Indian Journal of Emerging Electronics in Computer Communications
Vol.4, Issue 1 (2017) Page.630-637
ISSN: 2393-8366

An Analysis on Efficient Reversible Data Hiding Technique in Image Processing

Anigha Johnson[1], Ajeesh S[2], Anoopa Jose Chittilappilly[3]

[1]PG Scholar, [2]Assistant Professor, [3]Head,
Department of Electronics Communication Engineering, IES College of Engineering, Thrissur, India.
anigha333@gmail.com[1],ajeesh.ec@gmail.com[2],anoopajosec@yahoo.co.in[3]

Abstract: *Communication plays a major role in the technological field. Data hiding is one such application of communication where a secrecy or protection is maintained throughout a particular communication. The paper introduces a new technology for data hiding in image processing, called rhombus prediction embedding algorithm with boundary expansion. The paper also made an analysis of the compression of a location map that plays a major role in increased embedding efficiency. Later the entire hidden data can be retrieved with making no change in the original image thereby showing perfection in data retrieval from the image after use. The entire data hiding system for a particular image has been tried to analyzed and conclude in ModelSim software in VHDL language and MATLAB.*

Keywords*- Rhombus prediction, embedding efficiency, VHDL, MATLAB, boundary expansion, ModelSim.*

1. Introduction

Data hiding comes from a very efficient ancient art of communication among people in a protected manner. There are various techniques for data hiding. Image processing plays an important role in data hiding, where the message to be transferred is embedded in form of a compressed data beyond an image. Even though a lot of new emerging technologies have come in this field, the main aim of all of them remains still the same- to maintain secrecy in communication purposes. The major reasons behind data hiding are to avoid misuse of data, prevent accessing data from unauthorized identities, etc. Data embedding in image processing is by means of software process. The data to be sent is embedded in an image and at the same time one can analyze the embedding capacity of a particular image.

In this paper, a new algorithm called rhombus prediction double layered data embedding has been modified with boundary expansion to enhance the embedding capacity. The image that is the host for data hiding has been first converted to a block of pixels. In the algorithm, the adjacent pixels of a selected pixel for data embedding have been selected. The selection is based on the pattern in which the adjacent pixels lay, say a shape called rhombus. Hence the name rhombus algorithm. Boundary expansion allows inclusion of entire image for data embedding thereby increasing the embedding capacity to thousands of pixels. In data hiding a location map is created which is mandatory. In order to prevent the data overflow underflow conditions, pixels have been assumed as 0 to 1 and 255 to 254 in case of a 255 by 255 image. The purpose of location map is to indicate the particular change made while data hiding. Moreover, data is encrypted to prevent any unauthorized visit or attack that will affect the entire communication system. One of the major applications of data hiding comes in communication among the soldiers during a terrorist attack, where the secrecy of data is much important. Hence more efficient data embedding capacity means more possibility of secret message transmission.

Data retrieval is yet another important feature of this paper. After the particular application of communication, the hidden secret message is retrieved from the image. For this first the location map is decompressed. Then embedded secret message is retrieved. After that we get the original image back without any deformation. Finally, the image in text form is converted back to its original pixel combinations with the help of MATLAB software.

This paper gives an analysis of the embedding capacity of the conventional rhombus prediction algorithm and newly analyzed one with boundary expansion as the core principle. The paper also introduces a lossless compression of location map using new variable run length encoding scheme that is simple and easy to code and compress a particular set of run length composed of binary sequences. Later the entire hidden data is retrieved with making no change in the original image thereby showing perfection in data retrieval from the image after use. The paper is analyzed in ModelSim with the help of VHDL language and MATLAB used for conversion an image to text for pixel value calculations.

2. Existing Methodologies

There have been many technologies and algorithms to embed data. Among that most of them make use of converting image into pixel blocks. Then adjacent pixels are used for predicting a pixel value to hide a particular data. Most important existing methodologies for data hiding in an image discussed in the following session include-PEE, O-PEE, A-PEE and AO-PEE.PEE stands for prediction expansion error. In the techniques like c-pee, the pixel desired of an image is selected. Then its surrounding 2 pixels are taken. The average value is taken for calculating the prediction value. In pee based method, a predictor is employed to predict each pixel value named as xi.

Case I: in this, we take two adjacent pixels. If the differences say, D =0, it means no data hiding is needed for that particular pixel value. If D = -1, bit data is assumed to be -1.

Case II: one pixel and its surrounding pixels are considered here. As a result more embedding capacity can be seen here. So we take one pixel and its surrounding neighborhood pixels and average value is calculated.

