luo, Z.Chen, M. Chen, X. Zeng, and Z. Xiong, Apr. 2007	Watermarking Interpolation robustness	Very low distortion Relatively large capacity We utilize an interpolation technique to generate residual values named interpolation-errors and expand them by addition to embed bits.	This model is easy to attack the secure message. Huge capacity.
8.	Adaptive Reversible Data Hiding by Extending the Generalized Integer Transformationby YingqiangQiu, ZhenxingQian, Jun. 2010	Integer transformation. Reversible data hiding.	Use of after encryption techniques enables to encrypt the whole data and image. It maintains the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality.	The hackers recover the embedded data in original image, because the data placed in particular bit position. This method embeds the data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction/image restoration.
9.	Reversible watermarkUsing the difference expansion of a generalizedInteger transformby Adnan M. Alattar, Jan.2016	Difference expansion. Data embedding stegnography	Very high data hiding capacity has been developed for colour images. It is more flexible. High efficient and significant	It is easy for hackers to recover the secure messages. It is costly.
10	Very fast watermarking by reversible contrast mapping by Adnan M. Alattar. Aug. 2004	Embedding bit-rate Reversible contrast mapping	This method does not need additional data compression. It provides high data embedding bit rate at very low mathematical complexity.	Mathematical complexity of RCM scheme is very low ,so LUT implementation becomes costly.

3. Existing System

In the existing system more attention is paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be lossless recovered after embedded data is extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image. Previous methods implement RDH

in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption.

3.1 Drawbacks of Existing System

- The hackers recover the embedding data in original image because the data placed in particular bit positionwhich may be subject to some errors on data extraction and/or image restoration.
- Previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.
- To attack the hidden data using original image because referred the key value.

4. Proposed System

This method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of perfect secrecy. This method can achieve real reversibility, separate data extraction and greatly improvement on the quality of marked decrypted images. This method by reserving room before encryption with a traditional RDH algorithm, and thus it is easy for the data hider to reversibly embed data in the encrypted image. We can achieve real reversibility, that is, data extraction and image recovery are free of any error. The watermarking process and the embedding of data into the fused image is shown in figure 1.

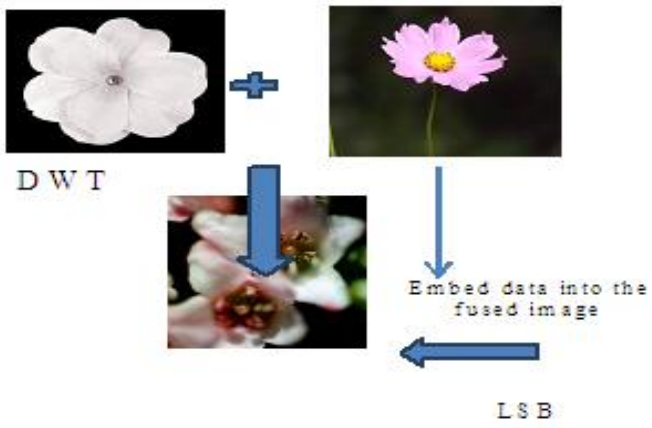

Fig.1: Watermarking of two images and data embedding

5. Module Description

5.1 Image Fusion

The first module is the image fusion where two images will be taken from the database and is fused/watermarked using the discrete wavelet transform DWT method where the image will be split as four quadrants like low, vertical value, horizontal value and the diagonal of the two images and fused to get the watermarked image and use IDWT to convert the whole image to binary format. It works just as shown in fig.1 and table 2 shows the four quadrants in which the image is divided using DWT.

LL	*H(0°)*
V(90°)	*D(45°)*

Table 2. Four quadrants split of image using DWT

5.2 Data Embedding

This model describes about the data embedding for secret sharing. Here data is embedded into a watermarked image. To embed a data into a watermarked image we use a LSB Steganography Technique which hides the data in the least significant bits of pixels color. For embedding data into a watermarked image first we need to convert both data and image into binary values. Then MSB bits of data will be embedded into the LSB bits of image. The resulting changes that are made to the least significant bits are too small to be recognized by the human.

5.3 Encryption Images

Encryptionis a process which uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. Cryptographic algorithms normally require a set of characters called a key to encrypt data. In encryption, we are using AES algorithm to hide the information from the data into the images. AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix .

5.3.1 High-Level Description of the AES Algorithm

- Key Expansion—round keys are derived from the cipher key
- Initial Round:
  - AddRoundKey—each byte of the state is combined with the round key using bitwise xor
- Rounds
  - SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
  - ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
    - MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    - AddRoundKey
- Final Round (no MixColumns)
  SubBytes

ShiftRows
AddRoundKey

5.4 Decryption Images

In the decryption module the watermarked image which contains the data embedded and encrypted is decrypted by using the encryption key given in the AES algorithm. While decrypting the image and the data which is embedded is extracted separately with full efficiency and accuracy from the watermarked image. Thus, ensuring full secrecy while decrypting and achieve real reversibility that is, data extraction and image recovery are free of any error.

6. Experimental Results

In the existing system of using generalized interger transformation the hackers recover the embedding data in original image because the data placed in particular bit position.Previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration.To attack the hidden data using original image because referred the key value. The proposed system overcomes the above drawbacks and thus This method can achieve real reversibility, that is, data extraction and image recovery are free of any error.It is easy for the data hider to reversibly embed data in the encrypted image. This method can embed more than 10 times as large payloads for the same image quality as the previous methods.

7. Conclusion

A novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction or image-recovery phases. It encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data hiding key to create space to accommodate the additional data. With both the keys, the additional data and the original content can be recovered exploiting the spatial correlation and with efficient embedding and more data can also increases the capacity of the data to be embedded. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation.

References

[1] A. Khan, A. Siddiqa, S. Munib, and S. A. Malik, “Recent Survey of Reversible Watermarking Techniques”,Inf.Sci. Vol. 279, pp.251-272, Sep. 2014
[2] DiljithM.Thodi and Jeffrey J. Rodríguez ,“Expansion Embedding Techniques for Reversible Watermarking ,”IEEE Trans. Image Process., Vol. 16, no.3, pp. 721-730, Mar. 2007
[3] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, “Reversible Data Hiding,” IEEE Trans. Circuits Syst.Video Technol., Vol.16,no.3,pp.354-362,Mar 2006
[4] 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, pp. 721-724, Mar 2008
[5] L .Luo, Z.Chen, M. Chen, X. Zeng, and Z. Xiong, “Reversible Image Watermarking Using Interpolation Technique,” IEEE Trans.Inf.ForencicsSecur., Vol. 5, no.1, pp. 187-193, Jan. 2010
[6] D.Coltuc and J.M.Chassery, “Very fast watermarking by reversible contrast mapping,” IEEE Signal Process.Lett., Vol.14, no.4, pp. 255-258, Apr. 2007
[7] X. Wang, X. Li, B. Yang, and Z.Guo, “Efficient Generalized Integer Transform for Reversible Watermarking,” IEEE Signal Process.Lett., Vol.17, no.6, pp. 567-570, Jun. 2010
[8] YingqiangQiu, ZhenxingQian, and Lun Yu, “Adaptive Reversible Data Hiding by Extending the Generalized Integer Transformation,” IEEE Signal Process.Lett., Vol.23, no.1, pp. 130-133 Jan.2016
[9] Adnan M. Alattar, “Reversible Watermark Using the Difference Expansion of A Generalized Integer Transform,” IEEE Trans. Image Process., Vol. 13, no.8, pp.1147-1156, Aug. 2004