Case III: here a range of pixel values can be kept as $a < e_i < b$, where **a** and **b** forms the two threshold values. But here also the data embedding is limited to these two pixel threshold values. Hence embedding capacity is limited.

3. Rhombus Algorithm

Rhombus algorithm is the core concept of this paper implementation. The paper is analyzed with modifying the rhombus system in order to increase the pixel - data embedding capacity. Rhombus algorithm make use of a pixel as reference and with respect to that the surrounding four pixels are taken to calculate the average prediction value in order to embed the secret data accordingly.

3.1. PEE Calculation

In the paper, cover image is divided into two sets denoted as “shadow” and “blank”. One half of the secret message will be embedded into shadow pixels and the rest half will be embedded into blank pixels.

In this case, twice embedding need to be processed to cover the whole image and the prediction of blank pixels is processed only after the embedding of shadow pixels is completed.

Here the “fig.1” has been analyzed by taking a sample of five pixels, four of them surrounding the selected pixel value in a rhombus shaped pattern in a nine squared number system. Pixel number V1, V2, V3 and V4 are the surrounding pixels of selected pixel xi. On taking their average value we get the $x_{i^\wedge}$.

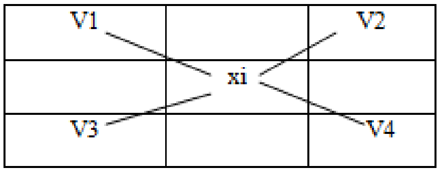

Figure.1.Rhombus formation of a selected pixel x_i

Then the prediction error, e_i is computed. The rhombus equation is given as,

$$\tilde{e_i} = \begin{cases} e_i, & \text{if } a_n < e_i < b_n \\ e_i + m, & \text{if } e_i = b_n \\ e_i - m, & \text{if } e_i = a_n \\ e_i + 1, & \text{if } e_i > b_n \\ e_i - 1, & \text{if } e_i < a_n \end{cases} \qquad (1)$$

Here, m is the secret message to be hidden or retrieved from the image as per the conditions. As an example during paper analysis, a_n is chosen as -2 and b_n as +2. So a_n and b_n can be considered as the two threshold values or limit up to which the embedding process is carried out. They can be taken any value under the condition that a_n must not be bigger than b_n.

3.2. Data Hiding

For paper implementation the following sample of “fig. 2” has been selected for the purpose of secret message embedding and retrieval. The entire image is divided into shadow and blank pixels. This is called shadow and blank pixels partitioning. Here, in order to accommodate the entire secret message beyond an image, first the secret bits in binary form are embedded inside shadow pixels. Then the remaining secret data, if available, are inserted in blank pixels. Blank pixel also accommodates location map and LSB replaced bits. Data hiding is from X1 to X9. Let x_i be the chosen pixel of an image for data hiding. In this paper LENA IMAGE has been selected.V1, V2, V3 and V4 are the neighboring pixels that form a rhombus shape around x_i. The average values of surrounding pixels are calculated.

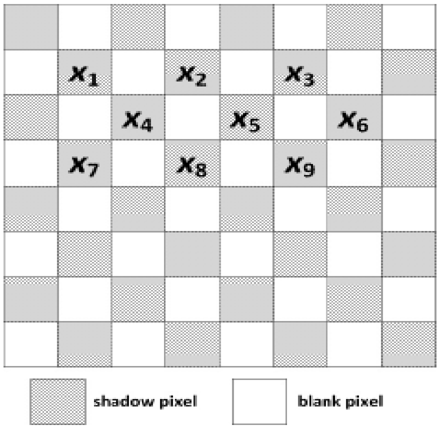

Figure.2.Shadow and blank pixel partitioning.

4. Proposed System

In the present paper reversible data hiding is performed by embedding a secret message of length 20 bits in a 512 by 512 image. Reversible means the data can be retrieved after the use without affecting the original image. For this rhombus error prediction algorithm is used in a modified manner to increase the embedding capacity. In this paper first the image is converted to textual file in MATLAB, and then with the obtained pixel values rhombus algorithm is performed. In that a boundary expansion technique is performed in order to increase the embedding capacity from the previous one. After that the compression of an already created location map is performed using variable run length coding scheme. The secret message to be embedded is encrypted for protection which lacks in many conventional technologies. After the particular use the data is extracted and original image is retrieved back to its form by converting text to image in MATLAB.

4.1. Image to Text

An image is comprised of a collection of pixel values. For the calculation of pixel values comprised in an image, the image is first converted to textual format using MATLAB language. For this the color image is converted to black and white that is RGB image to gray scale. Gray scale usually contains 512 lines with each 512 integer value.

4.2. Location Map

Within an image is the under flow or over flow condition of bits. This may lead to an insufficiency in secret data hiding. To avoid the over flow or underflow condition, 0 pixels is assumed to be 1 and 255 is assumed to be 254, respectively. Hence a location map is needed to indicate this change made. Therefore there comes a need to hide the location map along with the secret message inside an image. When the location map becomes very large it may consume the entire space for secret message embedding. Hence the location map needs to be compressed. Location map is a binary sequence of 0's and 1's.In previous rhombus embedding techniques location map is compressed arithmetically. Results have shown that arithmetic compression is a complex process making compression of location map difficult. By focusing on simplicity, in the present paper location map is compressed lossless using variable run length coding scheme. The total size of location map is assumed to be the exact size of image used. Initially, location map is set to zero. Later, a change of overflow or underflow condition produces a 1 in location map. During data retrieval, location map is expanded and cover image is obtained originally. Run length is a sequence of 0's ending with 1.codeword is obtained by adding +2 to the run length. If group number is ―n‖ then both improved code word and code sequence 2 will have n-bits and final code will have 2*n bits. The final code word is compressed and embedded. Sequence 2 gives the number of bits that is group number on data retrieval (when the location map is decompressed) and it always ends in 1.

4.3. Boundary Expansion

Boundary expansion is a modification to the figure no.2 of the conventional rhombus prediction algorithm. One of the major disadvantage of the conventional rhombus prediction algorithm is the exclusion or elimination of pixels located around the edge of an image. These pixels are not used for embedding the secret message, since in these pixels the rhombus calculation cannot be performed due to the lack of adjacent neighboring pixels that forms a rhombus structure. As a result the data hiding is started from pixel number X1 in figure 3.So this reduces the embedding capacity of secret message since the entire image is not utilized for this purpose. Here comes the need for boundary expansion where the entire image is included for data hiding. Hence more embedding capacity is obtained.

The technique of expansion is explained briefly in the following "fig.3".

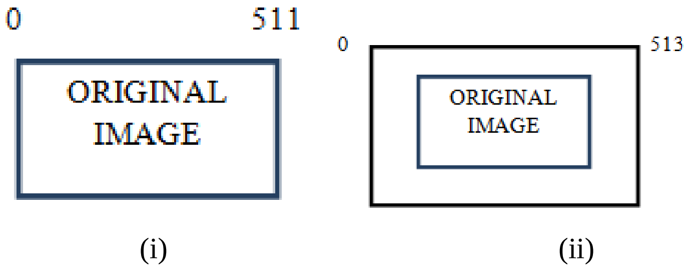

Figure.3.Different sections of boundary expansion: (i) shows the original image of 512 by 512 pixels,(ii) shows the boundary expanded around original image to increase pixel size by 514 by 514.

In the "fig 5(i)" the original image is about size 512 pixels. On adding two extra columns and rows around the figure the total size bedome 514 pixels. This extra added rows and columns forms the boundary expansion. The image with expanded boundary is known as expanded image. now the expanded image holds the following information:

1.secret message of length 20 bits

2.code word of length 32 bits (location map)

During data hiding first shadow pixels are focused. For this expanded boundary is utilized.

4.4.Embedding Capacity

Embedding capacity gives the maximum number of embedding bits. While calculating the embedding capacity the location map is eliminated. Total embedding pixels are given as count display. Count display varies in thousands of pixels from conventional rhombus method to the present analyzed paper.

4.5.Data Encryption

Data encryption is performed to give a protection or secrecy of data to prevent its access from unauthorized personalities. For this an encryption key is used whose length is equal to the length of secret message. Same length key word is selected and direct bit by bit XOR operation is performed and only key word is retrieved. Key word is known prior to the receiver and is send along with the receiver.

4.6.Data Retrieval

Data retrieval is efficiently implemented in this paper without making any change in the original image. Once the error value is obtained, the secret bit is retrieved from the pixel values. This equation is the reverse of equation no.1. Hence reversibility achieved. For data retrieval the following rhombus equation has been performed:

$$e_i = \begin{cases} \tilde{e}_i, & \text{if } a_n \leq \tilde{e}_i \leq b_n \\ \tilde{e}_i - 1, & \text{if } \tilde{e}_i > b_n \\ \tilde{e}_i + 1, & \text{if } \tilde{e}_i < a_n \end{cases} \qquad (2)$$

During extraction, first the 32 bit compressed location map and then the secret message is retrieved, i.e. in rhombus structure first the data hidden in blank pixels are taken back then the shadow pixels' data are considered.

4.7. PSNR count

PSNR means peak signal to noise ratio, is the error metrics used to compare the image compression quality. In this paper, PSNR is calculated in MATLAB coding language and studied its comparison.

5.Results And Discussions

The following section gives the experimental studies of the paper trying to implement in ModelSim software in VHDL language, section by section. The MATLAB software is used for conversion of image to pixel formats and for PSNR value calculation for the conventional rhombus prediction algorithm and the boundary expanded system.

The embedding capacity calculation is analyzed to be implemented in Modalism simulation which is expected to be increasing in case of the proposed boundary expansion technique. The following table 1 gives a brief analysis of the different modifications trying to be carried out in this whole paper.

Table.I. Comparison table showing deviation of proposed system from existing paper.

Feature	***Conventional method***	***Proposed method***
Data privacy	Protection not mentioned	Data encrypted
Location map compression	Arithmetic coding (Complex)	Variable run length losseles coding. (Simple technique)
Embedding capacity	Entire image not considered. (Capacity low)	Boundary expanded method. (Capacity raised)
PSNR	76.64	76.86

6.Conclusion

Hence a modified rhombus perdition data embedding system was able to be analyzed with increased embedding capacity. And a study on further boundary expansion was conducted as a future scope to increase the embedding capacity. The analyzed system finds its major application in real time communication purposes. eg; Secret communication among soldiers during a terrorist attack.

Acknowledgement

I express my sincere thanks to my guide Mr.Ajeesh S for his valuable guidance and useful suggestions, which helped me throughout this work.

REFERENCES

[1].Y. Q. Shi, *"Reversible data hiding," in Proc. IWDW, vol. 3304. 2004, pp. 1–12.*

[2]. R. Caldelli, F. Filippini, and R. Becarelli, *"Reversible watermarking techniques: An overview and a classification," EURASIP J. Inf. Security, vol. 2010, Jun. 2010, Art. ID 134546.*

[3].J. M. Barton, *"Method and apparatus for embedding authentication information within digital data," U.S. Patent 5 646 997, Jul. 8, 1997.*

[4].C. W. Honsinger, P. W. Jones, M. Rabbani, and J. C. Stoffel, *"Lossless recovery of an original image containing embedded data,"U.S. Patent 6 278 791, Aug. 21, 2001.*

[5].G. Coatrieux, C. Le Guillou, J.-M.Cauvin, and C. Roux, *"Reversible watermarking for knowledge digest embedding and reliability control in medical images," IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 2,pp. 158–165, Mar. 2009.*

[6].F. Battisti, M. Carli, and A. Neri, *"Secure annotation for medical images based on reversible watermarking in the Integer Fibonacci–Haar transform domain," Proc. SPIE, vol. 7870, p. 78700G, Feb. 2011.*

[7].S. Lee, C. D. Yoo, and T. Kalker, *"Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 321–330, Sep. 2007.*

[8].R. Y. M. Li, O. C. Au, C. K. M. Yuk, S.-K. Yip and T.-W. Chan, *"Enhanced image trans-coding using reversible data hiding," in Proc.IEEE ISCAS, May 2007, pp. 1273–1276.*

[9].K. Hwang and D. Li, *"Trusted cloud computing with secure resources and data colouring," IEEE Internet Compute., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.*

[10].J. Fridrich, M. Goljan, and R. Du, *"Invertible authentication," Proc. SPIE, vol. 4314, pp. 197–208, Aug. 2001.*

[11].J. Fridrich, M. Goljan, and R. Du*, "Lossless data embedding—New paradigm in digital watermarking," EURASIP J. Appl. Signal Process., vol. 2002, no. 2, pp. 185–196.*

ABOUT AUTHORS

Ms. Anigha Johnson, currently pursing PG in VLSI Design under APJ Abdul Kalam Technological University from IES college of Engineering, Thrissur, Kerala, India. She received her B.Tech in Applied Electronics and Instrumentation from University of Calicut in 2015.She has presented her B.Tech final year project in the event Mestech Paper presentation held at MES College of Engineering, Kerala and secured first prize. She has published her M.Tech mini project paper in journal, Vol.5. Her area of interests includes VLSI signal processing and Digital system design.

Mr. Ajeesh S, currently working as Assistant professor in Department of Electronics and Communication Engineering, in IES College of Engineering, Thrissur, Kerala, India. He completed his B.Tech from Cochin University of Science & Technology and M.Tech from Kerala University. He has an experience over five years. His area of interests includes Signal Processing, Image Processing and Microcontroller.

Ms. Anoopa Jose Chittilappilly, received her B.Tech degree in Electrical & Electronics Engineering from Kannur University in 2003 and M.E. degree in APPLIED electronics from Anna University in 2005.Since 2005 she is working I.E.S College of Engineering, Thrissur, Kerala. She is doing her Doctoral program at Karpagam University. Her research interests are Image & Signal Processing.